GMF
ASSURÉMENT HUMAIN

Cybercriminalité : prévenir, gérer, guérir

les bonnes pratiques

L'EXPERTISE WEKA

WEKA .media .jobs .fr

Sommaire

LE MOT DE L'ÉDITEUR

L'actualité de mars 2024 en France a été marquée par des cyberattaques contre plusieurs ministères, revendiquées par différents groupes de hackers réputés pro-russes, si bien qu'une proposition de loi visant à lutter contre les ingérences étrangères est débattue à l'Assemblée Nationale. Ce n'est, à la faveur d'un climat géopolitique détérioré, que la dernière manifestation d'une menace cyber en forte hausse en 2023, selon l'étatique Groupement d'Intérêt Public Action contre la Cybermalveillance (GIP ACYMA). Fin 2022, ce dernier s'associait à l'Association des Maires de France (AMF) pour établir un guide méthodologique destiné à sensibiliser les agents des collectivités, particulièrement exposés, à la cybersécurité : l'étude révélait le défaut de formation à la cybersécurité.

Le facteur humain apparaît bien comme essentiel : « nous ne sommes pas suffisamment acculturés aux enjeux du cyber » avertit le Général Marc Watin-Augouard ; pourtant, pour Dominique Bogé, Chef d'escadron et Chef du département Prévention et protection de l'Unité Nationale Cyber de la Gendarmerie Nationale, « si tout le monde suit les gestes simples d'hygiène numérique, on supprime 70 % des menaces ».

Retrouvez dans ce Livre blanc, élaboré en partenariat avec la GMF, des conseils pratiques et opérationnels des spécialistes des questions numériques et menaces cyber pour, associés à l'expertise WEKA, une approche simple et efficace de la cybersécurité.

Julien Prévotaux
Directeur éditorial & des rédactions – WEKA

Les organisations publiques face au défi de la cybersécurité

Françoise Gatel, sénatrice d'Île-et-Vilaine, Présidente de la délégation sénatoriale aux collectivités territoriales et à la décentralisation, auteure d'un Rapport d'information au Sénat avec Serge Babary : « Les collectivités territoriales face au défi de la cybersécurité ».

Général Marc Watin-Augouard, Président chez Le Trèfle alumni EOGN, Général d'Armée de Gendarmerie (2S), ancien directeur du Centre de Recherche de l'École des Officiers de la Gendarmerie Nationale (EOGN), fondateur du FIC (Forum International de la Cybersécurité), Président de l'Institut National pour la Cybersécurité et la Résilience des Territoires.

Françoise Gatel

Général Marc Watin-Augouard

■ **WEKA :** ***Sur quel périmètre la cybersécurité doit être appréhendée ? Au niveau intercommunal, peut-être au niveau régional, voire plus, et aussi peut-être dépasser la frontière entre le public et privé ?***

Françoise Gatel : Le Sénat a voulu se saisir de ce sujet en lien avec la délégation aux entreprises puisque nous sommes intimement convaincus qu'il est nécessaire de sensibiliser les collectivités, quelles que soient leur taille, qui pensent que les cyberattaques concernent des structures de profits, donc des entreprises, et que ça ne peut pas leur arriver alors même que c'est arrivé dans les hôpitaux, même dans une station d'épuration, dans des petites collectivités, quelle que soit leur taille.

Nous avons remarqué l'augmentation du risque et des attaques ainsi que le peu de connaissances et l'insuffisante appréhension par tous les élus de ces sujets. Quand vous êtes une commune de 150 habitants, il est évident que vous n'avez ni le budget, ni les personnels qualifiés pour identifier le risque, se l'approprier et mettre en œuvre les moyens nécessaires. Donc vous avez parfaitement raison, il est absolument indispensable de travailler à une échelle de coopération qui soit efficace pour gagner du temps, avoir de l'expertise et des solutions.

Cela est d'autant plus important dans les collectivités car aujourd'hui nous avons des connexions des systèmes d'information. Souvent, à l'échelle d'une intercommunalité, vous avez un dispositif de système d'information qui est partagé par toutes les collectivités qui en sont membres, voire des syndicats. Cela signifie que le maillon faible peut être la voie d'entrée du hacker et affaiblit tout le monde. Il faut donc travailler à une échelle pertinente et je suis personnellement assez favorable à ce qu'il y ait aussi des liens entre des entreprises et des collectivités. Donc travaillons à une échelle qui va aider à contaminer positivement la prise de conscience et qui, surtout, donnera des moyens humains et aidera à résoudre les choses par des échanges de bonnes pratiques.

■ **WEKA :** ***Il y a aussi, à l'intérieur de ces organisations, une question posée au management en ce qui concerne la formation à des nouveaux métiers, des cybermétiers, qui n'existent pas dans ces petites structures.***

Général Marc Watin-Augouard : Vous avez raison, aujourd'hui, il faut vraiment travailler sur les territoires en coopération, en collaboration. Pourquoi ? Parce que toute l'histoire de notre cybersécurité en France est une histoire qui est partie du haut et qui est descendue vers le bas, mais au travers de silos très précis. C'est-à-dire que nous avons commencé à se poser la question sur les opérateurs d'importance vitale, ceux sur lesquels il faut absolument se reposer si on veut pouvoir continuer à vivre tous les jours. Les grands opérateurs sont l'énergie, l'information, la santé. Ce faisant, nous avons laissé de côté un certain nombre d'acteurs : les petites entreprises, les collectivités territoriales et les services publics locaux, en se disant finalement que ces derniers ne seront jamais atteints mais cela est faux. Il n'y a pas de périmètre : vous êtes connecté, vous serez une cible potentielle. Soit une cible directe, soit une cible indirecte.

Si on prend l'exemple d'un maire d'une commune de 1 500 habitants, comme la mienne, quand je lui parle de l'activité de sa commune et que nous faisons l'inventaire de toutes les données qui sont récoltées, c'est absolument phénoménal : le cadastre, les informations sociales, les informations concernant la cantine scolaire, la bibliothèque scolaire, la maison de santé, l'EHPAD… Toutes nos données sont aujourd'hui dans les mains des collectivités territoriales, chacune, bien sûr, n'ayant que les données qui les concernent selon les compétences exercées. Mais cela vous montre bien qu'il y a une mine extraordinaire. Or, la donnée est de l'or noir. Il s'agit de la matière première, de la richesse du 21e siècle. Et cette donnée a une valeur, on peut soit l'échanger contre une rançon ou on peut l'utiliser pour l'exploiter et tirer des enseignements sur un territoire.

Il n'y a pas de périmètre : vous êtes connecté, vous serez une cible potentielle.

Aujourd'hui, on ne peut pas accepter d'abandonner les collectivités territoriales et donc pour moi, il faut, après la verticalité de l'action sur les opérateurs les plus essentiels, s'intéresser à l'horizontalité des territoires. Qu'est-ce qu'un bon territoire ? J'aurais tendance à dire que si l'on veut une action globale, c'est le département, mais pour les collectivités territoriales, je partage complètement votre analyse, il faut passer au niveau des établissements publics de coopération intercommunale (communauté d'agglomération, métropole, etc.). Mais nous ne pouvons plus laisser les petites communes en déshérence. Pourquoi ? Parce qu'un jour elles seront, sinon visées directement, visées comme point de départ. C'est-à-dire qu'on l'attaquera pour faire un saut de puce et attaquer la commune plus importante et ainsi de suite.

Donc aujourd'hui, c'est un véritable enjeu et vous l'avez dit vous-même, il faut d'abord former les élus. Ensuite, il faut former des personnes en mesure d'apporter une aide aux collectivités territoriales. Avec une l'association pour l'enseignement numérique, nous avons créé, il y a peu de temps aux Sables d'Olonne, la première formation pour les RSSI, responsables de la sécurité des systèmes d'information des collectivités territoriales. Ce sont des jeunes à qui on va apprendre ce qu'est une collectivité territoriale, comment elle fonctionne et comment on peut la protéger.

Bien sûr, la petite commune ne pourra pas se le payer, mais une communauté d'agglomération, elle, pourra peut-être s'en payer un à temps partiel, puis la métropole et puis le département peut-être. Et ainsi, nous allons fédérer, faire en sorte que personne ne soit abandonné.

■ **WEKA :** ***Avons-nous vraiment conscience de la place que représente le facteur humain ?***

Général Marc Watin-Augouard : L'Agence nationale pour la sécurité des systèmes d'informations le dit : 85 % des problèmes qui existent sur notre espace numérique sont liés à notre propre défaillance. Et notre défaillance est liée au fait que nous ne connaissons pas, nous ne sommes pas suffisamment acculturés aux enjeux du cyber. Si déjà on forme les personnels, si on forme la secrétaire ou le secrétaire de mairie, si on forme les agents des services publics locaux en leur disant « attention, il y a un enjeu » ou « attention, il y a des actes d'hygiène informatique ». Quand vous rentrez chez vous, vous ouvrez la porte, mais quand vous sortez, vous la fermez. Si vous ne faites pas ces actes essentiels dans le monde numérique, les mêmes que vous accomplissez dans le monde réel, alors il ne faut pas s'étonner d'être cyber attaqué.

Nous ne sommes pas suffisamment acculturés aux enjeux du cyber.

ENTRETIEN

« Conscientiser, prévenir et gérer : construisons ensemble une culture du risque cyber »

Oriana Labruyère, Avocate en droit du numérique et DPO, avocate associée de La Robe Numérique, partage des conseils pour développer une culture du risque cyber, basés sur ce que Me Oriana Labruyère appelle les « bonnes pratiques cyber ».

