PÔLE D'EXCELLENCE CYBER

GUIDE V.3

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

Novembre 2025

Région BRETAGNE

MINISTÈRE DES ARMÉES ET DES ANCIENS COMBATTANTS

SOMMAIRE

REMERCIEMENTS

Nous tenons à remercier les différents contributeurs à l'élaboration de cette 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** et Jérôme **LAINÉ** délégué régional Bretagne de l'ANSSI successifs qui nous ont accompagné dans cette initiative ;
- Guillaume **CHÉREAU** et Valentin **CHUZEL** responsables successifs du CSIRT Breton Breizh Cyber qui ont, en particulier alimenté nos réflexions de retours terrains très concrets ;
- Amandine **DEL AMO** de Cybermalveillance.gouv.fr qui nous a apporté tout le retour d'expérience de sa structure
- Florian **DUMAS**, RSSI du département de l'Isère et représentant le club de la sécurité numérique des collectivités, club regroupant plus de 120 RSSI de collectivités, pour ses contributions, en particulier sur le juste nécessaire dans la commande de services et produits de cybersécurité, 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, et Jeanne **DUGUE** qui nous ont apporté leur 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 ;
- Martin **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 pouvons compter pour la promotion de ces travaux.
- Jean-Nicolas **ROBIN**, AVOXA avocat associé, docteur en droit pour sa contribution sur le volet des assurances cybers.
- Nathan **VITAL** – Doctorant en psychologie cognitive – en CIFRE chez Alcyconie et Stéphanie **LEDOUX** – CEO Alcyconie pour leur contribution à la bonne prise en compte des effets physiques et psychologiques d'une crise cyber
- Nous remercions également Jérôme **ALLAIRE**, maire d'Entrammes (53260), qui nous a aidé à 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 assuré tout au long de nos travaux de l'adéquation du document au vécu et contraintes des maires de petites communes.

CSF des industries de sécurité

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

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 nouvelle 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. Il est complété de la version précédente d'un volet assuranciel, de quelques éléments sur les risques physique et psychologique d'une crise cyber sur les agents, de quelques éléments sur les responsabilités et les mesures à mettre en place en matière de protection des données personnelles ainsi que sur les bonnes pratiques cyber dans le cas d'achats de produits ou services.

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, comme pour cette version des éléments complémentaires mentionnés supra.

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, ces échanges ont mis en évidence des axes de travaux 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 ressources 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 2025 le 18 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 participation gratuite sous réserve d'inscription : www.european-cyber-week.eu

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 ce risque, 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, le peu de cadres 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.

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 principalement :

- Logiciel de gestion de la cuisine centrale communale (gestion des stocks, des commandes, du grammage des denrées, etc.) destiné à l'approvisionnement en repas des structures d'accueil, telles que les Établissement d'Hébergement pour Personnes Âgées Dépendantes (EHPAD) ou les écoles maternelles et élémentaires ;
- 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[3] [3]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. Il est à noter que 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. Ne pas hésiter à nous faire remonter ceux qui vous sembleraient manquer dans cette liste (pa.pincemin@rennesmetropole.fr ; jean.godot@all4tec.net).

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.

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

3 Une solution dite SaaS (« Software as a Service » ou en français : « logiciel en tant que service ») est une solution logicielle applicative hébergée dans le cloud et exploitée en dehors de la collectivité par un tiers, aussi appelé fournisseur de service.

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, en général, une note de rançon. Dans ce cas, il est recommandé de faire appel au CSIRT régional dont la commune dépend (voir liste en annexe A).

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 et de la faire figurer dans le PCS.

Le premier geste donc, le plus important, consiste à couper le réseau informatique en débranchant le câble réseau, se mettre en mode avion pour les connexions 4G/5G ou couper la box internet. L'attaquant n'aura alors plus de prise sur le système d'information.

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 ». Même si le réseau est coupé, des logiciels malveillants implantés par l'attaquant pourrait corrompre ces dernières si vous les connectez.

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 en contactant le 17Cyber[1] [1]
- Le CSIRT de votre région s'il y en a un (voir annexe A).

Pour le premier et le denier, 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 ExpertCyber5[2] délivré par Cybermalveillance.gouv.fr voire une qualification de l'ANSSI[3].

Il est aussi **impératif de prévenir au plus tôt les collaborateurs pour éviter de mauvaises manipulations** qui pourraient aggraver la situation. Sans doute prévoir un message type pour ce faire dans le PCS et d'y préciser qui le communique aux agents.

1 https://www.cybermalveillance.gouv.fr/17cyber

2 https://www.cybermalveillance.gouv.fr/tous-nos-contenus/securisation-cybersecurite-professionnels#definition-service-securisation

3 https://cyber.gouv.fr/decouvrir-les-solutions-qualifiees

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 les messages publics à porter collectivement. 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[4]. La liste des partenaires à prévenir en priorité doit figurer dans le PCS avec leurs coordonnées, parmi eux la DDFIP bien au fait des impacts des attaques cyber et des bonnes mesures les concernant pour limiter les impacts. Un message type peut aussi être prévu dans le PCS pour la première alerte publique.

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 et le délégué à la protection des données, ou la personne ayant cette fonction, en cas d'impact sur des données personnelles. Ne pas sous-estimer par ailleurs l'impact potentiel d'un crise cyber sur les moyens de communications (mail, téléphone, accès aux fichiers…).

La cellule de crise doit enfin permettre d'évaluer le niveau de risque pour la vie privée des personnes concernées en cas de violation de données personnelles et la nécessité de déposer plainte auprès des forces de l'ordre :

- 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 ;
- Les dépôts de plaintes peuvent être déposés auprès d'un commissariat de Police ou une Brigade de Gendarmerie.
- Préalablement vous pouvez vous appuyer sur une assistance technique par un policier ou un gendarme 24h/24, 7j/7. Il est accessible via https://www.17cyber.gouv.fr/.

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 ces 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 téléphones, noms, mails, risques particuliers 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/ou renseigner. La fiche réflexe à vocation à être intégrée dans le PCS. Elle doit pouvoir servir de fil rouge pour la cellule de crise.

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'affinent et cela permet de s'assurer que la fiche est à jour. Y convier quelques agents en observateur peut par ailleurs être des meilleurs effets en termes de sensibilisation mais aussi en termes de communication comme quoi le sujet est pris au sérieux.

Une fois le volet cyber de votre PCS élaboré, comparez-le à ceux des autres risques type ORSEC, cela vous permettra sans doute de l'affiner.

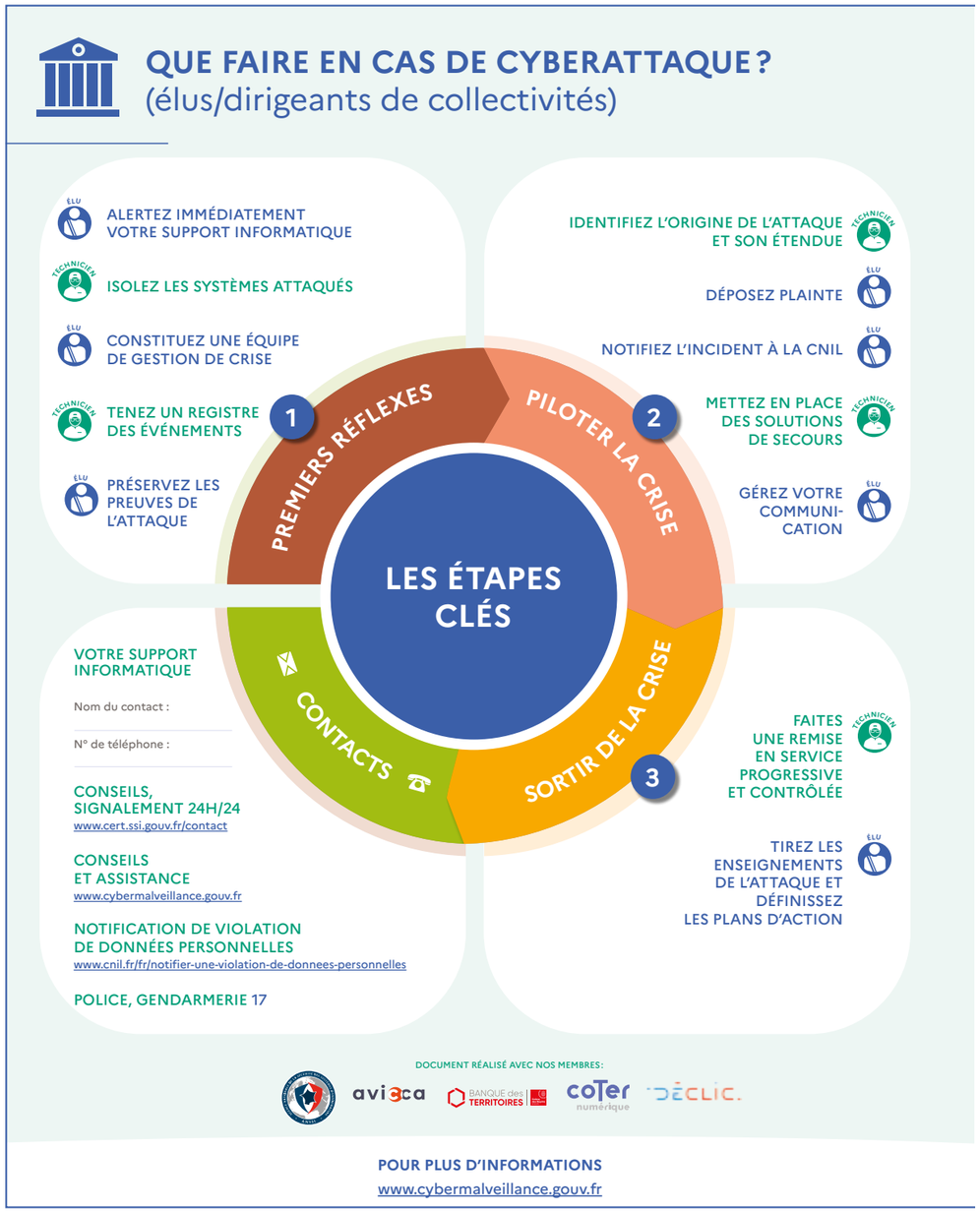
Dans une logique de partage de bonnes pratiques nous sommes preneurs de vos résultats afin de les partager dans des versions ultérieures du document (pa.pincemin@rennesmetropole.fr jean.godot@all4tec.net).

