Sujet élaboré par une cellule pédagogique nationale

EXAMEN PROFESSIONNEL DE PROMOTION INTERNE D'INGÉNIEUR TERRITORIAL

SESSION 2022

ÉPREUVE DE PROJET OU D'ÉTUDE

ÉPREUVE D'ADMISSIBILITÉ :

L'établissement d'un projet ou étude portant sur l'une des options, choisie par le candidat lors de son inscription.

Durée : 4 heures
Coefficient : 5

SPÉCIALITÉ : INFORMATIQUE ET SYSTEMES D'INFORMATION

OPTION : RÉSEAUX ET TÉLÉCOMMUNICATIONS

À LIRE ATTENTIVEMENT AVANT DE TRAITER LE SUJET :

- Vous ne devez faire apparaître aucun signe distinctif dans votre copie, ni votre nom ou un nom fictif, ni initiales, ni votre numéro de convocation, ni le nom de votre collectivité employeur, de la commune où vous résidez ou du lieu de la salle d'examen où vous composez, ni nom de collectivité fictif non indiqué dans le sujet, ni signature ou paraphe.
- Sauf consignes particulières figurant dans le sujet, vous devez impérativement utiliser une seule et même couleur non effaçable pour écrire et/ou souligner. Seule l'encre noire ou l'encre bleue est autorisée. L'utilisation de plus d'une couleur, d'une couleur non autorisée, d'un surligneur pourra être considérée comme un signe distinctif.
- Le non-respect des règles ci-dessus peut entraîner l'annulation de la copie par le jury.
- Les feuilles de brouillon ne seront en aucun cas prises en compte.

Ce sujet comprend 43 pages dont 3 annexes.

Il appartient au candidat de vérifier que le document comprend le nombre de pages indiqué.
S'il est incomplet, en avertir le surveillant.

- Vous répondrez aux questions suivantes dans l'ordre qui vous convient, en indiquant impérativement leur numéro.
- Vous répondrez aux questions à l'aide des documents et de vos connaissances.
- Des réponses rédigées sont attendues et peuvent être accompagnées si besoin de tableaux, graphiques, schémas…
- Pour les dessins, schémas, cartes et plans, l'utilisation d'une autre couleur que le bleu ou le noir ainsi que l'utilisation de crayons de couleur, feutres, crayon de papier sont autorisées.

Vous êtes ingénieur territorial dans la commune d'Ingéville (100 000 habitants). Au sein de la Direction des Systèmes d'Information, vous occupez le poste de responsable technique à la tête d'une équipe de 3 personnes (un administrateur système, un administrateur réseau et télécom et un administrateur poste de travail). Vous avez en charge la gestion de l'équipe, l'architecture technique et la sécurité du Système d'Information (SI).

Le directeur doit apporter un éclairage à l'élu référent sur l'exposition au risque informatique pesant sur le SI de la commune. Il vous demande de lui fournir des éléments pour faire face à la menace et guider les futurs investissements.

Question 1 (4 points)

Au travers d'une note de synthèse à l'attention du DSI, dressez un constat des cyberattaques et les enjeux pour Ingéville.

Question 2 (6 points)

a) Quels systèmes sous la responsabilité de la commune pourraient être la cible de cyberattaque et quels sont les risques encourus ? (2 points)

b) Quelles peuvent être les conséquences de tels piratages pour les administrés d'Ingéville ? (2 points)

c) Citez les moyens de réduction possibles des risques que vous avez abordés. (2 points)

Question 3 (6 points)

Apportez, à l'aide de vos connaissances personnelles, une réponse technique à la problématique de sécurisation des réseaux informatiques de la commune ainsi qu'un schéma d'architecture général (à réaliser sur votre copie) montrant une évolution des annexes 1 et 2.