■ **WEKA :** ***Comment se prémunir et se préparer à la mise en œuvre de la directive européenne NIS 2 ? Les obligations de résultats sont posées pour les acteurs publics territoriaux.***

Oriana Labruyère : Oui alors justement, ça c'est la grande nouveauté de NIS 2. Cette directive inclut le périmètre collectivité territoriale, en tout cas secteur public, dans le périmètre, ce qui n'est pas le cas de la première directive NIS. Les cellules de crise sont la bonne pratique à adopter parce que c'est l'obligation aussi pour le responsable légal d'avoir sa part sur le sujet. La cyber ce n'est pas qu'une question de technique, c'est aussi une question humaine. Quand on a bien formé les humains et que les outils sont là, c'est parfait, mais quand on n'a que les outils, l'erreur humaine existe toujours et elle va laisser passer l'info, il va y avoir une pénétration du système d'information, les outils ne suffisent pas. Je suis heureuse qu'on puisse parler cyber sans parler technique. On arrive bien à faire le lien avec la question sur la formation, à parler cyber, sans parler technique. Sensibiliser, oui ! Parce que lorsqu'on connaît mieux le risque, quand on est mal préparé d'un point de vue outil, on arrive à mieux réagir. Parfois on n'a pas les moyens d'acheter des outils, par contre on a les moyens de sensibiliser les gens. Il y a des outils qui ne coûtent pas cher. Sensibiliser, moi j'adore faire ça autour de chouquette ou autour d'un jeu afin d'enlever un peu la pression de ce sujet qui est quand même très anxiogène. Il ne faut pas être celui qui a mal cliqué sur un mail. Aujourd'hui, la culpabilité dans les organisations est liée au fait d'avoir cliqué à un mauvais endroit. Or il faut valoriser quand il y a des remontées, il ne faut pas cacher des choses parce qu'effectivement il

Oriana Labruyère, Avocate en droit du numérique et DPO, avocate associée de La Robe Numérique

y a la responsabilité pénale mais il y a aussi une responsabilité contractuelle. La garantie de l'intégrité et de la sécurité de la confidentialité des données, ce n'est pas que dans le RGPD, c'est aussi dans les contrats que vous avez vis-à-vis de vos clients, et ce que vous attendez de vos prestataires. Dire que j'ai une faille, mais que je l'assume, que je suis en responsabilité, que je déploie ce qu'il faut, etc., c'est aussi ne pas commettre une faute dans le cadre de l'exécution de contrats. L'obligation de sécurité aujourd'hui, c'est une obligation de sécurité mais aussi une obligation technique et une obligation juridique qui se matérialise aujourd'hui dans les contrats, dans le cadre légal, on ne peut plus l'ignorer.

■ **WEKA :** ***Comment peut-on se préparer en cas d'extraction non voulue, intentionnel ou accidentel des données ?***

Oriana Labruyère : Il faut faire une étude de cas de son système d'information, faire une cartographie. Même si cela n'est pas parfait ou exhaustif, ce n'est pas grave, on peut commencer avec ce qu'on a. On pourra élaborer des raisonnements sur les informations dont nous disposons et cela fera ressortir des alertes. Isoler la data, c'est selon moi quelque chose d'extrêmement important et dans le cas du risque d'extraction on voit bien que lorsqu'on a une data qui part en fonction de sa sensibilité, et là je ne veux pas parler du RGPD, je veux parler de sensibilité de l'information au regard de l'organisation. Avant de parler du RGPD, il faut déjà se poser la question d'où est-ce qu'on a mal si on appuie ici ou là ? Est-ce que l'organisation va pouvoir résister en cas d'extraction de cette base de données ? Est-ce qu'elle va pouvoir résister en cas d'extraction d'une autre ? Est-ce qu'elles sont imbriquées. Si c'est imbriqué, est-ce que c'est indispensable ? Et la plupart du temps, et j'en ai bien conscience, il y a une dépendance technologique qui est un coût, un coût financier lorsqu'on veut en changer mais qui est aussi un coût humain, parce que changer les habitudes, c'est ce qui a de plus compliqué. Mais connaître la faille, savoir que là on a un risque, ça permet simplement peut-être de réorienter la stratégie de gestion sur un axe précis parce qu'on sait qu'on ne peut pas faire les investissements. Il faut se demander alors comment je fais pour augmenter le niveau de sécurité de cette zone-là ? Le reste ça attendra, mais cette zone là c'est vraiment essentiel et ensuite se poser la question de comment je vais continuer à discuter avec ma direction. Aujourd'hui y a des outils qui permettent de d'échanger en étant en vase clos et qui permet de garantir la sécurité, il existe notamment des français. Il faut vraiment regarder ces outils qui sont pas des investissements lourds mais qui permettent de garantir un fil sécurisé pour se parler, se donner des documents, parler avec les avocats, parler avec la communication, parler avec le forensic et donc on ne va pas transmettre des informations à des tiers sans les maîtriser.

La cyber ce n'est pas qu'une question de technique.

Sur NIS 2 on attend une loi de transposition parce que ce n'est qu'une directive. C'est une réglementation qui vraiment implique les collectivités territoriales maintenant, dans le périmètre de l'obligation de de garantir la sécurité, c'est-à-dire que là on a une réglementation qui vient alourdir l'obligation. Pourquoi ? Parce que la maturité des acteurs économiques et sociaux aujourd'hui ne peut plus être laissé, entre guillemets, de côté. On a eu un déploiement massif de la solution numérique aujourd'hui, mais que fait-on si on n'a plus rien, qu'est-ce qu'on a ? On a le système D, il faut se poser la question de l'équivalent d'un plan blanc, c'est-à-dire comment je fais avec du zéro numérique dans ma commune, sans ma collectivité, est-ce que j'ai au moins des services que je juge essentiels à la population que je peux maintenir ? Est-ce que j'ai un ordi qui est off de tout réseau sur lequel il y a quand même un certain nombre d'éléments d'applications métiers que je vais pouvoir activer pour avoir quand même quelques services ? Ce sont des questions qui rentrent dans le périmètre NIS 2. Il y a des webinaires de l'ANSSI sur NIS 2 très intéressants et notamment sur le changement de positionnement de l'ANSSI puisqu'ils vont devoir rentrer dans une logique un peu différente d'aujourd'hui.

■ **WEKA :** ***Est-ce qu'il existe des formations aujourd'hui sur ces enjeux ?***

Oriana Labruyère : Oui il existe beaucoup de formations cyber. La difficulté c'est d'avoir une formation qui est adaptée aux acteurs qui sont en formation parce que les niveaux de maturité ne sont pas du tout le même. Rendre fort plutôt que rendre sensible, former des agents qui sont par exemple à l'accueil, qui sont en contact direct avec le public, et former des techniciens, c'est autre chose. Il faudrait inclure dans la prise de poste ces questions-là. Une sensibilisation, pas à la cyber en général, mais à la cyber chez vous, à la cyber sur son poste, aux procédures en interne. Il faut savoir qui prévenir si jamais il y a un incident, ça c'est important.

La difficulté c'est d'avoir une formation qui est adaptée aux acteurs.

Cybersécurité : une méthode clé en main pour sensibiliser les agents des collectivités

L'AMF s'est associée à Cybermalveillance.gouv.fr pour éditer un guide méthodologique destiné à sensibiliser les agents des collectivités à la cybersécurité.

À l'occasion du 104e Congrès des maires et des présidents d'intercommunalités de France, Cybermalveillance.gouv.fr, dispositif national d'assistance aux victimes d'actes de cybermalveillance, et l'AMF ont dévoilé, le 18 novembre 2022, une méthode « clé en main » destinée à sensibiliser les agents des collectivités aux enjeux de la cybersécurité. Ce guide méthodologique de 16 pages s'adresse à toutes les collectivités territoriales, sans exception, très exposées et néanmoins peu conscientes du risque encouru. En effet, le risque cyber est omniprésent – Cybermalveillance.gouv.fr a enregistré une augmentation de près de 70 % de demande d'assistance en ligne en 2021 – et les collectivités ne peuvent pas y échapper.

Une étude réalisée au cours du second semestre 2021 par Cybermalveillance.gouv.fr auprès des collectivités de moins de 3 500 habitants a mis en exergue leur faible préparation aux cyberattaques. Au-delà d'un manque de connaissance et d'information sur le sujet pour plus des deux tiers des publics concernés (maires, adjoints, DGS et agents), l'étude a révélé le défaut de formation à la cybersécurité des responsables ou des prestataires informatiques des collectivités. Ces résultats prouvent que les collectivités territoriales constituent une cible particulièrement vulnérable.

Cybermalveillance.gouv.fr et l'AMF ont donc élaboré une méthode clé en main pour sensibiliser et responsabiliser tous les agents. « On le sait

aujourd'hui, de nombreuses attaques ciblent l'humain. Un utilisateur averti permet de réduire considérablement les risques et contribue même à élever le niveau de sécurité collectif, d'où la nécessité d'impliquer toute la collectivité dans cette démarche, du stagiaire à l'élu en passant par les agents », insistent les rédacteurs du guide. Fort de ces constats, Cybermalveillance.gouv.fr et l'AMF ont conçu un dispositif composé, à la fois, d'une approche théorique et d'un plan d'action facile à mettre en œuvre, accompagnés d'un ensemble d'outils et de contenus pédagogiques. Ainsi, la méthode clé en main s'adresse à l'ensemble des collectivités qui initient une démarche de sensibilisation. « Présentée dans son intégralité, elle est une illustration idéale d'un programme de sensibilisation global. Sa mise en œuvre dépendra de la priorité donnée au risque cyber, de la disponibilité et des ressources à y dédier », soutiennent ses concepteurs.

Cette méthodologie se veut une « boîte à outils cyber », modulable et personnalisable. Elle détaille « 5 clés pour une sensibilisation réussie ». Au programme :

- Clé n° 1 : Prendre conscience du risque cyber
- Clé n° 2 : Impliquer les publics des collectivités
- Clé n° 3 : S'appuyer sur les bonnes ressources pédagogiques
- Clé n° 4 : Décliner et répéter les messages
- Clé n° 5 : Vérifier l'assimilation des messages

Traduction pratique, le guide propose ensuite un exemple de programme de sensibilisation des agents, en trois actes.

« Les agents des collectivités constituent le premier maillon de la chaîne de sécurité face au risque cyber dans nos communes. Faire face aux crises, c'est s'y préparer et toutes les actions présentées dans ce guide sont autant de clés permettant d'augmenter l'immunité de nos collectivités », explique le président de l'AMF David Lisnard. « De nombreuses attaques pourraient être évitées avec une sensibilisation aux risques numériques efficace et un apprentissage des bonnes pratiques au quotidien. Au travers de cette méthode « clé en main » coéditée avec l'AMF, nous avons voulu doter les collectivités des clés nécessaires pour appréhender le sujet, préparer, former et responsabiliser les agents face aux enjeux de la cyber et en faire de véritables partenaires de la sécurité de leur collectivité », complète Jérôme Notin, directeur général du GIP ACYMA, la structure qui pilote le dispositif national Cybermalveillance.gouv.fr.

CONSEILS DE CHRISTINE BERTRAND

Christine Bertrand, Directrice des systèmes d'information et numérique - Direction générale adjointe de l'administration et des ressources du Département de Seine-et-Marne.

■ **WEKA :** ***Quels sont vos conseils préventifs pour d'autres collectivités ?***

Christine Bertrand : La première des choses est de se poser la bonne question : il ne s'agit pas de se demander « est-ce qu'on sera attaqué ? » mais plutôt « quand ? ». Tout le monde peut potentiellement être attaqué. Il faut préparer en amont son plan de continuité et son plan de gestion de crise pour savoir quoi faire le jour où on sera attaqué.

Deuxième chose, il faut sécuriser son système d'information en privilégiant là aussi une sécurité avec des couches successives, avec des segmentations de zones, qui limitent les effets de l'attaque en empêchant la propagation.
Ensuite, il faut sensibiliser les agents à tout ce qui est phishing et usurpation d'identité.
La plupart des attaques commencent toujours par une usurpation d'identité d'un compte lambda. Enfin, il faut choisir sa sauvegarde en prévoyant une sauvegarde offline, à l'abri des attaques. La sauvegarde, c'est le dernier recours lors d'une cyberattaque.