Il est à noter que vous ne serez pas forcément les premiers à identifier l'attaque cyber qui se met en place au sein de votre commune. Le CISRT, les services de l'Etat, … peuvent, grâce à leurs outils qui fonctionnent en continue, entrevoir un tel évènement. Afin que vous ne soyez pas surpris de tels appels mais au contraire que vous les reconnaissiez comme des interlocuteurs de confiance, il faut les identifier en amont. Le délégué régional de l'ANSSI peut être une aide pour ce faire. Vous trouverez la liste des délégués dans les différents territoires en annexe A2 (https://cyber.gouv.fr/delegues-territoriaux).

4 pour approfondir ce point consulter le guide de l'ANSSI https://cyber.gouv.fr/publications/anticiper-

RÉPUBLIQUE FRANÇAISE
Liberté
Égalité
Fraternité

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



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

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.

Une crise d'origine cyber est une crise comme les autres. Aussi les principes généraux de gestion de crise s'appliquent. C'est pourquoi les collectivités dotées d'un PCS peuvent utiliser le dispositif de gestion de crise prévu dans ce cadre comme base de travail.

Les spécificités principales d'une gestion de crise cyber à prendre en compte sont les suivantes :

- La dégradation ou la compromission possible des moyens de communication et des systèmes d'information sur lesquels s'appuient les dispositifs de crise (et pour lesquels il faut définir des moyens et procédures dégradés)
- La nature transversale de la crise (ensemble des services et métiers de la collectivités impactés), les systèmes d'information irriguant l'ensemble des services
- Des impacts immédiats, et dans le cas des cyberattaques par rançongiciel, un temps de remédiation qui peut être très long et donc une cinétique de gestion de crise qui s'inscrit souvent dans le temps
- Une communication de crise difficile à appréhender étant donné les inconnues ou incertitudes en début de gestion de crise autour du déroulé des faits.

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

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[1] : 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 abonnements de téléphones portables de secours pour pallier toute panne imprévue ;
- Messagerie instantanée sécurisée : l'usage d'une messagerie instantanée sécurisée facilite les échanges rapides en asynchrone entre les membres de la cellule, notamment lorsqu'ils ne peuvent pas être présents simultanément. **Tchap,** solution développée par l'État, est à privilégier par rapport aux messageries grand public (WhatsApp, Messenger, etc.), car elle garantit un niveau de sécurité adapté aux communications sensibles et permet une interconnexion avec les agents disposant d'une adresse professionnelle. Son utilisation doit être anticipée, avec la création des groupes de discussion nécessaires et la vérification de l'accès pour chaque membre concerné.

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.

1 Lignes classiques encore fonctionnelles, qui ne dépendent pas d'une connexion Internet, pour assurer une solution de secours en cas d'indisponibilité des lignes téléphoniques numériques (VoIP)

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 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.

Il est impératif de garder à l'esprit qu'une crise cyber c'est plusieurs jours voire semaines de hauts risques.

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 d'une attaque cyber ou les prévenir en amont

1. Faire un test de maturité cyber de son organisation en 5mn

La maturité cyber reflète le niveau global de prise en compte des enjeux de cybersécurité par une organisation. Répondez à 6 questions pour obtenir votre évaluation indicative.

https://messervices.cyber.gouv.fr/test-maturite/

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

De nombreuses sources présentent 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. Séparez strictement vos usages à caractère personnel de ceux à caractère professionnel
2. Mettez régulièrement à jour vos outils numériques
3. Protégez vos accès par une authentification double-facteur lorsque c'est possible, ou a minima par des mots de passe complexes
4. Ne laissez pas vos équipements sans surveillance
5. Prenez soin de vos informations personnelles en ligne
6. Protégez votre messagerie électronique
7. Évitez les réseaux Wi-Fi publics ou inconnus
8. Sauvegardez régulièrement vos données
9. Protégez-vous des virus et autres logiciels malveillants
10. Accordez le juste niveau de privilèges

Vous retrouverez ces éléments en détail sur le site de l'ANSSI : https://cyber.gouv.fr/appliquer-les-dix-regles-dor-preventives

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.

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

La sensibilisation des agents aux risques cyber 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 «cybermois». 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://www.cybermalveillance.gouv.fr/tous-nos-contenus/actualites/cybermois-2025

4. Prise en compte de la protection des données personnelles lors d'une crise cyber

Chaque collectivité doit désigner un délégué à la protection des données (DPO) chargé d'accompagner les services dans la mise en conformité et la gestion des incidents liées aux données personnelles.

Il est à noter que pour une petite commune il n'est pas envisageable d'avoir un DPO à plein temps et il est très souvent difficile d'avoir parmi son personnel une personne qualifié pour porter cette mission. Pour ce faire certains organismes mettent en place des DPO partagés pour les collectivités au sein des centres de gestion départemental comme le CDG35, certains opérateurs publics de services numériques (OPSN)… C'est, pour les petites collectivités, la solution à privilégier.

Parmi ces incidents figure la violation de données qui survient lorsqu'un évènement compromet la sécurité des informations relatives à des personnes physiques. Ce type d'incident peut avoir différentes origines : vol ou perte de supports, accès non autorisé, modification accidentelle ou diffusion non maîtrisée de données. Il nécessite alors de s'interroger sur une possible atteinte à la vie privée, si une utilisation malveillante de ses informations venait à être faite.

Prévenir la survenance des risques en amont d'une crise cyber

L'intégration, dès la conception de vos traitements de données, des principes protection des données personnelles - telles que la minimisation des données collectées, une durée de conservation limitée, un contrôle rigoureux tout au long de leur utilisation, un encadrement contractuel approprié, des mesures de sécurité appropriées – permet de réduire significativement le risque qu'une cyberattaque compromette la vie privée de vos citoyens et de vos agents.

Il est également indispensable de tenir à jour le registre des traitements et de disposer d'une cartographie précise des données personnelles traitées, afin de pouvoir réagir rapidement et efficacement en cas de violation de données. Ces éléments vous permettront de fournir des informations détaillées sur : la nature de la violation, les personnes impactées et les conséquences potentielles pour celles-ci.

Agir pendant une crise cyber

En cas de cyberattaque entraînant une violation de données personnelles, une gestion rapide et structurée est indispensable. Dès la réunion de crise, il convient d'évaluer le niveau de risque que cette violation fait peser sur les personnes concernées et les obligations qui en découlent.

Cas où la violation de données ne présente aucun risque pour les personnes
Une violation de données ne présente aucun risque lorsque l'incident est maîtrisé et n'a pas d'impact potentiel sur les droits, la sécurité ou la vie privée des personnes concernées. Cela signifie que les données n'ont pas été exposées, qu'elles sont toujours protégées ou qu'elles sont inexploitables pour un tiers. Dans ce cas l'incident doit seulement être documenté en interne.

Exemple : Perte d'un support chiffré (ordinateur, clé USB) dont le chiffrement est robuste et les clés de déchiffrement sécurisées, erreur de destinataire lors d'un envoi ne révélant pas d'informations sur les personnes.