Question 4 (4 points)

a) Quelles sont les actions à mener en priorité consécutivement à une cyberattaque ? (2 points)

b) Proposez une organisation de crise adaptée à l'échelle d'Ingéville en réponse à la survenance d'un risque majeur. (2 points)

Liste des documents :

Document 1 : « La France risque-t-elle un Pearl Harbor cyber ? » - *challenges.fr* - 17 mai 2021 - 3 pages

Document 2 : « En Iran, une cyberattaque vise la centrale de Natanz » - *lemondeinformatique.fr* - 12 avril 2021 - 2 pages

Document 3 : « Les compétences "eau et assainissement" » - *collectivites-locales.gouv.fr* - consulté le 14 décembre 2021 - 7 pages

Document 4 : « Les fichiers d'état civil » - *cnil.fr* - 2 octobre 2019 - 2 pages

Document 5 : « Floride : le piratage d'un réseau d'eau potable tourne court grâce à la vigilance d'un employé » - *lci.fr* - 9 février 2021 - 2 pages

Document 6 : « Après le piratage informatique de la mairie de Douai, des données personnelles des habitants volées ? » - *francebleu.fr* - 14 avril 2021 - 1 page

Document 7 : « Cyberattaques : les communes de plus en plus victimes du rançonnage » - *Francetvinfo.fr* - 23 novembre 2020 - 1 page

Document 8 : « Cyberattaque à Angers : deux mois après, la police ne peut toujours pas dresser de PV » - *lci.fr* - 25 mars 2021 - 1 page

Document 9 : « Comment Colonial Pipeline a géré une attaque de ransomware » - *kaspersky.fr* - 17 mai 2021 - 2 pages

Document 10 : « Les données personnelles d'agents du Grand Annecy diffusées cinq mois après la cyberattaque » - *Lagazettedescommunes.com* - 19 mai 2021 - 1 page

Document 11 : « Comment se prémunir contre les rançongiciels » *Lagazettedescommunes.com* - 5 novembre 2020 - 3 pages

Document 12 : « Une cyberattaque coûte 550 000 euros à la ville de Chalon-sur Saône » - *Lagazettedescommunes.com* - 29 juillet 2021 - 2 pages

Document 13 : « Les RSSI des collectivités territoriales créent un réseau de partage » - *lemondeinformatique.fr* - 16 février 2021 - 1 page

Document 14 : « Le service d'assainissement des eaux d'Oloron-Sainte-Marie a été pris pour cible par des hackers » - *usine-digitale.fr* - 30 Septembre 2021 - 1 page

Document 15 : « Loi de programmation militaire 2019/2025 : Une protection accrue contre les attaques informatiques» - *datalegaldrive.com* - 6 mars 2019 - 3 pages

Document 16 : « 4 questions à vous poser pour bien choisir votre solution de gestion de crise» - *journaldunet.com* - 24 août 2021 - 3 pages

Liste des annexes :

Annexe 1 : « Réseau global simplifié » - *Ingéville* - 2021 - 1 page

Annexe 2 : *« Salle machine »* - *Ingéville* - 2021 - 1 page

Annexe 3 : « Le système d'Information de la commune » - *Ingéville* - 2021 - 1 page

Documents reproduits avec l'autorisation du C.F.C.

Certains documents peuvent comporter des renvois à des notes ou à des documents non fournis car non indispensables à la compréhension du sujet.

DOCUMENT 1

« La France risque-telle un Pearl Harbor cyber ? » - *Challenge.fr* - 17 mai 2021

Une cyberattaque a contraint Colonial Pipeline à stopper l'activité d'un oléoduc qui fournit 45% du carburant de la côte Est. Si elle protège plutôt bien ses industriels stratégiques, la France n'est pas à l'abri de ce genre de scénario.

Un site de Colonial Pipeline, dont un oléoduc stratégique a été bloqué par une cyberattaque

DRONE BASE

Pour les Etats-Unis, c'est l'humiliation de trop. Washington avait déjà dû faire face, depuis le début de l'année, à deux attaques majeures sur le front cyber: la découverte d'un logiciel espion - probablement d'origine russe- chez l'éditeur texan Solarwinds, fournisseur de grands groupes et d'agences fédérales américaines; et une cyberattaque massive contre la messagerie Exchange de Microsoft, attribuée à des hackers chinois, qui avait vu la compromission de données de dizaines de milliers de clients. La dernière attaque, identifiée le 7 mai, se révèle encore plus symbolique. Cette fois, c'est un pipeline stratégique de la côte Est des Etats-Unis qui a été mis hors service lors d'une attaque par rançongiciel contre son

propriétaire, la société Colonial Pipeline. La société a mis plusieurs jours pour redémarrer cet oléoduc, qui fournit 45% du carburant de la zone.