Fiche 12806

Appréhender les obligations du RGPD en matière de données RH

CONTEXTE

Le règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016, dit règlement général sur la protection des données (RGPD), entré en vigueur le 25 mai 2018, accroît sensiblement les obligations pesant sur les collectivités en matière de traitement des données personnelles.

Les ressources humaines sont directement impactées par le RGPD dont la logique est quadruple : **simplification, transparence, sécurisation des données et responsabilisation des acteurs**.

Dans le cadre de ses missions, la direction des ressources humaines est amenée à traiter un grand nombre de données personnelles. Comment définir un traitement de données RH ? Quelles sont les procédures à mettre en œuvre pour respecter le RGPD ?

▶ 1 - Identifier et cartographier les données personnelles gérées en matière de ressources humaines

Le RGPD réaffirme les principes essentiels de la protection de la vie privée et notamment la minimisation et l'exactitude des données, la restriction d'utilisation, la limitation du stockage, la confidentialité.

Le RGPD a accordé de nouveaux droits aux agents publics : accéder à leurs données, en obtenir une copie, les rectifier, s'opposer à leur utilisation et le droit à l'oubli.

Le règlement a également introduit un droit à réparation du préjudice subi pour toute personne ayant subi un dommage matériel ou moral du fait de l'utilisation de ses données personnelles.

Les collectivités doivent disposer d'un registre précis des fichiers détenus par les services de la collectivité, les informations qu'ils détiennent sur leurs agents, leur usage, leur localisation exacte et les personnes qui peuvent y accéder.

La plupart des données nécessaires à la gestion des ressources humaines, par exemple le nom de l'agent, son numéro de téléphone, son numéro de Sécurité sociale, son adresse, ses coordonnées bancaires mais aussi son CV, sa photographie, ses documents d'identité…, peuvent être considérées comme personnelles.

Le traitement de données personnelles en matière de gestion des ressources humaines est effectué dans les domaines suivants :

Recrutement :

- Gestion des dossiers de candidatures et des CVthèques.
- Organisation d'entretiens ou de tests de recrutement.
- Organisation de concours et gestion de listes d'aptitude.

Gestion administrative des agents :

- Tenue du dossier individuel par la collectivité ou l'établissement mais également le centre de gestion si la collectivité ou l'établissement est affilié.
- Réalisation d'études statistiques ou de listes d'agents.
- Gestion des annuaires, des organigrammes.
- Gestion des dotations en fournitures, équipements, etc.
- Organisation des élections professionnelles.
- Secrétariat des réunions des organismes paritaires ou des instances médicales.

Mise à disposition d'outils informatiques aux personnels :

- Gestion des listes informatiques permettant de définir les autorisations d'accès aux applications et au réseau.
- Gestion de la messagerie électronique professionnelle.

Gestion des carrières :

- Gestion des avancements et promotions.
- Secrétariat des réunions des organismes paritaires ou des instances médicales.
- Évaluation professionnelle des agents.
- Validation des acquis de l'expérience professionnelle.
- Gestion des fiches de poste.
- Gestion de la mobilité professionnelle.
- Suivi des demandes de formation et des périodes de formation effectuées.
- Organisation des sessions de formation.
- Suivi des procédures disciplinaires et des sanctions.
- Gestion des arrêts maladie, des déclarations d'accident de service ou de maladie professionnelle, des dossiers d'inaptitude.
- Gestion des dossiers de retraite.
- Gestion de l'assurance chômage.

Conditions de travail :

- Gestion des horaires, des cycles de travail, des heures supplémentaires, des astreintes, des permanences, des agendas et des feuilles de temps.
- Gestion des demandes de congés et d'autorisations d'absence.
- Gestion des rémunérations.
- Médecine du travail.
- Service social d'assistance ou de soutien psychologique.
- Gestion de l'assurance statutaire.
- Action sociale.
- Protection sociale complémentaire.
- Évaluation des risques professionnels…

Le RGPD impose que l'employeur prenne toutes les mesures propres à garantir la sécurité des données personnelles de ses agents.

Pour la mise en œuvre de cette obligation de garantie, le RGPD introduit une obligation de tenir un **registre des traitements** (RGCP, art. 30).

L'article 35 du RGPD impose en outre d'effectuer une **étude d'impact** relative à la protection des données « *lorsqu'un type de traitement est susceptible d'engendrer un risque élevé pour les droits et libertés des personnes physiques* ».

Même en l'absence d'obligation de tenue d'un registre des traitements, il est nécessaire de cartographier les différents traitements de données RH afin d'identifier les risques et les mesures à mettre en place mais également de répondre aux sollicitations d'accès ou de rectification de données pouvant être formulées par les agents.

Par ailleurs, ce recensement doit permettre à la collectivité de se mettre en conformité avec le RGPD mais également de garantir l'exercice des nouveaux droits dont les agents publics disposent, la responsabilité de la collectivité pouvant éventuellement être engagée si un préjudice moral peut être démontré par l'agent.

La méthodologie d'élaboration de la **cartographie** repose sur deux préalables :

- le recueil des données déjà identifiées dans les systèmes d'information ;
- et la mise en place de questionnaires auprès des responsables de service afin d'identifier les fichiers et les traitements réalisés.

▶ 2 - Minimiser et sécuriser les données RH

Pour les traitements RH, notamment à l'occasion des recrutements, l'employeur ne peut collecter que les données adéquates, pertinentes et strictement nécessaires à la finalité du traitement.

Exemple : demander à un candidat son numéro de Sécurité sociale dès la phase de l'entretien de recrutement paraît inadéquat car sans rapport avec la capacité à occuper le poste proposé.

La finalité recouvre la raison par laquelle les données sont collectées mais également leur utilisation.

Si un responsable des ressources humaines peut faire parvenir du matériel de vote à des agents en cas de vote par correspondance aux élections professionnelles, le fichier ne pourra pas être utilisé par le maire pour l'envoi d'un bulletin municipal.

La question de la conservation de certains documents se pose pendant toute la carrière de l'agent. Par exemple, les CV de candidats non retenus ne peuvent être conservés indéfiniment.

La direction des ressources humaines doit s'assurer qu'une politique de sécurisation et de durée de conservation des données a bien été définie et que les données sont supprimées une fois que l'objectif poursuivi est atteint.

Les supports sur lesquels sont stockées les données personnelles des agents doivent être sécurisés. S'agissant des dossiers individuels des agents, ils doivent être conservés dans des armoires fermées à clé ou dans des dossiers informatiques protégés, afin de garantir leur confidentialité. Il en est de même des comptes rendus d'évaluation professionnelle. Une procédure doit être mise en place s'agissant des personnes pouvant avoir accès à ces informations comme les responsables de service ou les supérieurs hiérarchiques.

Les mesures de sécurisation peuvent être organisationnelles et techniques (sensibilisation des agents, mise en place d'une charte, anonymisation des données, cryptage…).

▶ 3 - Informer et recueillir le consentement des agents

Lors de la collecte de données, les candidats et agents doivent être informés, notamment, sur :

- l'identité et les coordonnées du responsable du traitement et du délégué à la protection des données (DPD) ;
- le fondement juridique et les finalités du traitement ;
- les destinataires des données ;
- la durée de conservation des données ou les critères utilisés pour déterminer cette durée ;
- l'existence du droit de demander l'accès aux données, la limitation, la portabilité, la rectification ou l'effacement de celles-ci ;
- le droit d'introduire une réclamation auprès de l'autorité de contrôle, à savoir la Commission nationale de l'informatique et des libertés (Cnil) (RGPD, art. 5).

Les agents doivent être également informés des mentions suivantes :

- l'intention d'effectuer un traitement ultérieur des données à d'autres fins ;
- si les données n'ont pas été collectées auprès de la personne concernée : leur source et, le cas échéant, une mention indiquant qu'elles sont issues ou non de sources accessibles au public…

Cette information doit apparaître de façon claire et précise sur les supports tels que les formulaires de candidature, les comptes rendus d'évaluation, les dossiers pour transmission à l'assureur, à la CNRACL, au médecin de prévention…

Outre l'obligation de mettre en œuvre les mesures de sécurité nécessaires pour protéger les données, l'employeur doit, sous certaines conditions, informer la ou les personnes concernées quand la violation de données est « *susceptible d'engendrer un risque élevé pour les droits et libertés* » (RGPD, art. 34).

Certaines données sensibles nécessitent le consentement préalable de l'agent (RGPD, art. 9). Ce consentement doit être précis, non équivoque et constituer un acte positif en s'effectuant par une case à cocher ou une autorisation écrite. Le RGPD exonère les collectivités de cette obligation de consentement lorsque le traitement de données est nécessaire à une obligation légale ou à une mission de service public.

Le recueil du consentement des agents préalablement au traitement de leurs données à caractère personnel n'apparaît pas systématique et non nécessaire au regard de ces deux fondements.

Toutefois, le recueil du consentement est obligatoire en matière de traitement de données sensibles, comme les données médicales, celles relatives à l'appartenance syndicale ou une photographie.

Le décret n° 2018-1117 du 10 décembre 2018 relatif aux catégories de documents administratifs pouvant être rendus publics sans faire l'objet d'un processus d'anonymisation précise les catégories de données pouvant-être publiées publiquement. Il indique notamment que sont communicables sans occultation *« 1° Les documents nécessaires à l'information du public relatifs aux conditions d'organisation de l'administration, notamment les organigrammes, les annuaires des administrations et la liste des personnes inscrites à un tableau d'avancement ou sur une liste d'aptitude pour l'accès à un échelon, un grade ou un corps ou cadre d'emplois de la fonction publique ».*

Exemple de mention en cas de transmission à l'assurance statutaire

La collectivité est responsable du traitement. Le transfert de données à l'assureur nécessite le consentement de la personne concernée (RGPD, art. 6, 1-a).

Les catégories de données concernées sont :

- *état civil ;*
- *numéro de Sécurité sociale ;*
- *coordonnées ;*
- *données de santé : certificats médicaux établis dans le cadre de l'accident, prescriptions, ordonnances médicales… ;*
- *informations liées à la rémunération.*

Les destinataires des données sont les compagnies d'assurances et notamment le médecin-conseil en charge du dossier, les avocats ou conseils juridiques desdites compagnies.

Les données enregistrées sont conservées conformément aux prescriptions des archives départementales et aux prescriptions des Archives de France. Lorsqu'il existe un recours contre un tiers ou un contentieux, les données sont conservées jusqu'à l'intervention de la décision définitive.

Conformément aux articles 49 et suivants de la loi « informatique et libertés » du 6 janvier 1978 modifiée, vous bénéficiez d'un droit d'accès, de rectification aux informations qui vous concernent.