Cas où la violation de données présente un risque pour les droits et libertés des personnes
Une violation de données présente un risque lorsqu'elle peut entraîner un préjudice potentiel pour les personnes concernées tel qu'une atteinte à la confidentialité, à la sécurité ou à une perte de contrôle des données. Dans ce cas l'incident doit être documenté en interne et faire l'objet d'une notification à la CNIL dans les 72h après la prise de connaissance de la violation de données via le portail suivant : https://notifications.cnil.fr/notifications/index

Exemple : Accès non autorisé à un nombre limité de données (nom, prénom) sans éléments sensibles.

Cas où la violation de données présente un risque élevé pour les droits et libertés des personnes
Une violation de données présente un risque élevé lorsqu'elle entraîne des conséquences graves ou irréversibles pour les personnes : usurpation d'identité, exposition de données sensibles, fraude… Elle concerne souvent un volume important de données et/ou une sensibilité élevée et/ou une large diffusion non maîtrisée. Dans ce cas, l'incident doit être documenté en interne, faire l'objet d'une notification à la CNIL dans les 72h après la découverte de la violation de données et les personnes concernées doivent être informées individuellement, dans les meilleurs délais, de la nature de la violation, de ses conséquences et des mesures prises pour y remédier.

Exemple : Accès non autorisé à des données relatives à la santé physique ou mentale des personnes, un grand volume de données de citoyens a été rendu publique, vol d'un mot de passe et d'un identifiant d'un compte possédant des droits étendus type «administrateur» ou volonté de nuire aux personnes en diffusant via le compte des propos injurieux, des messages malveillants.

Chapitre VI : Crises cyber : les impacts psychologiques durables sur les agents des collectivités territoriales

Les cyberattaques visant les collectivités territoriales se multiplient, révélant leur vulnérabilité face à des menaces numériques de plus en plus sophistiquées. Mais au-delà des dégâts techniques et des blocages institutionnels, ces crises provoquent aussi des effets psychologiques profonds et durables chez les agents territoriaux. Ces derniers, en première ligne pour tenter de maintenir un minimum de service public, doivent faire face à une réalité déstabilisante : la perte soudaine de leurs outils, de leurs repères et parfois de leur utilité apparente.

La sidération initiale et la rupture brutale du quotidien

Dès les premières heures d'une attaque, les agents se retrouvent confrontés à une situation inédite : ordinateurs inutilisables, téléphonie coupée, impossibilité d'accéder aux données, voire aux bâtiments dans certains cas. Cette paralysie numérique peut se traduire en impacts psychologiques forts impliquant une projection brutale des agents dans un environnement de travail dégradé, sans consignes claires, avec le sentiment d'être livrés à eux-mêmes.

Cette sidération est souvent amplifiée par un sentiment profond d'incompréhension. En effet, peu de formations intègrent véritablement la culture du risque cyber et encore moins l'idée que ce type de menace puisse un jour les concerner directement. Or, la littérature scientifique souligne l'importance de prendre en compte certains déterminants psychologiques dans la préparation à ce type de crise. La perception du risque cyber, le sentiment d'auto-efficacité (de réponse face à ces crises) ou encore le sentiment de contrôle (sur la situation) sont autant de facteurs qui influencent la manière dont les individus vivent et réagissent face à une situation de crise d'origine cyber. D'où la nécessité de leur fournir des ressources appropriées pour favoriser une meilleure préparation psychologique et opérationnelle.

Cependant, dans ce contexte organisationnel de plus en plus numérisé accompagné d'une dépendance aux systèmes d'informations, cette irruption soudaine du chaos informatique provoque un désalignement brutal entre les missions attendues et les moyens disponibles (en amont comme en aval) pour les remplir.

Assurer la continuité du service public : une pression mentale intense

L'un des éléments les plus marquants est la tension entre le devoir de continuité du service public– un pilier du travail en collectivité – et l'impossibilité matérielle d'y répondre. Cette dissonance, ainsi que la pression résultant de la situation, engendrent un stress intense. Pour de nombreux agents, notamment ceux en contact direct avec la population (état civil, aides sociales, inscriptions scolaires…), ne pas pouvoir aider ou répondre aux besoins des usagers génère un fort sentiment d'impuissance et d'auto-efficacité réduite quant à ses prérogatives professionnelles, pouvant se traduire par la culpabilité.

Cette pression est d'autant plus forte que les usagers, eux aussi, sont souvent dans l'incompréhension. L'absence de communication claire ou régulière sur la nature de la crise ou les délais de rétablissement jouent défavorablement sur la confiance accordée envers l'institution, pouvant ainsi accroître l'agressivité ou l'hostilité de certains administrés, renvoyée directement aux agents.

Une crise qui s'inscrit dans la durée… et dans les esprits

Contrairement à d'autres formes de crise, une attaque cyber n'est pas un événement ponctuel.
Les effets se déploient dans le temps : les investigations techniques, les restaurations de données, les phases de test, la réintégration progressive des outils numériques… Tout cela peut prendre des semaines, voire des mois. Cette temporalité longue fragilise les agents, qui doivent jongler entre solutions bricolées et procédures transitoires, sans perspective claire de retour à la normale.

Ce flou prolongé alimente la fatigue psychologique (traduit par une charge cognitive amplifiée), d'autant plus marquée chez les agents chargés de la gestion de crise ou ceux désignés pour porter la communication auprès des équipes. Pour ces derniers, la répétition des mauvaises nouvelles, la surcharge émotionnelle et l'absence de reconnaissance peuvent conduire à un véritable épuisement.

Le retour à la normale : une illusion ?

Lorsque les systèmes sont enfin rétablis, on parle souvent de "retour à la normale". Mais pour les agents, sur le plan psychologique, rien n'est vraiment comme avant. D'un point de vue professionnel, plusieurs aspects peuvent être touchés. L'expérience de la crise laisse des traces : anxiété latente, perte de confiance dans les outils ou les procédures internes, méfiance envers les outils numériques persistante voire sentiment d'abandon par la hiérarchie si l'accompagnement post-crise a été déficient. Certains agents témoignent aussi d'une forme de dévalorisation de leur travail durant la crise, perçu comme secondaire ou inefficace. D'autres conservent un sentiment d'illégitimité : pourquoi ont-ils été si peu préparés ? Pourquoi n'ont-ils pas su quoi faire ? Ce besoin de sens, de reconnaissance et de formation ressort comme un facteur clé dans la prévention des effets psychologiques à long terme.

D'un point de vue intra-individuel, la littérature scientifique nous renseigne sur les conséquences psychiques que peuvent avoir ces situations. Les recherches indiquent que certaines formes de cyberattaques peuvent entraîner des effets psychologiques comparables à ceux d'événements traumatiques plus classiques. Les victimes peuvent développer un stress émotionnel important, parfois accompagné de symptômes dépressifs ou de réactions proches du trouble de stress aigu.

La nature immatérielle de l'agression n'en diminue pas l'impact : elle le rend parfois plus insidieux, car difficile à circonscrire ou à verbaliser.

Vers une prise en compte du facteur humain

Face à ces constats, les collectivités doivent intégrer dans leur stratégie de résilience non seulement les outils techniques et les processus, mais aussi le facteur humain. L'anticipation passe par la sensibilisation et la formation, mais aussi par l'organisation d'exercices de crise qui permettent de se confronter à ces situations et de rassurer les équipes. Ainsi l'objectif est de pouvoir influencer favorablement des facteurs psychologiques clés afin que les opérateurs soient toujours mieux préparés à ces situations.

Si les retours d'expérience, à l'occasion d'entretiens individuels et collectifs (à systématiser après un exercice de crise ou une crise réelle) peuvent permettre aux collaborateurs de mettre des mots sur la période traversée, sur son intensité et ce qu'elle a fait naître, un accompagnement post-crise – psychologique, collectif et managérial – peut s'avérer essentiel pour permettre aux agents de retrouver un équilibre et reconstruire un sentiment d'utilité et de sécurité dans leur mission de service public.

Et concrètement ?

1. Préparer les équipes en amont :
- Sessions de sensibilisation intégrant la dimension psychologique et non uniquement technique ;
- Exercices de crise incluant toutes les strates de l'organisation, pas seulement l'IT ;
- "Kit de crise" accessible : consignes, contacts internes, ressources psychologiques.

2. Soutenir pendant la crise :
- Cellule de communication interne régulière et claire en ayant une attention particulière à la communication interne ;
- Relais psychologiques ou RH identifiés et disponibles ;
- Suivi de la charge des équipes mobilisées pour éviter l'épuisement ;
- Accompagnement spécifique des équipes de réponse à incident, particulièrement ciblées par la pression des attaquants.