Ces trois attaques réussies en à peine six mois interpellent les spécialistes. Selon le classement du Belfer Center, un laboratoire de recherche rattaché à Harvard, les Etats-Unis étaient, en 2020, la première puissance cyber mondiale, devant la Chine, le Royaume-Uni, la Russie, les Pays-Bas et la France. "Quand on voit les moyens cyber gigantesques mis sur la table par les Etats-Unis, cette série d'attaques est une véritable humiliation, estime Bernard Barbier, fondateur du cabinet BBCyber et ancien directeur technique de la DGSE. Avec les attaques contre Solarwinds et Microsoft notamment, la Russie et la Chine ont montré qu'elles pouvaient toucher des acteurs américains stratégiques."

Porosité américaine

Comment expliquer la porosité des défenses cyber américaines? "Malgré leur puissance financière, les Etats-Unis ont du retard sur la France sur la protection de leurs acteurs stratégiques, indique Jacques de la Rivière, patron de la pépite cyber française Gatewatcher. Leur agence de cybersécurité, la CISA (Cybersecurity and Infrastructure Security Agency), l'équivalent de l'ANSSI, n'a été créée qu'en 2018." Le gendarme français du cyber, l'ANSSI (Agence nationale de la sécurité des systèmes d'information), avait quant à lui été créé en 2009. Il a, depuis, imposé aux entreprises et administrations stratégiques, dites OIV (opérateurs d'importance vitale), des obligations sur leur protection cyber.

Les quelques 220 OIV, dont la liste exacte est classifiée (industriels et administrations dans l'énergie, l'eau, la défense, les transports, la santé, l'alimentation, l'espace...), doivent ainsi se conformer à une vingtaine de règles strictes dont l'ANSSI vérifie le respect. Ils doivent par exemple déployer des sondes de détection de cyber-attaques qualifiées par l'agence (Gatewatcher, Thales) dans leurs serveurs les plus stratégiques. Ils doivent cartographier et sécuriser leurs systèmes d'information d'importance vitale (SIIV), et les points d'importance vitale (PIV), les établissements et installations essentielles à la vie de la nation. Ils doivent disposer d'un SOC (Security Operation Center), un dispositif de surveillance qui permet de détecter des incidents informatiques, qu'ils peuvent créer en interne ou déléguer à un prestataire qualifié.

Ces obligations, issues de la loi de programmation militaire votée fin 2013, ont fait de la France un des précurseurs de la protection cyber des acteurs stratégiques, avec plusieurs années d'avance sur les Etats-Unis. "Le système américain est, historiquement, plus libéral, avec moins d'obligations réglementaires et une place plus grande à la responsabilité des entreprises", explique Bernard Barbier. La CISA, équivalent de l'ANSSI, avait connu des début laborieux. Donald Trump avait limogé fin 2020 son premier patron, Chris Krebs, pour avoir démenti ses accusations de fraude électorale.

"Pearl Harbor" cyber possible en France

Pour autant, la France aurait tort de se croire à l'abri d'un scénario type Colonial Pipelines. "En ce qui concerne la menace pour la France, celle d'un 'Pearl Harbour' (cyber, NDLR) est possible, évidemment", prévenait en mars 2020 devant la commission de la défense de l'Assemblée nationale le patron du commandement de la cyberdéfense (Comcyber), le général Didier Tisseyre. Comme Guillaume Poupard, directeur général de l'ANSSI, le général Tisseyre mettait notamment en garde contre des "implants" informatiques, des logiciels malveillants prépositionnés dans des serveurs stratégiques par des groupes de hackers plus ou moins affiliés à des Etats (Russie, Chine...).

Ces "agents dormants cyber" peuvent être activés à tout moment par des puissances étrangères. Les cyberattaquants "préparent une sorte de boîte à outils, un panel d'options qui pourraient être présentées à leurs autorités, expliquait le directeur général de l'ANSSI Guillaume Poupard en 2018. La logique, c'est: 'Je place des charges explosives sous le pont de l'Alma, au cas où un jour on me demande de faire sauter le pont de l'Alma.'" Devant le Sénat fin 2018, le patron de l'ANSSI était encore plus explicite: "Nous avons détecté des cas très inquiétants dans l'année écoulée, notamment une tentative d'intrusion de systèmes de cartographie liés au secteur de l'énergie, qui n'avait qu'un but: la préparation d'actions violentes futures, indiquait-il. Imaginez les conséquences sur le fonctionnement d'un pays d'une attaque sur les réseaux de distribution d'énergie. Ne nous leurrons pas, tel est l'objectif d'un certain nombre d'équipes, de pays, d'armées, pour anticiper les conflits de demain et être prêts à agir si l'ordre leur en est donné."