Vous pouvez également définir le sort de vos données après votre décès, en vous adressant, par voie postale, au délégué à la protection des données.

Vous pouvez également, pour des motifs légitimes, vous opposer au traitement des données vous concernant, sauf si ce droit a été écarté par une disposition législative et introduire une réclamation auprès de la Cnil (loi du 6 janvier 1978 modifiée, art. 56).

Dans le cadre de la mise en œuvre du RGPD, l'information et la formation des responsables de service ou des managers est indispensable.

Il convient de les sensibiliser sur certains éléments : quelles sont les données personnelles utilisées et pouvant être collectées ? Dans quel but et pendant combien de temps doivent-elles être conservées ? Dans quelles conditions un traitement de données peut-il être constitué ? Qui peut avoir accès aux données ? Etc.

La sensibilisation doit permettre de comprendre les impacts du RGDP sur les pratiques RH internes et faire évoluer les manières de travailler des managers.

Un plan de formation des agents à la thématique « protection des données » peut également être mis en place dans la collectivité en collaboration avec le délégué à la protection des données.

▶ 4 - Répondre aux sollicitations des agents

Le RGPD crée de nouveaux droits pour les agents tels que le droit à l'oubli et le droit à la portabilité des données.

Les agents peuvent saisir leur service RH pour exercer leurs droits sur leurs données personnelles. Le RGPD raccourcit les délais de réponse à la sollicitation d'un agent : l'employeur dispose d'un mois, ou de deux en cas de demandes complexes, pour y répondre.

NOTRE CONSEIL

- Collectez uniquement les données strictement nécessaires à la finalité du traitement.
- Reportez-vous aux guides pratiques relatifs à la méthode et aux outils en matière d'analyse d'impact mis en ligne par la Cnil.
- Assurez-vous que vos prestataires RH comme les éditeurs de logiciels de paie, de carrière, etc. vous offrent toutes les garanties de conformité au RGDP et notamment de sécurité et de confidentialité des données transmises ou hébergées.

ÉVITEZ LES ERREURS

Les collectivités territoriales avaient déjà, dans le cadre de la loi n° 78-17 du 6 janvier 1978 , dite « loi informatique et libertés », mis en place des procédures de traitement des données personnelles de leurs agents. Toutefois, ne négligez pas l'importance d'adapter ces procédures à la logique du RGPD.

Depuis le 25 mai 2018, l'obligation déclarative auprès de la Cnil a été supprimée et remplacée par la tenue d'un registre interne des traitements de données à caractère personnel. Ce registre doit être tenu à la disposition de la Cnil.

FAQ

Est-il possible de collecter des données sensibles ?

L' article 6 de la loi n° 78-17 du 6 janvier 1978 modifiée par l' ordonnance n° 2018-1125 du 12 décembre 2018 prévoit qu'il est interdit de traiter des données à caractère personnel qui révèlent la prétendue origine raciale ou l'origine ethnique, les opinions politiques, les convictions religieuses ou philosophiques ou l'appartenance syndicale d'une personne physique, ou de traiter des données génétiques, des données biométriques aux fins d'identifier une personne physique de manière unique, des données concernant la santé ou des données concernant la vie sexuelle ou l'orientation sexuelle d'une personne physique.

Des exceptions à cette interdiction sont mentionnées à l'article 9 du RGPD et notamment lorsque la personne concernée a donné son consentement explicite au traitement de ces données à caractère personnel pour une ou plusieurs finalités spécifiques ou lorsque le traitement est nécessaire aux fins de l'exécution des obligations et de l'exercice des droits propres au responsable du traitement ou à la personne concernée en matière de droit du travail, de la Sécurité sociale et de la protection sociale.

Quelle est la procédure à respecter en cas de vol d'un ordinateur ou d'un téléphone professionnel ?

Le RGPD impose des obligations renforcées en cas de perte ou de vol de données.

Si l'ordinateur portable ou le téléphone est volé ou perdu, l'employeur doit le déclarer à la Cnil dans les 72 heures, « *à moins que la violation en question ne soit pas susceptible d'engendrer un risque pour les droits et libertés des personnes physiques* » (RGPD, art. 33).

ALLER PLUS LOIN

Références juridiques

- Règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, et abrogeant la directive 95/46/CE (règlement général sur la protection des données)
- Ordonnance n° 2018-1125 du 12 décembre 2018 prise en application de l'article 32 de la loi n° 2018-493 du 20 juin 2018 relative à la protection des données personnelles et portant modification de la loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés et diverses dispositions concernant la protection des données à caractère personnel
- Loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés, article 6
- Décret n° 2018-1117 du 10 décembre 2018 relatif aux catégories de documents administratifs pouvant être rendus publics sans faire l'objet d'un processus d'anonymisation

ENTRETIEN

« Conscientiser, prévenir et gérer : construisons ensemble une culture du risque cyber »

Oriana Labruyère, Avocate en droit du numérique et DPO, avocate associée de La Robe Numérique, partage des conseils pour développer une culture du risque cyber, basés sur ce que Me Oriana Labruyère appelle les « bonnes pratiques cyber ».

■ **WEKA :** ***Lorsqu'on est victime d'une cyberattaque, en tant qu'acteur public, quelles sont nos obligations et que doit-on faire ?***

Oriana Labruyère : On se place au moment où il y a la crise : qu'est-ce que je dois faire ? Vous n'êtes plus seul. Qui appeler ? Il faut contacter Computer Security Incident Response Team pour savoir où ils sont et les identifier correctement par rapport à la région. Puis on se coupe de l'extérieur, il ne faut pas éteindre les ordinateurs, mais il faut au moins se couper du réseau, couper Internet pour que ça circule en vase clos. C'est la première réaction et c'est peut-être la réaction sur laquelle il faut former. Il faut former les collaborateurs, les équipes qui travaillent avec vous. Ensuite, on doit informer, il y a des obligations légales d'information, de l'ANSSI, de la CNIL et de l'assurance, évidemment. Posez-vous ces questions en amont, car une fois que l'attaque est là, que la situation se présente, c'est un peu tard. Je ne me mets pas à chercher les informations au dernier moment, quand vraiment je n'ai plus le choix parce que la panique, la sidération, font qu'on se perd, donc avoir des éléments facilement accessibles c'est essentiel. Dans les obligations légales, l'information à l'ANSSI doit être faite dès que possible et l'information à la CNIL si des données à caractère personnel sont impactées par la cyberattaque, dans un délai de 72 h. Là-dessus, vous pouvez ouvrir une déclaration, ne pas la clôturer, ce qui permet de gagner quelques précieuses heures ou jour pour la compléter ensuite, sur la partie notamment des volumes de données et du degré de gravité. Ensuite, on a la fameuse question : est-ce que je paye quand on prend un cyber locker ? Pour moi la réponse est toujours

Oriana Labruyère, Avocate en droit du numérique et DPO, avocate associée de La Robe Numérique

non parce que c'est le financement d'un comportement très terroriste. Si vous payez vous n'êtes pas garanti de récupérer vos datas, et peut être qu'ils reviendront parce qu'ils ont été payés. Ensuite, l'information est une obligation. Il faut informer pour permettre à la chaîne des bénéficiaires de vos prestations de savoir ce qui se passe et d'avoir une vigilance augmentée. Même si on ne sait pas exactement le périmètre de l'attaque, on peut tout à fait communiquer. Dans la chaîne complète, il faut cette information pour que les tentatives d'attaques par rebond soient coupées et soit rendue impossible. Même si c'est délicat à cause de la culpabilité de la victime.

C'est le financement d'un comportement très terroriste.

CONSEILS DE CHRISTINE BERTRAND

Christine Bertrand, Directrice des systèmes d'information et numérique - Direction générale adjointe de l'administration et des ressources du Département de Seine-et-Marne.

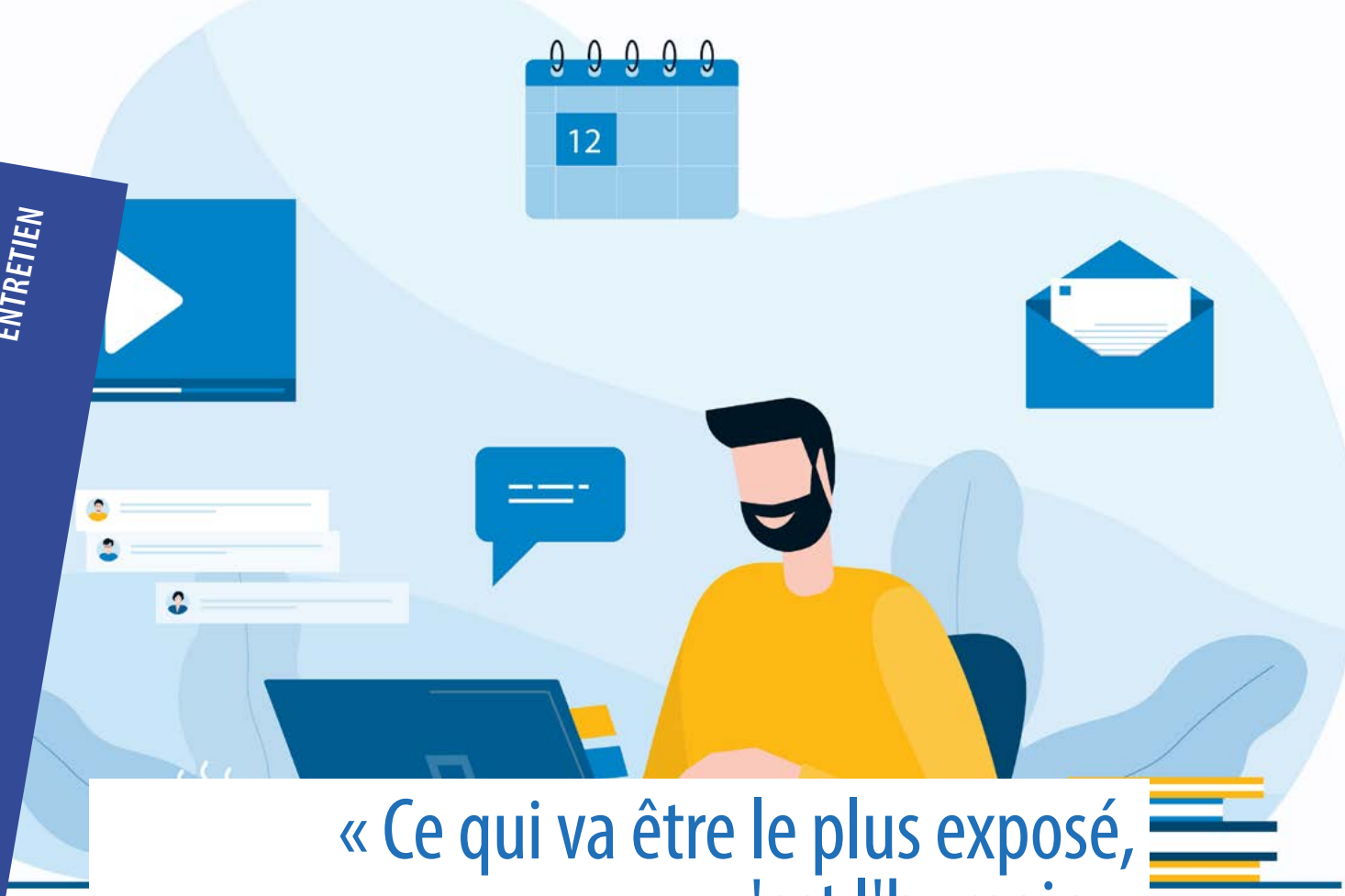
■ **WEKA :** ***Comment bien réagir quand sa collectivité est victime d'une cyberattaque ?***

Christine Bertrand : Le premier conseil est de limiter la progression des impacts : débrancher le réseau est la première action réaliste. Deuxième chose, il faut informer en communiquant à différents niveaux : en interne, à la direction générale, vers vos partenaires, vers vos prestataires et surtout vers les citoyens. Il doit s'agir d'une communication adaptée en fonction de la cible et en fonction de l'attaque. L'objectif est d'éviter le blackout, garder le lien, garder la confiance et communiquer sur les enjeux et sur le plan de continuité d'activité.