3. Accompagner après la crise :
- Debriefings collectifs et individuels pour verbaliser et partager l'expérience ;
- Mise à disposition de dispositifs d'écoute psychologique et ou de psychologues du travail et des organisations directement sur place ;
- Reconnaissance officielle de l'engagement des équipes et intégration des enseignements dans les plans futurs.

Chapitre VII : Spécification pour la commande du juste nécessaire en solutions de cybersécurité

La sécurité d'un Système d'Information (SI) repose avant tout sur la réduction des risques qui le menacent.
Pour bien protéger votre SI, il est indispensable de commencer par évaluer les risques existants et les mesures de sécurité déjà en place. Cette étape permet d'avoir une vision claire de la situation et de définir une stratégie de sécurisation adaptée.

Pour ce faire, vous pouvez vous référer au chapitre IX : Comment savoir où en est la résilience des systèmes et le niveau de protection des données : éléments d'analyse de risque…

1. Prioriser les actions selon les faiblesses identifiées

Il est **important d'identifier les points faibles de votre SI** et de concentrer les efforts sur ces éléments en priorité. Rappelez-vous :

La **sécurité globale de votre SI sera toujours limitée par la protection de son maillon le plus faible.**
Par exemple, installer une porte blindée très sécurisée à l'entrée d'une maison n'aura que peu d'effet si les autres portes ou fenêtres restent faciles à ouvrir. Il en va de même pour votre SI : un attaquant cherchera toujours le chemin le plus simple, c'est-à-dire le moins protégé.

2. Protéger les données, un enjeu central

Les **données sont au cœur de l'activité** de chaque commune. Elles **doivent donc être protégées en priorité**. Pour cela, il est fortement recommandé de mettre en place un plan de sauvegarde régulier comprenant une copie des données conservée hors ligne ou sur un site distinct. Cela permet de limiter les conséquences en cas de cyberattaque (destruction, altération, etc.).

La fréquence des sauvegardes (quotidienne, hebdomadaire, mensuelle) dépendra de vos besoins et de votre tolérance à la perte de données. Pour les services externalisés (hébergement, cloud ou SaaS), vérifiez que le prestataire propose un plan de sauvegarde adapté à vos objectifs. Sinon, envisagez une sauvegarde indépendante.

3. La sauvegarde seule ne suffit pas

Attention : sauvegarder vos données ne suffit pas à sécuriser votre SI. Si vous restaurez des données sur un système vulnérable, vous risquez une nouvelle compromission rapidement. Il est donc essentiel de renforcer l'ensemble des protections autour de vos données, en combinant plusieurs mesures de sécurité.

À toutes fins utiles, pour ceux qui souhaiterait approfondir ce sujet, vous trouverez en annexe J quelques éléments sur les objectifs de sécurité et les mesures de réduction de risques ainsi que la liste des produits et services qualifiés ou certifiés.

Chapitre VIII : Comment prendre en compte la cybersécurité dans l'achat de produits et services

1. Quelques recommandations pratiques

La prise en compte de la sécurité dans les achats de logiciels, matériels, …

Les exigences de cybersécurité lors de l'achat d'une solution logicielle et matérielle doivent dépendre de la sensibilité de cette solution : il faut s'interroger sur les impacts de perte de confidentialité des données du système, de perte d'intégrité ou de perte de disponibilité du système. Plus les impacts sont élevés, plus les exigences doivent être fortes.

De la même façon, lors de l'achat d'une solution logicielle destinée à traiter des données personnelles, il est essentiel d'adapter les mesures de sécurité au niveau de sensibilité des données concernées. Plus les données seront sensibles, plus les mesures de sécurité devront être fortes. Il convient également de formaliser, dans les contrats, l'ensemble des exigences relatives à la protection des données personnelles.

Lors d'un achat, **le point le plus important à négocier concerne la sauvegarde**. Il s'agit de s'assurer de pouvoir restaurer les données et programmes en cas de compromission. Cette sauvegarde doit être réalisée à intervalles réguliers pour éviter la perte de données, sur un site différent du site de production pour pallier des risques comme l'incendie. Et elles doivent être déconnectées du système d'information pour être sûr qu'un pirate l'ayant compromis ne peut pas porter atteinte à la sauvegarde. Attention, une sauvegarde n'est pas une réplication. La réplication d'un système corrompu est également corrompue…

Sur l'hébergement externe, la vérification majeure concerne la sécurité physique du site, la redondance des services essentiels comme l'alimentation électrique, les liaisons opérateurs, la climatisation, … Les labels ou certifications amènent un certain nombre de garanties faciles à contrôler : HDS, ISO 27001, Tier 3 ou 4 ou encore pour les plus exigeants, le label SecNumCloud. Le lieu d'hébergement est à regarder aussi : préférer des hébergements en France voire en Europe.

Un **système d'authentification peu robuste constitue également un angle d'attaque facile.** Il est aujourd'hui considéré que l'authentification multi facteurs constitue un rempart intéressant contre le piratage. Il s'agit d'associer un facteur de connaissance (un mot de passe, un code connu) avec un facteur de possession (un smartphone, un badge, une clé physique, …) pour autoriser l'authentification. Exiger une authentification multi facteurs pour les systèmes les plus sensibles est un gage de résilience. Pour les autres, il faut travailler sur la robustesse des mots de passe : longueur de 12 caractères minimum, avec une complexité imposée (1 minuscule, 1 majuscule, 1 caractère spécial, 1 chiffre par exemple). Et surtout ne pas oublier la formation et la sensibilisation des utilisateurs qui doivent utiliser un mot de passe différent sur chaque système et gérer leurs mots de passe sur un outil logiciel appelé coffre-fort de mots de passe.

Pour éviter les fuites de données, il est intéressant d'exiger du chiffrement : chiffrement des données lors de leur stockage sur les systèmes informatiques (dit chiffrement au repos) ou lors de leur mouvement (dit chiffrement des flux) avec des protocoles tels que TLS. Sur ce point, une exigence de base peut être de demander le respect des recommandations ANSSI (RGS et Recommandations de sécurité relatives à TLS par exemple).

Un point essentiel concerne le maintien en conditions de sécurité de la solution. En effet, au fil du temps, des vulnérabilités sont publiées sur les solutions informatiques et les attaquants n'ont qu'à les exploiter pour pénétrer dans un système. Toute solution informatique mise en place doit avoir un mainteneur qui s'occupe de surveiller les vulnérabilités et de faire les mises à jour de sécurité.

Enfin, **lors de tout achat, il faut exiger un droit à l'audit qui permet de demander à un «hacker éthique» d'établir un diagnostic sur la robustesse d'une solution informatique** et de dresser un plan d'action de remédiation priorisé en cas de découverte de vulnérabilités. Exiger préalablement l'exécution du plan de remédiation dans le cadre d'un contrat de maintenance permet de diminuer les frais en cas de problème également.

2. 15 bonnes questions à poser à son prestataire de site web

Une cyberattaque de votre site Internet peut avoir de multiples conséquences sur votre activité : arrêt de services, pertes financières, vol d'informations, pertes de confiance et de crédibilité, coût de remédiation, responsabilité juridique…

Voici 15 questions à poser à votre support informatique pour évaluer le niveau de sécurité de votre site Internet et définir les axes d'améliorations nécessaires :

https://www.cybermalveillance.gouv.fr/medias/2022/04/Fiche_mon-site-internet-est-il-securise.pdf

RÉPUBLIQUE FRANÇAISE
Liberté
Égalité
Fraternité

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

MON SITE INTERNET EST-IL SÉCURISÉ ?

Une cyberattaque de votre site Internet peut avoir de multiples conséquences sur votre activité : arrêt de services, pertes financières, vol d'informations, pertes de confiance et de crédibilité, coût de remédiation, responsabilité juridique…

Que vous soyez une entreprise, une collectivité ou une association, voici **15 questions à poser à votre support informatique pour évaluer le niveau de sécurité de votre site Internet** et définir les axes d'améliorations nécessaires.