Ensuite, il convient de porter plainte et d'informer la Commission nationale de l'informatique et des libertés (CNIL) pour tout ce qui concerne l'indisponibilité de services et la fuite de données.

Enfin, il vous faut investiguer sur l'attaque en elle-même en parallèle, pour vous permettre d'évaluer le périmètre, les dégâts et en déduire le plan de remédiation. En dernier lieu, vous devez réaliser ce plan de remédiation pour arriver à un rétablissement du service et, tout au long de ces étapes, toujours communiquer.

ENTRETIEN



« Ce qui va être le plus exposé, c'est l'humain »

Dominique Bogé, Chef d'Escadron, Chef du département Prévention et protection, Unité Nationale Cyber, a accepté de répondre à nos questions sur les dispositifs concrets à mettre en place après une cyberattaque, ainsi que sur sa vision de l'avenir de la cybersécurité.

■ **WEKA :** ***Quelles bonnes pratiques à adopter pour tout agent, pour limiter les menaces cyber ?***

Dominique Bogé : Premièrement, il faut accepter le principe que ce qui va être le plus exposé c'est l'humain.

Une machine peut être dysfonctionnelle, mais une fois qu'on a eu une action correctrice sur elle, son état est constant. Pour un humain, ce n'est jamais le cas.

Sur ce principe, la messagerie est le vecteur de 90 % des cybermenaces et en particulier des ransomware. Donc, le premier point d'attention doit porter sur ce qu'on va recevoir par mail. En tenant compte de l'état émotionnel de l'homme qui n'est pas forcément constant, on devrait appliquer ce qu'on appelle des protocoles, c'est-à-dire faire toujours la même chose tout le temps, de manière calibrée et préétablie, ce qui permet de ne pas dépendre de l'état émotionnel de la personne concernée. Un mail inconnu, non identifié, qui nous paraît étrange ne devrait par principe jamais être ouvert.

Il faut prendre du recul et le temps nécessaire pour relire tranquillement le mail. Rien n'est jamais si urgent qu'il nécessite d'être traité dans la seconde. Vous devez prendre votre temps pour analyser et regarder l'adresse mail. Parfois, l'adresse est censée être une adresse institutionnelle comme pour les services des impôts ou une autre administration. Cependant, si on regarde bien la fin de l'adresse mail des mails piégés, on retrouve souvent @gmail ou @outlook, voir des domaines professionnels sans rapport avec l'objet de celui-ci. Ça ne peut pas provenir d'une administration car elle n'utilise pas ce genre d'adresse de messagerie.

Si l'adresse mail passe le premier filtre de l'analyse, le second point d'attention concerne le contenu du mail. S'il y a une décision à prendre, de l'argent à engager, ça ne doit jamais reposer sur une seule

Dominique Bogé, Chef d'Escadron, Chef du département Prévention et protection, Unité Nationale Cyber

personne. On fait un double appel, on croise les données et on vérifie la véracité de la demande. Un simple mail, avec un seul opérateur et sans authentification, ne peut pas être suffisant pour engager une structure, une entreprise, une administration dans des décisions qui vont être irréversibles ou difficilement réversibles.

Ensuite, il y a des choses évidentes : on ne consulte pas de documents qui ne nous sont pas destinés. Évidemment, on ne clique pas sur les liens qu'il y a dans les mails, on va soi-même (en tapant l'adresse) sur le site et on va chercher ce dont on a besoin. Il ne faut pas, dans la même logique, aller sur des sites difficilement identifiables, non officiels ou dangereux.

Quand on part de son poste de travail, on le verrouille.

Concernant les protocoles de sécurité d'usage, il faut aussi mettre un mot de passe complexe, différent pour chaque type d'utilisation. L'utilisation d'un gestionnaire de mot de passe permet de ne pas devoir tous les retenir.

Quand on part en vacances, il faut faire attention à ses communications extérieures, sur les réseaux sociaux, par mail ou dans un message d'absence qui donnerait trop d'informations. La prudence est de mise parce que celui qui va vouloir faire une fraude directe ou indirecte va capter ces informations et les croiser. Il lui suffit d'avoir un nom et tout le reste, involontairement, c'est nous qui le donnons.

Ce n'est pas difficile, il suffit d'avoir un nom.

Il faut aussi être prudent dans les conversations qu'on peut avoir en direct ou par téléphone, ou dans les usages du smartphone. Ces échanges peuvent être captés, écoutés et, pour tout dire, s'ils sont confidentiels, ne devraient pas se produire dans des lieux publics. Il ne faut pas mélanger les usages privés des usages professionnels car si le smartphone est volé, la vie personnelle peut être accessible, mais la vie professionnelle aussi.

Il y a enfin et évidemment des conseils de bon sens sur les sauvegardes à réaliser parce que s'il n'y a pas de sauvegardes automatiques, et qu'il y a un dysfonctionnement, on perd tout.

Les mises à jour sont à faire (ou sont poussées automatiquement). Ce n'est pas toujours le cas dans les petites collectivités, c'est parfois les agents qui les font. L'antivirus et le pare feu doivent aussi avoir des mises à jour. Une machine a également des logiciels embarqués de traitement de texte, de visionneur, de vidéo, des logiciels de comptabilité, etc., ces logiciels-là ont des correctifs qu'il faut appliquer. Sans cela, c'est la porte ouverte à une compromission.

Pour ce qui concerne l'exploitation délictueuse d'une faille humaine, Kevin Mitnick qui a inventé l'ingénierie sociale donne un bon exemple.

Dans les années 70-80, il a réussi à pirater les standards de la plus grosse compagnie de téléphonie américaine AT&T. Kevin Mitnick explique que pour contaminer une entreprise, ce n'est pas compliqué : il suffit d'entrer dans une société, de prendre l'ascenseur avec une disquette rouge sur laquelle il y aurait une étiquette indiquant « strictement confidentielle, à ne pas consulter », puis de monter et redescendre au rez-de-chaussée. Avant de partir, il laisserait accidentellement tomber la disquette dans l'ascenseur. Il conclut ainsi : « N'ayez aucun doute, dans les dix minutes, la disquette est dans un des ordinateurs de la société ».

■ **WEKA :** ***Quels sont les bons réflexes à adopter immédiatement lorsqu'on prend conscience d'une cyberattaque dans notre collectivité ?***

Dominique Bogé : La crise qui a l'impact le plus violent et le plus pérenne sur une structure, c'est le ransomware ou le rançongiciel. Les systèmes et les fichiers sont chiffrés et inaccessibles. Parfois, on n'a plus accès à rien. La téléphonie, qui passe de plus en plus par Internet avec la téléphonie sur IP, est dysfonctionnelle elle aussi.

Celui qui constate la crise va donner l'alerte au responsable des systèmes d'information, aux services informatiques, et à sa hiérarchie directe, pour que les premières opérations soient lancées. S'il existe un plan de secours, il faut le mettre en œuvre tout de suite et ouvrir un chrono pour documenter

heure par heure, voire minute par minute, ce qui a été fait et qui l'a fait. Cet impératif permet d'aider à investiguer les machines. Il faut pouvoir différencier ce qui constitue une action de l'auteur, de ce qui constitue une action, soit d'un agent, soit de quelqu'un qui a été appelé pour résoudre la crise. En outre, ce chrono permet d'aider à la remise en production des systèmes et parfois de donner des éléments de communication.

Ensuite, il faut trouver le « patient zéro » (la machine à l'origine de la compromission), couper la connexion internet, au cas où il y aurait des processus malicieux en cours, mais ne pas éteindre les machines. Si une machine est identifiée comme étant le « patient zéro », il faut trouver le moyen de l'isoler du reste du réseau.

Quand il y a un câble réseau, c'est simple : on débranche le câble.

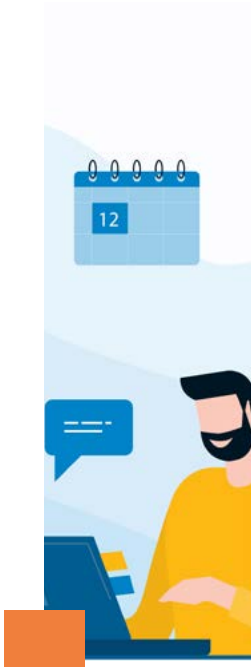
Quand on a le Wifi, il faut désactiver le Wifi pour que cette machine-là ne continue pas à communiquer avec le réseau interne, et finisse par infecter les autres machines. Il faut savoir s'il y a des postes qui sont connectés ou qui peuvent l'être de manière nomade, car ils peuvent contribuer soit à propager, soit à entraver l'opération visant à circonscrire l'attaque en cours.

Une autre raison de ne pas éteindre la machine compromise est que cela permet parfois de récupérer des données. Dans certains cas il y a des éléments sur les clés de chiffrement qui sont en mémoire vive. La mémoire vive est volatile, et si on éteint l'ordinateur, elle disparaît et on ne la récupère pas. Il y a de multiples éléments techniques qui peuvent être récupérables en faisant de l'investigation. Si la gendarmerie ou des experts numériques ont besoin d'investiguer sur les machines et l'origine du problème, les données contenues en mémoire vive peuvent être utiles (une copie de la mémoire vive s'appelle un DUMP).

Ensuite, il faut se dire que s'il y a une crise, il y a des services importants voire essentiels qui ne pourront pas fonctionner et il va falloir communiquer sur cela. Ce n'est pas une option, c'est une nécessité. Qui communique ? Comment ? Et surtout, qu'est-ce qu'on dit ? Il ne faut pas mentir. L'information, même non communiquée officiellement, va se propager de toute façon et si vous ne contrôlez pas ce qui est dit avec les éléments que vous voulez bien partager, quelqu'un va communiquer à votre place et ça sera pire. Viendra ensuite la phase de mode dégradé : on a besoin de fonctionner mais tout n'est pas encore résolu ou opérationnel.

On va essayer de trouver le patient zéro.

S'il n'y a pas de protocole de gestion de crise, de guide qui permette de déterminer qui fait quoi, les premiers temps vont être compliqués car ce sera la panique, voire la sidération. Or Il y a beaucoup de petites communes qui n'en ont pas, parce qu'elles pensent que ce n'est pas nécessaire, ou qu'elles n'ont pas l'argent pour cela. Mais il faut un plan de « gestion de crise » ou un plan de reprise ou de continuation d'activité. Et au moins une fois par an, il faudrait faire un exercice de simulation d'un ransomware. Ça ne voudra pas dire qu'il n'y aura pas un moment de panique si ça arrive réellement, mais ce sera moins difficile d'avoir les bons réflexes. De plus, cela limite le vertige de l'effet de surprise.



■ **WEKA :** ***Quels experts sont mis à disposition pour accompagner les collectivités dans cette gestion de crise ?***

Dominique Bogé : Pour le volet premier secours, la question peut être posée à l'ANSSI. Il y a dans certaines régions des CERT (Computer Ermergency Response Team, un centre d'alerte et de réaction aux attaques informatiques destinés aux entreprises et aux administrations) régionaux qu'on peut appeler pour avoir les conseils de première urgence.

Il y aussi les PASSIs (Prestataires d'Audit de la Sécurité des Systèmes d'Informations) qui sont qualifiés par l'ANSSI sur les audits et dans de nombreux cas, un niveau reconnu en matière de remédiation. Lorsque vous n'avez pas votre propre prestataire

ou que vous ne savez pas qui choisir, cybermalveillances.gouv.fr propose, si vous le souhaitez, des prestataires, soit référencés, soit labellisés ; le prestataire labellisé a obtenu une validation par l'AFNOR de ses compétences en termes de remédiation et d'audit. Pour autant, cette démarche reste quand même entre les mains de la collectivité, c'est à elle de déclencher les choses, évidemment d'alerter la gendarmerie parce qu'il peut y avoir un dépôt de plainte (c'est vivement recommandé bien sûr). Il faut également prévenir l'ANSSI, parce que c'est l'autorité de référence en la matière et, le cas échéant la CNIL, parce qu'une fuite de données ou un risque de fuite de données peut arriver. Vous pouvez, en outre, avoir l'obligation de prévenir dans certains cas toutes les personnes dont les données ont été compromises.

■ **WEKA :** ***Que faut-il mettre en place pour apprendre et se prémunir d'autres attaques ? Quelle est l'importance d'un RETEX et comment le mettre en place ?***

Dominique Bogé : Premièrement, sécuriser l'interface homme/machine. Il faut revoir son système d'information, identifier ce qui doit être amélioré, une machine obsolète doit être remplacée et la sécurité générale du système doit être durcie. La gendarmerie propose aux collectivités de dérouler un « pré-diagnostic cyber » basé sur la norme ISO 27 001 à laquelle ont été ajoutés les attendus du RGPD. Ça s'appelle DiagONal (acronyme de « Diagnostic Opérationnel National »). Il comporte une centaine de questions qui sont déroulées sur l'intégralité de ce qu'il est nécessaire de prendre en compte dans un système d'information allant de la machine à l'humain, en passant par la sécurité physique de ces machines. On l'a décliné sur les collectivités, les entreprises et les établissements de santé, avec des conseils sur les points d'attention sur lesquels revenir. On fait référence aux guides et aux aides qui existent déjà à l'ANSSI par exemple. Cet outil ne dispense pas de faire réaliser un vrai audit par un expert. Il y a une nécessité impérieuse de faire très régulièrement des opérations de prévention et de sensibilisation, ce qu'on appelle l'hygiène numérique. Il y a une courbe d'apprentissage qui va monter, puis on va arriver à un point sommital où on sera avisé et on connaitra les choses, mais derrière on va un peu oublier, faire moins attention, et la courbe va redescendre petit à petit. Il faut alors recommencer une autre opération de sensibilisation et de prévention pour rafraîchir la mémoire et revenir à un état nominal de sécurité satisfaisant.

C'est un exercice qui est sain, et pour tout le monde.

Certaines personnes sont victimes de ce qu'on appelle un biais cognitif qui s'appelle l'effet Dunning-Krueger, qui consiste à surestimer son niveau de compétence. Si tout le monde suit les règles de sécurité informatique, avec les gestes simples d'hygiène numérique, on supprime 70 % des menaces. C'est valable pour les collaborateurs comme pour l'équipe de direction. J'ai eu des entretiens avec des cadres brillants qui étaient arrivés là parce qu'ils étaient au sommet de leurs connaissances mais un jour, ils se sont fait prendre et ils se sont demandés comment ça avait pu leur arriver. Et on en revient à mon propos d'introduction concernant l'état émotionnel de l'humain qui est inconstant, cela doit éveiller les consciences sur le fait que l'hygiène numérique concerne tout le monde, tout le temps. Avec un suivi et un rappel régulier on peut résoudre bien des risques numériques.

Deuxièmement, le RETEX. Si une crise est survenue, il est nécessaire, au retour du mode de fonctionnement normal, de se rassembler, avec l'équipe de direction, les experts mais également les collaborateurs et débriefer la crise. Certains ont subi un traumatisme. Il faut se demander ce qu'il s'est passé, ce qui a été fait individuellement et collectivement, et ce qu'on peut faire pour que ça ne se reproduise plus. Si cela doit se reproduire, réfléchir pour ne pas dupliquer les mêmes erreurs commises par ignorance. C'est important de le faire. C'est un exercice qui est sain, et pour tout le monde.

■ **WEKA :** ***Le secteur public (hôpitaux, collectivités) a subi beaucoup d'attaques, a-t-il pris conscience de l'ampleur de cette menace ? Est-il aujourd'hui mieux et suffisamment préparé pour les gérer ?***

Dominique Bogé : On constate une amélioration de la prise en compte du risque cyber, mais il y a encore une marge de progression.

À titre d'illustration, d'après nos statistiques de DiagONale cyber (plus de 1 500 diagnostics réalisés auprès des collectivités), 40 % des collectivités n'ont pas désigné de délégué à la protection des données. Le respect du RGPD (Règlement Général relatif à la Protection des Données) ou la sécurité des systèmes d'information sont encore perçus à tort comme secondaires parce que les collectivités se disent qu'elles n'ont pas grand-chose comme informations, qu'elles sont toutes petites.

C'est une méconnaissance des cybermenaces dont font parties les ransomwares. L'attaque ciblée va rentrer dans un système d'information, trouver le moyen de pénétrer puis de cartographier tout le système, y passer des semaines, chiffrer les données et demander la rançon. Un autre type d'attaque consiste à envoyer des centaines, voire des milliers de requêtes avec une charge virale, un ransomware, et celui qui est le moins bien protégé se fait prendre et se fait chiffrer les données. C'est presque plus intéressant pour les hackers, car cela représente beaucoup plus de monde et coûte moins d'argent donc présente moins de risques. L'attaque est réalisée sur des cibles plus petites et souvent moins bien protégées, avec des systèmes où les correctifs ne sont pas toujours faits, où les serveurs ont des mots de passe par défaut, où l'agent peut se connecter à la mairie en télétravail et n'a pas de VPN. Des vulnérabilités, y compris humaines, sont déjà existantes et vont faciliter le travail aux hackers. Il suffit d'envoyer un mail, que quelqu'un clique dessus et c'est fini.

Les collectivités ne sont pas plus attaquées que les autres, mais elles sont bien plus exposées car souvent moins bien protégées.

■ **WEKA :** ***Les menaces s'accentuent-elles ? Dans un avenir proche, les JO relèvent-ils le niveau d'alerte ? Dans un futur plus lointain, doit-on s'attendre à une menace plus persistante et plus efficace ?***

Dominique Bogé : Ce qui fonctionne le mieux et qui correspond à 80 ou 90 % de la cybercriminalité, c'est de s'attaquer à un humain. Lui faire faire quelque chose qu'il ne devrait pas faire. Ça ne nécessite pas un niveau technique très important et ça va continuer longtemps parce que ça marche. Le ratio coût de fabrication/bénéfice est gigantesque pour le ou les auteurs. Le coût de la cybercriminalité dans le monde est de 7 000 milliards de dollars. Ça rapporte plus que le trafic de stupéfiants, ça rapporte plus que le trafic d'êtres humains, et ça apparaît moins dangereux.

Des IA génératives vont être utilisées pour cibler certains types de personnes.

Ce qui va changer, c'est l'usage des algorithmes. Des IA génératives vont être utilisées pour crédibiliser, industrialiser et dans certains cas, cibler certains types de personnes. Par exemple ça permettra de faire une campagne de phishing qui ne visera que les personnes dont on a récupéré les données de santé, avec un mail qui ressemblera à un mail médical. L'IA générative va beaucoup plus vite qu'un humain, elle peut automatiser un certain nombre de tâches. Cela va permettre d'affiner les techniques pour tromper des personnes, et être beaucoup plus réactifs.

Le problème des campagnes de phishing pour ceux qui les génèrent, c'est que ça a une durée de vie courte, c'est assez rapidement détecté, les noms de domaines associés sont repérés et blacklistés et plus aucun accès n'est possible. Plus rien ne fonctionne pour les flibustiers du net. Les hackers sont alors obligés de passer à autre chose et de régénérer une nouvelle forme de campagne. Certaines campagnes ne durent que quelques heures. Les risques induits par les JO sont évidents à l'échelle macro puisque pendant toute la durée des Jeux Olympiques de Paris, la France sera vue par plusieurs milliards de personnes. Il faut s'interroger sur ce qui va intéresser les hackers : le vol de données, l'extorsion de fonds, l'attaque de déstabilisation ou encore l'action politique.

Les opportunités seront présentes, parce qu'une bonne partie des forces institutionnelles seront

mobilisées pour défendre des risques d'attentats. Les risques seront importants pour les systèmes de communication, pour les systèmes hospitaliers, pour les aiguillages. Pour autant, il ne faut pas céder à la psychose car il faut un sacré niveau pour y arriver. Attaquer des cibles plus petites, mais en nombre, ça fait parler de soi. Lorsque les communes ont des systèmes de pilotage informatique pour les éclairages publics par exemple, il pourrait y avoir une tentative pour en prendre le contrôle, c'est une attaque facile qui ne nécessite pas énormément de moyens mais qui a un effet visible, immédiatement et largement, de nature à créer une angoisse au sein de la population. Des petites choses peuvent avoir de grandes conséquences. Il y a également le risque que les sites internet de collectivités se fassent attaquer, pour des actions revendicatives et que ce soit tout particulièrement visible d'un maximum de personnes.