		OUI	NON	NSP*
1	**LES ACCÈS À MON SITE INTERNET SONT-ILS FILTRÉS PAR UN PARE-FEU ?** Un pare-feu est un équipement qui permet de limiter les accès aux seuls services et machines autorisées.	☐	☐	☐
2	**MON SITE INTERNET EST-IL PROTÉGÉ CONTRE LES ATTAQUES EN DÉNI DE SERVICE ?** Votre opérateur et/ou votre hébergeur peuvent mettre en place des solutions pour absorber la surcharge de trafic de ce type de cyberattaque.	☐	☐	☐
3	**MON SITE INTERNET EST-IL PROTÉGÉ PAR UN ANTIVIRUS ?** Un antivirus peut détecter et bloquer des programmes malveillants qui pourraient être déposés ou stockés sur votre site.	☐	☐	☐
4	**MON SITE INTERNET EST-IL RÉGULIÈREMENT MIS À JOUR DE TOUS LES CORRECTIFS DE SÉCURITÉ MATÉRIELS ET LOGICIELS ?** L'application des mises à jour de sécurité sur toutes les composantes de votre site permet de supprimer les failles de sécurité connues.	☐	☐	☐
5	**MON SITE INTERNET EST-IL RÉGULIÈREMENT SAUVEGARDÉ ET SES SAUVEGARDES TESTÉES ?** Une sauvegarde opérationnelle est indispensable pour pouvoir rétablir votre site Internet dans l'état antérieur à un incident.	☐	☐	☐
6	**LES SERVICES OUVERTS SUR MON SITE INTERNET SONT-ILS LIMITÉS AU STRICT NÉCESSAIRE ?** Chaque service ouvert sur votre site Internet est une porte d'entrée possible pour un cybercriminel. Il convient donc de les limiter à l'indispensable.	☐	☐	☐
7	**L'ACCÈS EN ADMINISTRATION OU PUBLICATION SUR MON SITE INTERNET EST-IL LIMITÉ AUX SEULES PERSONNES ET MACHINES AUTORISÉES ?** Les accès permettant de gérer votre site Internet ou de le modifier doivent être différenciés et faire l'objet d'un contrôle renforcé.	☐	☐	☐

*NE SAIT PAS

RÉPUBLIQUE FRANÇAISE
Liberté
Égalité
Fraternité

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

		OUI	NON	NSP*
8	**LES MOTS DE PASSE D'ACCÈS À MON SITE INTERNET SONT-ILS « SOLIDES » ET « UNIQUES » POUR CHAQUE PERSONNE AUTORISÉE ?** Une mauvaise gestion des mots de passe est l'une des premières causes des cyberattaques.	☐	☐	☐
9	**L'ACCÈS EN ADMINISTRATION OU PUBLICATION SUR MON SITE INTERNET EST-IL PROTÉGÉ PAR UNE DOUBLE AUTHENTIFICATION ?** L'authentification en deux étapes renforce la sécurité des mots de passe en demandant un code de confirmation à chaque nouvelle connexion.	☐	☐	☐
10	**LES COMMUNICATIONS AVEC MON SITE INTERNET SONT-ELLES SÉCURISÉES EN HTTPS ?** Le protocole HTTPS permet de protéger d'une interception les informations échangées entre les postes utilisateurs et votre site Internet.	☐	☐	☐
11	**LE NOM DE DOMAINE DE MON SITE INTERNET EST-IL PROTÉGÉ (DÉPÔT INPI, UTILISATION D'UN VERROU DE REGISTRE…) ?** Il est important d'utiliser les solutions disponibles pour éviter le vol ou le détournement du nom de votre site Internet.	☐	☐	☐
12	**LES EXTENSIONS LOGICIELLES UTILISÉES SUR MON SITE INTERNET SONT-ELLES INDISPENSABLES ET RÉPUTÉES SÛRES ?** Ces extensions peuvent améliorer les fonctionnalités de votre site mais sont également des portes d'entrée possibles pour les cybercriminels.	☐	☐	☐
13	**TOUS LES ACCÈS À MON SITE INTERNET SONT-ILS BIEN ENREGISTRÉS OU JOURNALISÉS ?** La journalisation des accès permet d'identifier des accès illégitimes et de retracer la chronologie d'une attaque.	☐	☐	☐
14	**L'ACTIVITÉ DE MON SITE INTERNET EST-ELLE RÉGULIÈREMENT SURVEILLÉE POUR DÉTECTER UN PIRATAGE ?** La surveillance des connexions et des modifications de votre site permet de détecter et de réagir au plus tôt aux tentatives de cyberattaque.	☐	☐	☐
15	**LA SÉCURITÉ DE MON SITE INTERNET EST-ELLE RÉGULIÈREMENT VÉRIFIÉE ?** Votre site Internet évolue sans cesse. Le maintien de son niveau de sécurité doit donc être régulièrement contrôlé (audit) par des spécialistes.	☐	☐	☐

*NE SAIT PAS

Ce questionnaire peut également vous servir à définir la base contractuelle de la sécurisation de votre site Internet avec vos prestataires en charge de son hébergement, de son maintien en condition opérationnelle, ou de son alimentation en informations.

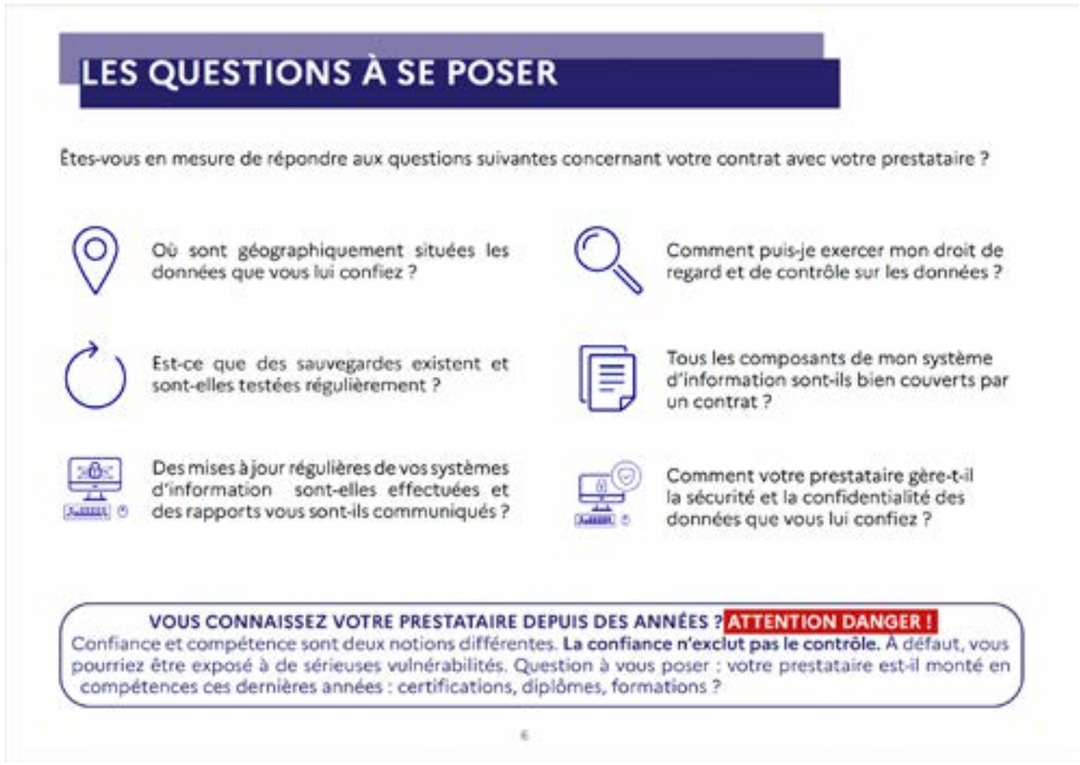
Pour vous aider à sécuriser votre site Internet, vous pouvez faire appel à un professionnel labellisé ExpertCyber sur Cybermalveillance.gouv.fr.
En savoir plus sur la sécurisation de site Internet

3. Cas particulier des infogéreurs

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



Chapitre IX : 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 :

- Vous souhaitez vous protéger contre les cyberattaques mais ne savez pas comment vous y prendre ? Faites un test de maturité cyber de votre organisation : https://messervices.cyber.gouv.fr/test-maturite/ Puis prenez votre cyberdépart ! Bénéficiez d'un premier diagnostic gratuit accompagné d'un Aidant cyber et commencez à renforcer rapidement le niveau de cybersécurité de votre organisation : https://messervices.cyber.gouv.fr/cyberdepart

- Pensé pour et par les entités publiques, MonServiceSécurisé a pour mission d'aider les entités publiques à sécuriser et homologuer les services publics numériques (sites web, applications mobiles et API) : https://monservicesecurise.cyber.gouv.fr/

- L'ANSSI met à disposition des opérateurs réglementés et de la sphère publique une capacité de **cartographie de la surface d'exposition sur Internet** au travers du service SILENE. Cette capacité vise à donner de la visibilité à ces opérateurs sur leur niveau d'exposition et à les accompagner par l'application progressive de mesures adéquates pour le réduire. Cette prestation s'appuie sur l'expérience et l'expertise acquises par l'Agence lors des audits et s'enrichit également, au fil du temps, de l'observation des modes opératoires utilisés par les attaquants. Voir les modalités du service SILENE en annexe H.

- L'ANSSI met à disposition des opérateurs réglementés et de la sphère publique une **capacité d'audit des annuaires Active Directory** (et Samba) au travers du service ADS (Active Directory Security). Voir les modalités du service SILENE en annexe I.

- 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 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 X : L'assurance cyber peut-elle améliorer la cybersécurité des collectivités locales ?