Si je devais conclure en forme de clin d'œil je dirais qu'en matière de sécurité numérique, la meilleure défense… c'est la défense.

il ne faut pas céder à la psychose.

La menace cyber en forte hausse en 2023 pour les collectivités, selon Cybermalveillance.gouv

Hameçonnage, rançongiciel et piratage de compte se sont distingués parmi les demandes d'assistance des collectivités et administrations sur la plateforme Cybermalveillance.gouv.fr, en 2023. Pour les collectivités et administrations, comme pour les entreprises et associations, les principales menaces qui les visent continuent donc de gagner en intensité.

Dans son rapport d'activité présenté le 5 mars 2024, Cybermalveillance.gouv fait le point sur les recherches d'assistance de cybercriminalité en 2023. Pour sa sixième année d'existence, la plateforme relève trois principaux motifs de consultation de demandes d'assistance des collectivités et administrations. En tête, l'hameçonnage ou phishing, avec 27 % des demandes, suivi des attaques par rançongiciel (21 %) et du piratage de compte en ligne (17,5 %). La violation de données (9,7 %) et le virus (8,1 %) restent également très préoccupants, suivis du faux support technique (6,7 %) et de la défiguration de site internet (4,6 %).

Cybermalveillance.gouv précise que si, par rapport à 2022, les variations en proportion ne paraissent pas significatives, les variations en volume présentent souvent des hausses très importantes. Ainsi, en un an, les défigurations de site internet ont augmenté de 73 %, les programmes malveillants (virus) de 71 %, les fraudes au faux support technique de 54 % et les violations de données de 45 %. Les logiciels de demande de rançon ont crû de 36 % et le phishing de 26 %.

En 2023, les contenus de Cybermalveillance.gouv sur l'hameçonnage et les moyens d'y faire face ont recueilli, tous types de visiteurs confondus, 1,5 million de consultations et plus de 50 000 recherches d'assistance. Mails, SMS (smishing), messages instantanés, publications sur les réseaux sociaux, liens sponsorisés sur les moteurs de recherche, appels téléphoniques (vishing), QR codes frauduleux (quishing)… Tous les moyens sont bons. « L'hame-

çonnage vise toujours à créer, sous une apparence légitime et crédible, un sentiment d'urgence ou d'intérêt chez les victimes pour les tromper », pointe le rapport. Avec, pour objectif, de les inciter à fournir des données personnelles ou confidentielles (mots de passe, coordonnées de carte bancaire, codes de validation…) ou à télécharger un programme malveillant qui prendra le contrôle de leur appareil.

L'IA AIDERA À SE PROTÉGER DES CYBERCRIMINELS

Depuis plusieurs années, un écosystème cybercriminel de l'hameçonnage commercialise à des tarifs toujours plus compétitifs des méthodes, listes d'adresses mail ou de numéros de téléphone actifs, faux messages, faux sites très réalistes, qui les rendent accessibles à une petite cyberdélinquance en fort développement. Les informations sont ensuite revendues sur les places de marché cybercriminelles dans le darknet et les délinquants rivalisent d'imagination : piratage de compte, débits bancaires frauduleux, infection virale, attaque par rançongiciel, appel de faux conseillers bancaires…

Quant à l'intelligence artificielle (IA), « comme toute évolution technologique », ses possibilités « ne peuvent que retenir l'attention des cybercriminels » et des modèles d'IA générative cybercriminels ont déjà été développés : WormGPT, FraudGPT, ThreatGPT… Pour autant, cela ne devrait pas bouleverser le panorama des cybermenaces. Surtout, « l'IA s'imposera certainement aussi comme une opportunité d'aider les publics à mieux et plus facilement identifier les menaces et s'en protéger », conclut le rapport.

Marie Gasnier

Les logiciels de demande de rançon ont crû de 36 % et le phishing de 26 %.

FICHE MÉTHODOLOGIQUE WEKA

Fiche 14305

Mise à jour le 29 mars 2024

La cybersécurité dans les collectivités et leurs établissements

CONTEXTE

En 2021, la cybercriminalité a touché 58 % des institutions contre environ 30 % en 2020.

En 2023, selon le ministère de l'Intérieur, 1 entreprise sur 5 a été victime d'une cyberattaque au cours de l'année.

Un constat s'impose face à ces chiffres en forte augmentation : les collectivités sont malheureusement devenues une cible de choix pour les pirates informatiques.

Si cibler les collectivités peut être la porte d'entrée pour acquérir une grande quantité de données personnelles très sensibles, elles font également souvent l'objet de chantage à la divulgation des données dérobées *via* des *ransomwares*. Les pirates réclament en effet de l'argent pour ne pas diffuser lesdites données.

La **protection informatique** est donc devenue un axe primordial dans un monde où tout va très vite. Le secteur public doit se tourner vers des outils capables de **contrer ces attaques permanentes** mais également d'établir une **stratégie sur le long terme** afin de limiter la perte de données en cas d'intrusion informatique.

▶ 1 - La cybersécurité dans les collectivités : enjeux et cadre juridique

En 2020, 30 % des collectivités territoriales ont déjà été victimes d'une **attaque *ransomware*** (*source* : étude Clusif, 2020).

Dans ce contexte, l'Agence nationale de la sécurité des systèmes d'information (Anssi) a également précisé que toutes les collectivités sont concernées, quelle que soit leur taille.

Ces attaques consistent en un blocage des accès aux ordinateurs et fichiers en les chiffrant. Un chantage est organisé : il est demandé le paiement d'une somme d'argent pour « déchiffrer » les fichiers. Selon le ministère de l'Intérieur, le montant moyen des rançons s'est élevé en 2023 à 6 400 € et elles connaissant une hausse constante (50 % en moyenne par an depuis 2016), certaines pouvant même atteindre plusieurs millions d'euros en fonction de la taille de la structure visée.

La **cyberattaque** est une tentative d'accès non autorisée aux systèmes d'information d'une structure, à une ressource ou encore à un périphérique (téléphone, PC, copieur/imprimante) appartenant au réseau.

En 2021, 58 % des collectivités ont été touchées par un *ransomware*, 59 % rapportent une augmentation du volume d'attaques, 59 % rapportent une augmentation de la complexité des attaques, 56 % rapportent une augmentation de l'impact des cyberattaques (*source* : LIvre blanc Sophos, février 2023).

Dans ce cadre, la majorité des collectivités et leurs établissements ont déclaré que l'attaque avait eu un impact sur leur capacité à fonctionner.

Les conséquences d'une attaque peuvent être très importantes, il peut s'agir de la perte de données confidentielles, d'un arrêt de production, de la mise à l'arrêt d'un service, de la fuite avec utilisation malveillante des données, de pertes financières et d'une dégradation de la réputation de la structure qui sera considérée comme peu fiable en termes de protection des données sensibles…

La perturbation des services publics peut être avoir des conséquences graves, par exemple

des interruptions de services d'urgences ou de services liés aux énergies (eau, électricité), et bien souvent l'ensemble des données ne peut pas être entièrement restauré suite à une cyberattaque.

Les données volées par les pirates informatiques peuvent être partagées et utilisées à des fins frauduleuses sur le Dark Web moyennant rémunération ; il peut s'agir de les utiliser dans le but de réaliser des usurpations d'identité, par exemple. De ce fait, la réputation de la collectivité peut être entachée auprès des administrés. Les structures publiques doivent donc, en fonction de leurs moyens financiers, réfléchir à des mesures préventives.

▶ 2 - Le droit et la cybersécurité

Le cadre juridique de la cybersécurité s'est considérablement développé depuis une décennie. Il poursuit l'objectif de renforcer la confiance des usagers dans les services numériques du secteur public en renforçant la sécurité dans la protection de leurs données personnelles. Les principaux textes sont les suivants :

- Mai 2010 : le référentiel général de sécurité (RGS) fixe le premier cadre français de la confiance numérique pour les téléservices et au sein de l'administration.
- Décembre 2013 : la loi n° 2013-1168 du 18 décembre 2013 relative à la programmation militaire (LPM) garantit la protection des activités d'importance vitale.
- Avril 2016 : l'Union européenne adopte une réforme majeure de son cadre de protection des données avec le règlement général sur la protection des données (RGPD) du 27 avril 2016. Ce dernier est applicable depuis le 25 mai 2018. Il a pour objectif, entre autres, de responsabiliser les acteurs publics et privés quant à la protection des données personnelles.
- Juillet 2016 : la directive *Network and Information Security* (NIS) du 6 juillet 2016 garantit la protection des services essentiels au sein de l'Union européenne.
- Octobre 2016 : la loi n° 2016-1321 du 7 octobre 2016 pour une République numérique (LRN) introduit de nouvelles dispositions relatives à l'*open data* et confirme les dispositions du RGPD en matière de protection des données personnelles.
- Mars 2022 : la loi n° 2022-309 du 3 mars 2022 pour la mise en place d'une certification de cybersécurité des plateformes numériques destinée au grand public (cyberscore) est promulguée.

Ce corpus juridique instaure une véritable responsabilité des collectivités et de leurs établissements publics, d'une part, en ce qui concerne leurs services numériques et, d'autre part, en ce qui concerne le traitement des données.

Outre la responsabilisation du secteur public, ces normes imposent à l'administration l'instauration d'une logique de prévention des risques, avec une mise en conformité permanente et volontaire de leurs systèmes de sécurité informatique.

▶ 3 - Les actions à mettre en œuvre pour sécuriser les téléservices, les données sensibles et les systèmes d'information d'importance vitale ou essentiels

Sécuriser les téléservices

Afin de se mettre en conformité avec le référentiel général de sécurité, il conviendra, d'une part, de procéder à une analyse des risques et à la définition des mesures de sécurité adaptées aux enjeux et aux menaces. Cela signifie que dès l'élaboration du projet de mise en place du téléservice, tout le contexte dans lequel évolue celui-ci devra être analysé ainsi que la vraisemblance, les conséquences et la gravité d'éventuels incidents de sécurité.

D'autre part, il conviendra de procéder à une homologation de sécurité du téléservice préalablement à sa mise en place. La décision d'homologation est prononcée pour 5 ans maximum et doit faire l'objet d'une révision à l'expiration de ce délai.

Afin d'aider les collectivités territoriales et leurs établissements dans cette démarche d'homologation, l'Anssi a publié un guide d'homologation en 9 étapes.

Enfin, un suivi opérationnel et des actions d'amélioration continue sont indispensables.

Veiller à la protection des données personnelles

Afin de répondre aux exigences du règlement général sur la protection des données, il est nécessaire :

- de nommer un délégué à la protection des données ;
- de mettre en place un registre des traitements ;
- d'analyser les effets d'un traitement susceptible de présenter un risque élevé pour les droits et les libertés des personnes concernées ;
- de mettre en place des clauses relatives à la protection des données personnelles avec

ses fournisseurs et sous-traitants ;
- de notifier les violations de données personnelles à la Commission nationale de l'informatique et des libertés (Cnil) au plus tard dans les 72 heures après avoir pris connaissance de la violation.

Protéger les systèmes d'information d'importance vitale ou essentiels

Il s'agit ici de répondre aux prescriptions de la loi n° 2013-1168 du 18 décembre 2013 relative à la programmation militaire et de la directive *Network and Information Security* en définissant une politique de sécurité des systèmes d'information dirigée par les principes directeurs suivants :

- confidentialité (seules les personnes habilitées ont accès aux données) ;
- disponibilité (rapidité d'accès aux informations) ;
- intégrité (assurance que les données n'ont pas été altérées) ;
- traçabilité (accès aux données qui sont conservées et exploitables).

Cela se traduit également par le fait de réaliser une cartographie des systèmes d'information et d'analyser les risques sur les activités d'importance vitale ou des services essentiels.

Les systèmes d'information doivent être également homologués et un audit de sécurité doit être mené.

▶ 4 - Les actions indispensables pour protéger son système d'information

Sensibiliser le personnel aux risques de cyberattaques

Il existe des leviers accessibles pouvant être actionnés afin de contrer les cyberattaques : il s'agit de déployer des actions de formation du personnel complétées par des mises en situation.

Les attaques des pirates aboutissent souvent du fait de la méconnaissance ou de l'ignorance des outils informatiques que les collaborateurs utilisent. Afin de remédier à cette méconnaissance, il est important de communiquer de façon régulière *via* des emails informatifs sur les possibilités de piratage mais aussi de former les équipes.

Les sujets essentiels sur la prévention sont :

- le téléchargement de fichiers et ses risques (le fait de ne pas télécharger des pièces jointes inconnues reçues par mail ou disponibles sur un site Internet non habituel) ;
- les mots de passe et authentifications sur les sites Internet (le fait de ne pas préenregistrer ses mots de passe) ;
- les réseaux sociaux et la confidentialité (ne pas divulguer des données sensibles) ;
- le comportement à adopter au télétravail (être vigilant à la navigation, aux téléchargements) ;
- la responsabilité de chacun sur son utilisation d'Internet et des emails (vérifier la provenance de l'email, apprendre à détecter les provenances suspectes).

La formation pourra être complétée de mises en situation avec la simulation de réception de mails suspects afin de vérifier le respect des consignes de sécurité par les collaborateurs. Un rappel des règles pourra être réalisé à cette occasion.

Procéder à la mise à jour régulière des outils informatiques

La mise à jour des outils informatiques est primordiale afin d'éviter les intrusions. En effet, cela permet d'empêcher les failles de sécurité connues et ferme la porte aux tentatives d'intrusion.

Des outils comme un serveur de gestion de type WSUS permettra la mise à jour de l'ensemble du parc informatique.

Protéger les équipements

La protection des équipements au sein des collectivités est essentielle et un système de chiffrage garantit une sécurité supplémentaire en cas de vol ou de piratage. Les cybercriminels ne pourront pas ainsi déchiffrer les données.

Installer un antivirus et un pare-feu sur le réseau et sur les postes

L'utilisation de l'antivirus est essentielle pour sécuriser les collectivités sur l'ensemble de leur parc informatique et pour détecter et éliminer l'ensemble des éléments malveillants des ordinateurs.

Le pare-feu (ou *firewall*) est primordial afin de garantir l'intégrité des flux de données transitant sur le réseau de la collectivité en entrées et en sorties.

Assurer la sauvegarde des données

La sauvegarde des données est la partie essentielle de la politique de préservation de l'intégrité du système d'information de la collectivité. Toutefois, elle est souvent négligée à tort !

Sans sauvegarde fonctionnelle, il existe un fort risque de perte des données et d'impossibilité de reprise de l'activité. Dans ce cadre, le risque de pertes financières est bien présent.

Pour éviter cela, des logiciels de sauvegarde existent. Ils permettent des sauvegardes en local et dans le *cloud* externalisé, car une sauvegarde en local ne garantit pas la perte de données.

Enfin, il est nécessaire de prévoir des tests réguliers de restauration de données afin de garantir le bon fonctionnement de votre sauvegarde et, de ce fait, l'intégrité de vos données.

Contrôler les accès des utilisateurs

Le contrôle d'accès des utilisateurs sur le serveur de données est nécessaire au sein d'un système d'information. Afin d'illustrer ce propos, prenons l'exemple du service petite enfance qui n'a pas à avoir accès aux données du service juridique et vice versa.

Une réflexion de fond est donc à mener concernant la mise en place d'un répertoire des données classées par contrôle d'accès en fonction des ressources, avec un respect absolu de celui-ci sur le long terme.

Définir des mots de passe uniques et complexes

Posséder un mot de passe trop simple va donner l'opportunité aux hackers d'accéder de façon rapide aux données des agents ainsi qu'à leurs applications professionnelles.

Aussi, il est essentiel d'utiliser des mots de passe complexes mélangeant des caractères alphanumériques et des caractères spéciaux, comportant au moins 12 caractères, voire 16 caractères idéalement. En effet, un mot de passe de 8 caractères composé de chiffres, majuscules, minuscules et caractères spéciaux sera piraté en 1 seconde (*source* : Hive Systems 2023).

De plus, une stratégie de changement de mot de passe avec une périodicité mensuelle est à adopter afin d'éviter la redondance des mots de passe. Pour cela, un gestionnaire de mots de passe peut être intégré au système d'information de la collectivité afin d'assurer leur gestion.

Enfin, une solution multifacteur (MFA) qui comprend l'envoi d'un SMS ou l'utilisation d'une clé de sécurité permettra d'améliorer la sécurité des connexions.

Faire preuve de vigilance sur la pratique des téléchargements

Le téléchargement d'applications est à éviter ainsi que le partage de fichiers extérieurs.

Il convient également d'examiner les mails reçus avec les pièces jointes. En effet, aujourd'hui, le phishing est l'une des principales sources de piratage.

Naviguer sur des sites sécurisés

Il est primordial de faire en sorte que chaque collaborateur ne navigue que sur des sites sécurisés. Aussi, il est nécessaire de ne pas se connecter sur des réseaux Wi-Fi publics qui sont souvent mal sécurisés. Il est conseillé de privilégier un réseau privé virtuel (VPN).

Souscrire à une assurance cyber

Contracter une assurance cybersécurité peut, dans certain cas et selon le piratage subi, couvrir une partie des frais engendrés par l'attaque et vous accompagner dans la gestion de cette crise sous réserve des garanties souscrites.

NOTRE CONSEIL

La principale faille en matière de sécurité informatique reste l'être humain. Les hackers se servent de la méconnaissance technique des collaborateurs afin d'atteindre leur but : s'immiscer dans votre système informatique. Aussi, il est essentiel de bien veiller à la sensibilisation et à l'information du personnel en n'hésitant pas à effectuer des procédures de rappel et tests.

ÉVITEZ LES ERREURS

- Ne cliquez jamais sur un lien contenu dans un mail qui ne vous concerne pas ou qui vous semble suspect.
- N'ouvrez jamais une pièce jointe inconnue.
- Ne donnez pas ou ne saisissez pas vos mots de passe sur des formulaires que vous ne connaissez pas.
- Vérifiez toujours le nom de domaine de votre destinataire (ex. : prenom.nom@**xxxx.com**).

FAQ

Que faire si vous avez cliqué sur un lien, rempli un formulaire sur Internet et donné votre mot de passe et que vous n'êtes pas certain de votre démarche ?

Contactez immédiatement votre service informatique car il convient d'agir vite, le temps de réaction est primordial.

Existe-t-il un site *via* lequel je peux obtenir des informations générales, des conseils, et émettre des signalements lorsque je suis victime d'une cyberattaque ?

Oui, le site Internet www.cybermalveillance.gouv.fr a pour missions d'assister les particuliers, les entreprises, les associations, les collectivités et les administrations victimes de cybermalveillance, de les informer sur les menaces numériques et les moyens de s'en protéger.

Il propose les services suivants : des e-sensibilisations, le partage de bonnes pratiques, une rubrique pour signaler une escroquerie ou un contenu illicite et une rubrique dédiée au dépôt de plainte suite à une cybermalveillance.

ALLER PLUS LOIN

Références juridiques

- Règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, et abrogeant la directive 95/46/CE (règlement général sur la protection des données)
- Directive (UE) 2016/1148 du Parlement européen et du Conseil du 6 juillet 2016 concernant des mesures destinées à assurer un niveau élevé commun de sécurité des réseaux et des systèmes d'information dans l'Union, dite « directive *Network and Information Security* » (NIS)
- Loi n° 2022-309 du 3 mars 2022 pour la mise en place d'une certification de cybersécurité des plateformes numériques destinée au grand public
- Loi n° 2016-1321 du 7 octobre 2016 pour une République numérique
- Loi n° 2013-1168 du 18 décembre 2013 relative à la programmation militaire pour les années 2014 à 2019 et portant diverses dispositions concernant la défense et la sécurité nationale

Sites Internet

- cyber.gouv.fr : site de l'Agence nationale de la sécurité des systèmes d'information, où consulter le guide d'homologation en 9 étapes
- www.cnil.fr : site de la Cnil, où consulter le *Guide de la sécurité des données personnelles*
- www.cert.ssi.gouv.fr : site du Centre gouvernemental de veille, d'alerte et de réponse aux attaques informatiques
- www.cybermalveillance.gouv.fr : site d'assistance et de prévention en sécurité numérique
- www.yeswehack.com/fr : exemple de plateforme de « bug bounty », lorsque les hackers éthiques viennent contribuer à la sécurité des systèmes informatiques

PARTENARIAT
GMF X WEKA

Retrouvez gratuitement tous les livres blancs et les replays des webconférences sur l'actualité :

OU

https://bit.ly/443IUqz

GMF WEKA .media .jobs .fr

L'accompagnateur au quotidien des décideurs publics

Depuis 40 ans, Weka met son savoir-faire au service des professionnels des collectivités territoriales et de la fonction publique.

Nous apportons des réponses pratiques et concrètes issues de l'expérience d'experts publics à leurs problématiques quotidiennes, dans les domaines d'intervention suivants :

- Marchés publics
- Finances & comptabilité
- Ressources humaines
- Services à la population
- Culture & communication
- Aménagement des territoires
- Gouvernance locale
- Éducation
- Action sociale
- Santé

.media
.jobs
.fr

Graphiste : Christian LE GALL
Éditrice : Alice LECOMTE

Éditions WEKA – Pleyad 1 – 39, boulevard Ornano 93288 Saint-Denis Cedex
Tél. : 01 53 35 17 17 – Fax : 01 53 35 17 01
Site internet : www.weka.fr