Les cyberattaques contre les collectivités locales se multiplient en France. Ransomwares visant des hôpitaux, paralysie des systèmes de gestion municipale, vols massifs de données personnelles : autant de menaces qui mettent en péril la continuité des services publics. Face à ce risque croissant, l'assurance cyber apparaît comme une solution financière et technique, permettant de couvrir les pertes et d'apporter un accompagnement de crise. Mais cette réponse est-elle réellement un levier d'amélioration de la cybersécurité des collectivités, ou seulement un filet de sécurité a posteriori ?

Le rôle de l'assurance cyber : une réponse financière et d'accompagnement

L'assurance cyber vise d'abord à couvrir les coûts financiers liés à une attaque : frais de reconstitution des données, perte d'exploitation, assistance technique et juridique, communication de crise.
Depuis la Loi d'Orientation et de Programmation du ministère de l'Intérieur (LOPMI), l'article L.12-10-1 du Code des assurances précise que l'indemnisation est conditionnée au dépôt d'une plainte dans un délai de 72 heures. Cette disposition, entrée en vigueur en avril 2023, a renforcé la dimension réactive de l'assurance cyber.
Certaines polices incluent aussi un volet accompagnement : mise à disposition d'experts en gestion de crise, négociation avec les attaquants, assistance à la remise en état. Pour une collectivité victime, cet appui peut être décisif.

Les limites structurelles de l'assurance cyber pour les collectivités

Malgré son intérêt, l'assurance cyber n'est pas une réponse universelle. Plusieurs limites apparaissent :
1. Le coût des primes : pour de nombreuses petites communes, les tarifs pratiqués sont inabordables. Les grandes collectivités peuvent négocier, mais les petites restent souvent exclues du marché.
2. Des conditions strictes d'éligibilité : les assureurs exigent de plus en plus la mise en place de mesures préventives (PCA, PRA, audit, segmentation réseau). Une collectivité qui n'a pas atteint un certain niveau de maturité cyber ne sera pas assurable ou verra sa couverture très limitée.
En pratique, l'assurance ne bénéficie donc pleinement qu'aux collectivités disposant déjà d'une gouvernance numérique structurée.

Une solution adaptée aux grandes collectivités, mais moins aux petites

La taille et les moyens financiers conditionnent directement l'accès à l'assurance cyber :
- Les grandes collectivités (régions, métropoles) disposent de directions informatiques, de budgets conséquents et de partenariats, ce qui facilite leur conformité aux exigences des assureurs. Pour elles, l'assurance peut jouer un rôle complémentaire efficace.
- Les petites communes, souvent dépourvues de DSI et de moyens dédiés, peinent à financer une couverture adaptée et à répondre aux critères de sécurité imposés.

Des solutions alternatives émergent : mutualisation intercommunale, recours aux dispositifs publics (ANSSI, Cybermalveillance.gouv.fr), ou encore le développement de mutuelles territoriales d'assurance. Ces mécanismes pourraient rendre l'assurance plus accessible et équitable.

L'assurance cyber représente une réponse précieuse, mais elle ne constitue pas en elle-même une politique de cybersécurité. Elle intervient après coup, une fois l'attaque réalisée, et ne saurait remplacer l'effort de mise en conformité exigé par le droit européen et national. Pour les collectivités locales, surtout les plus petites, la priorité doit rester la prévention et la gouvernance numérique. L'assurance, quant à elle, doit être envisagée comme un complément, particulièrement pertinent pour les grandes collectivités, mais encore peu adaptée aux petites structures.

Le défi des prochaines années sera donc de faire évoluer ce marché, avec l'appui des pouvoirs publics, afin que l'assurance contribue réellement à améliorer la résilience de l'ensemble des collectivités françaises.

Chapitre XI : 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.

www.cybermalveillance.gouv.fr/medias/2020/04/240320_ToisiemeKit_SCREEN.pdf

Par ailleurs, pour animer des ateliers de sensibilisation à la cyberbersécurité sur les usages du quotidien notamment pour les nouveaux arrivants cybermalveillance.gouv.fr propose une MalletteCyber

www.cybermalveillance.gouv.fr/tous-nos-contenus/actualites/lancement-mallette-cyber-inclusion-numerique

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, d'une durée de 1h30 à 2h, 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

Par ailleurs, l'ANSSI a réalisé un guide spécifique pour organiser sur table un exercice de gestion de crise cyber. Vous pourrez trouver tous ses éléments sur ce dernier sur le lien suivant :

https://cyber.gouv.fr/publications/organiser-un-exercice-de-gestion-de-crise-cyber

Plus globalement l'ANSSI met à disposition de nombreuses ressources sur l'anticipation et la gestion de crise cyber que vous pouvez retrouver sous ce lien :

https://cyber.gouv.fr/anticiper-et-gerer-une-crise-cyber

Pour approfondir la sécurisation de son organisation

L'ANSSI développe depuis plusieurs années de nombreuses ressources qui s'adressent 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 applicables 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

Vous trouverez de multiples services et ressources de l'ANSSI, pour certaines déjà mentionnées, sur leur site :
https://messervices.cyber.gouv.fr/

Annexe A1 : 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.

L'équipe de France des centres de réponse à incidents

Annexe A2 : les délégués régionaux de l'ANSSI des différents territoires

https://cyber.gouv.fr/delegues-territoriaux

Déroulé type d'une assistance

Déclenchement
- Collecte des éléments de symptômes remontées par la victime

Qualification et définition de la réponse
- Détermination du type d'incident rencontré par la victime
- Définition de la stratégie de réponse adaptée

Mise en œuvre de la réponse
- Assistance directe par Breizh Cyber
- Mise en relation avec des prestataires (*)
- Assistance à la judiciarisation et notification à la CNIL

Clôture
- Constatation d'un retour à la normale
- Bilan et recommandations d'améliorations de la posture de sécurité

(*) La mise en relation avec des prestataires n'est pas systématique.

Breizh Cyber

Annexe B : trames de fiches "réflexe"

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

- Fiche réflexe « consignes en cas de cyberattaque » de la MEL
- Fiche réflexe « que faire en cas de cyberattaque » pour les élus et dirigeants de collectivités réalisée 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

Si vous adhérez à la Centrale d'Achat Métropolitaine (CAM), la société XXXXX peut vous accompagner dans la réponse à un incident de sécurité : **xxxxxxxxxx@prestataire.fr**

Prévenez le service mutualisé cybersécurité et protection de la donnée : **XX XX XX XX XX**
xxxxxxxxxx@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

Nom du contact : _____

N° de téléphone : _____

Conseils, signalement 24h/24

Centre gouvernemental de veille, d'alerte et de réponse aux attaques informatiques (ANSSI/CERT-FR) www.cert.ssi.gouv.fr/contact

Conseils et assistance

Dispositif national de prévention et d'assistance aux victimes de cybermalveillance
www.cybermalveillance.gouv.fr

Notification de violation de données personnelles

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

PAP 2024_09_13

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 → 0 800 200 008 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.

Annexe H : Modalités du service SILENE

RÉPUBLIQUE FRANÇAISE
Liberté
Égalité
Fraternité

SERVICE SILENE

1. DESCRIPTION DU SERVICE

L'ANSSI met à disposition des opérateurs réglementés et de la sphère publique une capacité de cartographie de la surface d'exposition sur Internet au travers du service SILENE. Cette capacité vise à donner de la visibilité à ces opérateurs sur leur niveau d'exposition et à les accompagner par l'application progressive de mesures adéquates pour le réduire. Cette prestation s'appuie sur l'expérience et l'expertise acquises par l'Agence lors des audits et s'enrichit également, au fil du temps, de l'observation des modes opératoires utilisés par les attaquants.

Les scans réseaux effectués par l'Agence dans le cadre de ce service visent spécifiquement les ports les plus classiquement ciblés lors des campagnes de cyberattaques.

De plus, les données échangées au niveau applicatif respectent les standards établis sans jamais essayer de contourner les protocoles définis. Les requêtes effectuées dans le cadre de ce service sont similaires à celles auxquelles vos équipements sont régulièrement exposés sur Internet.

Le service SILENE est pensé à la fois pour les chaînes SSI et les équipes d'exploitation. Pour les premières, l'application fournit une vision globale et synthétique à travers des tableaux de bord et indicateurs associés ; pour les secondes, elle détaille les recommandations à appliquer et accompagne les opérateurs dans le pilotage de leurs équipes techniques ou de leurs prestataires.

2. MODALITÉS D'ACCÈS AU SERVICE

Pour bénéficier du service, la procédure à suivre est la suivante :

1	Faire la demande de création d'un compte nominatif en lançant la procédure d'inscription sur https://club.ssi.gouv.fr
2	Connectez-vous sur le portail Club SSI.
3	Déclarez adresses IP publiques et noms de domaine sous votre responsabilité dans l'onglet « Services d'audits automatisés > SILENE » en cliquant sur le bouton « Nouveau périmètre »
4	Vous recevrez mensuellement un rapport pour chaque périmètre déclaré à partir du début du mois suivant votre demande.

Dès réception des adresses IP et des noms de domaine, l'ANSSI partagera périodiquement les résultats de la cartographie avec les bénéficiaires du service, sous forme d'un rapport détaillé présentant les différents points de contrôle qui ont révélé des défauts de configuration pouvant entraîner des risques de sécurité.

3. UNE APPROCHE LUDIQUE ET PERSONNALISÉE

Le rapport SILENE développe un certain nombre de points de contrôle et met en évidence des déviances ou des mauvaises pratiques qui pourraient permettre à un attaquant de prendre pied sur le système d'information.

Les résultats sont mis à disposition au travers d'une interface web qui détaille et classe les vulnérabilités et recommandations afférentes. Lors de chaque audit, le niveau de sécurité des services exposés sur Internet est traduit par un niveau qui se situe sur une échelle de 1 à 5. Le niveau obtenu dépend de la gravité des vulnérabilités trouvées, le niveau 1 étant synonyme de défauts critiques, le niveau 3 d'une sécurité non dégradée (installation de services légitimes, sans durcissement particulier) et le niveau 5 d'un niveau de sécurité à l'état de l'art.

Un niveau donne ainsi accès à une liste de recommandations adaptées. L'administrateur réseau peut alors démontrer de manière objective et factuelle que les actions menées améliorent significativement le niveau de sécurité des services exposés sur Internet, et par conséquent la difficulté pour des acteurs malveillants de pouvoir accéder au SI de l'organisation. L'application de l'ensemble des recommandations portant sur les points importants d'un niveau permet de passer au niveau supérieur et d'accéder à une liste complémentaire de recommandations.

DES QUESTIONS SUR LE SERVICE ?
Consultez la FAQ accessible sur **https://club.ssi.gouv.fr/#/faq**
ou contactez-nous par email à **club@ssi.gouv.fr**

4. EN SAVOIR PLUS

CONNAÎTRE L'EXPOSITION DE SES SERVICES SUR INTERNET

Il est indispensable de bien maîtriser son exposition sur Internet, et de conserver une visibilité sur cet aspect fondamental de la sécurité d'un système d'information dans la durée. En effet, les services exposés sur Internet peuvent être exploités par des acteurs malveillants ou par des robots. Ils permettent alors parfois simplement de recueillir des données techniques sur l'infrastructure d'une organisation mais peuvent également constituer un point d'entrée dans le cadre d'une compromission d'un système d'information.

De mauvaises pratiques, des erreurs de configuration des équipements filtrants ou encore des oublis d'anciens services obsolètes ont souvent comme résultat l'exposition d'interfaces d'administration ou de services internes qui sont autant de points d'entrée dans le système d'information.

Pour un niveau donné, le rapport détaille trois catégories d'indications :

- **Des problèmes importants :** vulnérabilités critiques qui devront être corrigées pour passer au niveau supérieur ;
- **Des points d'attention :** vulnérabilités logicielles potentielles faisant l'objet d'une attention prioritaire par l'Agence, services exposés sur les ports hauts ;
- **Des points d'information :** informations sur certains points-clé. Par exemple, sont ou seront indiqués :
  - L'ensemble des services exposés ;
  - L'ensemble des services exceptés les services classiques (par exemple : web, mail, etc) ;
  - L'ensemble des services web, mail et de de téléphonie ;
  - L'ensemble des services d'administration ;
  - L'ensemble des fichiers partagés sans authentification.

	Détails des niveaux
1	Compromission instantanée possible ;
2	Exposition de services internes qui peuvent affaiblir le niveau de sécurité du SI, ou mettre en danger l'intégrité des données ;
3	Services inconnus, ou configuration non optimale de services exposés ;
4	Services sur des ports non standards ;
5	Aucun problème relevé.

L'ambition de l'ANSSI est d'accompagner progressivement les opérateurs vers une exposition réseau aussi limitée que possible grâce à l'application de recommandations adéquates et dans une approche ludique.

Ainsi, les opérateurs sont en capacité de définir un plan d'action en fonction de la sévérité des vulnérabilités identifiées tout en prenant en compte les exigences de leurs activités.

Annexe I : Modalités du service ADS

RÉPUBLIQUE FRANÇAISE
Liberté
Égalité
Fraternité

ANSSI

SERVICE ADS

1. DESCRIPTION DU SERVICE

L'ANSSI met à disposition des opérateurs réglementés et de la sphère publique une capacité d'audit des annuaires *Active Directory* (et Samba) au travers du service ADS (*Active Directory Security*).

Cette capacité vise à donner de la visibilité aux opérateurs réglementés et de la sphère publique (ministères, Opérateurs d'Importance Vitale, Opérateurs de Service Essentiel, collectivités territoriales, etc.) sur le niveau de sécurité de leur annuaire et à les accompagner dans son durcissement par l'application progressive de mesures adéquates. Cette prestation s'appuie sur l'expérience et l'expertise de l'agence sur les sujets d'*Active Directory* (AD) et s'est enrichie par sa participation aux différentes opérations de cyberdéfense.

Le service ADS permet ainsi à la fois de quantifier le niveau de sécurité de l'annuaire et d'accompagner progressivement les bénéficiaires vers un niveau de sécurité à l'état de l'art. Cette capacité est pensée à la fois pour les chaînes SSI et les équipes d'exploitation. Pour les premières, l'application fournit une vision globale et synthétique à travers des tableaux de bord et indicateurs associés ; pour les secondes, elle détaille les recommandations à appliquer et accompagne les bénéficiaires dans le pilotage de leurs équipes techniques ou de leurs prestataires.

À ce jour l'ANSSI constate une nette amélioration du niveau de sécurité des annuaires des bénéficiaires ayant souscrit à ADS dans la mesure où ce service permet un suivi régulier et continu du niveau de sécurité tout en contrôlant la bonne application dans le temps des recommandations.

2. MODALITÉS D'ACCÈS AU SERVICE

Pour bénéficier du service, la procédure à suivre est la suivante :

1	Faire la demande de création d'un compte nominatif en lançant la procédure d'inscription sur **https://club.ssi.gouv.fr/** ;
2	Télécharger la dernière version de l'outil de collecte ORADAD (Outil de Récupération Automatique de Données de l'Active Directory) sur GitHub **[https://github.com/ANSSI-FR/ORADAD/releases]** ;
3	Extraire les fichiers exécutables (exécutable ORADAD.exe et fichier de configuration) ;
4	Ouvrir un terminal et exécuter l'outil avec un compte du domaine et depuis un poste membre du domaine. Le fichier de configuration doit être positionné dans le dossier contenant l'exécutable ORADAD.exe [commande à lancer : ORADAD.exe]. Le compte utilisé n'a pas besoin de privilèges spécifiques ;
5	Connectez-vous sur le portail Club SSI ;
6	Téléverser les résultats sur le portail Club SSI, dans l'onglet « Services d'audits automatisés > ADS » : **https://club.ssi.gouv.fr/#/audit/ads**

Dès réception des fichiers de collecte, l'ANSSI lancera les analyses et en partagera les résultats avec le bénéficiaire dans un délai de 15 jours, sous forme d'un rapport détaillé présentant les différents points de contrôle qui ont révélé des défauts de configuration pouvant entrainer des risques de sécurité.

DES QUESTIONS SUR LE SERVICE ?
Consultez la FAQ accessible sur **https://club.ssi.gouv.fr/#/faq**
ou contactez-nous par email à **club@ssi.gouv.fr**

3. UNE APPROCHE LUDIQUE ET PERSONNALISÉE

Les résultats sont rendus disponibles depuis une interface web qui détaille et classe les vulnérabilités et recommandations afférentes. Lors de chaque audit, le niveau de sécurité de la configuration de l'*Active Directory* est traduit par un niveau qui se situe sur une échelle de 1 à 5. Le niveau obtenu dépend de la gravité des vulnérabilités trouvées, le niveau 1 étant synonyme de défauts critiques et le niveau 5 d'un niveau à l'état de l'art.

Un niveau donne ainsi accès à une liste de recommandations adaptées. L'évolution relative à chaque niveau est quantifiée par un score et représentée sur l'interface graphique par une barre de progression. Même si elle ne permet pas toujours d'accéder aux vulnérabilités et recommandations du niveau suivant, la correction progressive des vulnérabilités à un niveau donné, se traduit néanmoins par l'obtention de points. L'administrateur peut ainsi justifier de manière objective et factuelle que les actions menées améliorent significativement le niveau de sécurité de l'*AD* et donc du SI. L'application de l'ensemble des recommandations portant sur les points importants d'un niveau permet de passer au niveau supérieur et d'accéder à une collection complémentaire de recommandations.

Pour un échelon donné, l'application détaille trois niveaux d'indications :

- Des problèmes importants : vulnérabilités critiques ordonnées qui devront être corrigées pour passer au niveau supérieur ;
- Des points d'attention : mauvaises pratiques manifestes du point de vue de la sécurité, mais non prioritaires au vu des autres vulnérabilités identifiées à ce niveau ;
- Des points d'information : informations sur certains points-clé de l'AD.

	Les niveaux sont échelonnés de la façon suivante :
1	L'annuaire Active Directory présente des problèmes critiques de configuration qui mettent en danger immédiat l'ensemble des ressources hébergées. Des actions correctrices sont à prendre dans les plus brefs délais ;
2	L'annuaire Active Directory présente des lacunes de configuration et de gestion suffisantes pour mettre en danger l'ensemble des ressources hébergées. Des actions correctrices sont à prendre à court terme ;
3	L'annuaire Active Directory possède un niveau de sécurité basique non affaibli depuis son installation ;
4	L'annuaire Active Directory dispose d'un bon niveau de sécurité ;
5	L'annuaire Active Directory dispose d'un niveau de sécurité à l'état de l'art.

Par conséquent, l'enjeu devient majeur pour les opérateurs réglementés et sphère publique de mettre en place et de maintenir un niveau de sécurité satisfaisant de leurs annuaires. Ainsi, l'ambition de l'ANSSI est d'accompagner progressivement vers un niveau de sécurité à l'état de l'art grâce à l'application de recommandations adéquates et dans une approche plus ludique.

4. EN SAVOIR PLUS

L'annuaire Active Directory, centre névralgique de la sécurité des systèmes d'information Microsoft

L'annuaire *Active Directory* (*AD*) est un élément critique permettant la gestion centralisée de l'ensemble des permissions sur les différents domaines qui composent un système d'information (SI) Microsoft. L'obtention de privilèges élevés sur l'AD entraîne par conséquent une prise de contrôle instantanée et complète de tout le SI.

Le faible niveau de sécurité des annuaires met en danger les systèmes d'information

Les prestations d'audit effectuées par l'ANSSI auprès de ses bénéficiaires font apparaître un manque de maturité critique et récurrent sur la sécurité des annuaires *Active Directory*. Ce défaut de sécurité affaiblit significativement le niveau global de sécurité de ces SI. Ce constat est renforcé par la connaissance acquise au contact des différents réseaux compromis sur lesquels l'agence est intervenue lors d'opérations de cyberdéfense. Au-delà du manque de maturité, l'agence note par ailleurs que le niveau de sécurité des annuaires *Active Directory* décroît en fonction du temps et du cycle de vie du SI.

Développement d'une capacité spécifique et ouverture d'un service

Au sein de l'agence, les prestations d'audit sur un système d'information donnent habituellement lieu à la rédaction d'un rapport détaillé, répertoriant à un temps les vulnérabilités qui touchent le système d'information, les recommandations correspondantes et la priorité de leur déploiement. Ces rapports, souvent volumineux, ne permettent pas toujours de prioriser avec aisance les actions à mener. Par ailleurs, si un audit évalue le niveau de sécurité à un instant donné, il ne mesure pas dans la durée l'évolution du niveau de sécurité.

Face à ce constat, l'ANSSI a développé une nouvelle capacité dont l'objectif est d'auditer, à la demande du bénéficiaire et de manière autonome, le niveau de sécurité des annuaires *Active Directory* des opérateurs stratégiques de l'État.

Annexe J

1. Objectifs de sécurité et mesures de réduction des risques

Vous trouverez dans le tableau ci-dessous des éléments qui pourrons vous orienter dans le choix des éléments et mesures à mettre en œuvre, par ordre de priorité :§ idem 5

Outil / Mesure	Objectifs de sécurité	Risques
Sauvegarde	Protection des données Continuité et Reprise d'activité	Chiffrement ou altération des données Perte de données Arrêt/disfonctionnement de l'activité
Antivirus	Protection contre les fichiers malveillants sur les postes et serveurs	Logiciel malveillants (Rançongiciel, …) Fuite/vol de données
Antispam	Filtrage des mails malveillants, Filtrage des fichiers malveillants,	Hameçonnage, Logiciels malveillants
Proxy	Filtrage des sites malveillants ou inadaptés, Filtrage des fichiers malveillants, Traçabilité des accès internet	Logiciels malveillants Fuite de données Conformité règlementaire, traçabilité
Parefeu	Contrôle des accès et des flux de données Segmentation du S.I. Zones de sécurité filtrée : zones utilisateurs, zones serveurs, zones DMZ	Intrusion dans le S.I Fuite de données Propagation, latéralisation de l'attaque Non maitrise des flux de données
Annuaire	Centralisation des comptes utilisateurs Gestion des droits des utilisateurs et des groupes Séparation des droits utilisateurs et administrateurs	Mauvaise Gestion et revue des comptes, Mauvaise gestion des droits utilisateurs, Accès illégitime Logiciels malveillants Défaut de confidentialité de données
Supervision	Informations sur le fonctionnement des équipements et applications Traitement des incidents et alertes	Détection tardive ou non traitement des incidents ou des disfonctionnements.

Outil / Mesure	Objectifs de sécurité	Risques
Charte Informatique	Responsabilisation des utilisateurs Droits et devoir d'utilisation du S.I	Mauvais usages des outils numériques, Shadow IT, respect des réglementations et de la Politique interne
Sensibilisation	Amélioration des pratiques et des usages des outils numériques Renforcement de la culture et des connaissances cyber	Hameçonnage, Ingénierie sociale, Erreur de manipulation, Mauvais usages des outils numériques, Non-Conformité règlementaire
RSSI / DPO	Pilotage et suivi de la sécurité Analyse de risques PSSI, Gestion de crise Conformité réglementaire	Défaut de sécurisation Absence de pilotage et de suivi Non-conformité règlementaire
VPN	Chiffrement des accès distants et interconnections réseaux (partenaires) Sécurisation des utilisateurs nomades	Fuite de données Logiciels malveillants Expositions des applications
Puits de logs	Traçabilité des accès Traçabilité des actions Surveillance des évènements	Perte ou suppression des traces d'activités malveillantes ou règlementaires.
Reverse proxy	Contrôler et sécuriser l'exposition internet d'applications	Exposition directe d'application Compromission, accès non maitrisés
Bastion	Contrôle des accès distants Contrôle des prestataires Contrôles des administrateurs Traçabilité des actions	Accès distant non autorisé Détournement d'accès
EDR / xDR	Protection contre les fichiers et actions malveillantes sur les postes et serveurs Surveillance des évènements	Logiciel malveillants (Rançongiciel, …) Fuite/vol de données
Passerelle API	Filtrage et Contrôle des appels d'API entrants et sortant vers les services externes (Cloud, SaaS, partenaires, hébergeurs, …)	Détournement d'API Vol, extraction de données Non maitrise des flux API entrants/sortants

2. Produits et services qualifiés et certifiées

L'ANSSI recommande l'utilisation de produits et services qualifié aussi souvent que possible. Vous trouverez sur le site cyber.gouv.fr, un certain nombre de services, outils et prestataires ayant obtenu une attestation ou certification de sécurité.

PACS : Prestataires d'accompagnement et de conseil en sécurité des systèmes d'information
https://cyber.gouv.fr/prestataires-daccompagnement-et-de-conseil-en-securite-des-systemes-dinformation-pacs

SECNUMCLOUD : Prestataires de Services Informatique en nuage
https://cyber.gouv.fr/prestataires-de-services-dinformatique-en-nuage-secnumcloud

PRIS : Prestataires de Réponse aux Incidents de Sécurité
https://cyber.gouv.fr/prestataires-de-reponse-aux-incidents-de-securite-pris

PAMS : Prestataires d'administration et de maintenance sécurisées
https://cyber.gouv.fr/prestataires-dadministration-et-de-maintenance-securisees-pams

PDIS : Prestataires de Détection des Incidents de Sécurité
https://cyber.gouv.fr/prestataires-de-detection-dincidents-de-securite-pdis

Vous pourrez également accéder aux listes des produits et services qualifiés par l'**ANSSI**
https://cyber.gouv.fr/produits-services-qualifies

Catalogue des produits et services qualifiés, agréés certifiés :
https://cyber.gouv.fr/decouvrir-les-solutions-qualifiees

Liste des solutions certifiées :
https://cyber.gouv.fr/decouvrir-les-solutions-certifiees

PÔLE D'EXCELLENCE
CYBER

www.pole-excellence-cyber.org