Rançon payée

La France fait clairement partie des cibles privilégiées par les attaquants russes. Début 2018, comme dévoilé par *L'Express*, un malware avait été détecté par la DGSE dans un ferme éolienne française. Ce programme informatique devait servir de porte d'entrée vers le réseau de distribution électrique d'Enedis. Les experts de la direction technique de la DGSE avaient attribué l'attaque au groupe russe APT29, ou Cozy Bear, réputé proche des services de renseignement russes. Trois ans plus tard, ce même groupe a été accusé par les Etats-Unis d'être à l'origine de l'attaque sur l'éditeur Solarwinds, dont les départements américains de la Défense, du Trésor et du Commerce figurent parmi les plus grands clients.

Des pirates russes seraient également, selon la Maison Blanche, à l'origine de l'attaque contre le pipeline de Colonial Pipeline. "Nous ne pensons pas que le gouvernement russe était impliqué dans cette attaque, mais nous avons de bonnes raisons de croire que les criminels responsables de ces attaques vivent en Russie", indiquait le président Joe Biden le 13 mai. Humiliation supplémentaire pour les Etats-Unis: Colonial Pipeline a rapidement payé la rançon demandée par les pirates. Selon l'agence Bloomberg, celle-ci s'est élevée à près de 5 millions de dollars.

DOCUMENT 2

« En Iran, une cyberattaque vise la centrale de Natanz » - *lemondeinformatique.fr* - 12 avril 2021

Déjà ciblée par un acte de sabotage en juillet dernier, la centrale d'enrichissement d'uranium de Natanz aurait cette fois fait les frais d'une cyberattaque. Cette-dernière est intervenue dimanche après l'inauguration officielle des dernières centrifugeuses plus performantes.

L'Iran a lancé sur le site de Natanz des tests sur des centrifugeuses d'enrichissement d'uranium IR-9. (crédit : Euronews)

Infecté par Stuxnet en 2010 puis en 2018 par un de ses variants, le site nucléaire de Bushehr n'est pas le seul en Iran à faire l'objet de cyberattaques. Egalement régulièrement visée depuis par des actions de sabotage, la centrale d'enrichissement nucléaire de Natanz (Shahid Ahmadi Roshan) en Iran a été prise pour cible ce dimanche. Si son origine n'a pas été confirmée, il semblerait bien que l'on ait encore une fois affaire à une cyberattaque. Le site de Natanz est le premier site d'enrichissement primaire en uranium d'Iran.

Cette intrusion intervient moins d'un an après la provocation d'un incident ayant débouché sur l'incendie d'une partie du site en juillet 2020. Cette présente attaque survient quelques heures après l'inauguration, d'après The Guardian, de 164 nouvelles centrifugeuses IR-6 permettant d'accroitre les

capacités de l'Iran en matière d'enrichissement d'uranium à des fins militaires. Et également de l'annonce de tests sur des centrifugeuses IR-9 pour enrichir plus rapidement et dans des volumes plus importants, de l'uranium. Cet incident intervient au moment où des efforts diplomatiques ont repris entre les Etats-Unis et l'Iran pour revenir sur l'accord nucléaire de 2015 rejeté par l'administration Trump.

L'Iran pourrait réagir face à Israël

Suite à ce sabotage, l'Iran a qualifié cette action de terrorisme nucléaire. Il semble toutefois qu'aucune fuite radioactive n'a résulté de cette attaque. Suite à cet incident, Behrouz Kamalvandi, porte-parole de l'organisation de l'énergie atomique a indiqué que ces dommages qui n'ont pas entrainé de conséquences humaines ni de pollution, a perturbé une partie du réseau de distribution d'électricité.

Le vice-président iranien et chef de l'Organisation de l'énergie atomique, Ali Akbar Salehi, a lui condamné ce qu'il a appelé « un acte terroriste » visant l'installation souterraine de Natanz, et a souligné que l'Iran se réserve le droit de réagir. L'attribution de cette cyberattaque - dont les contours restent plus que troubles - pourrait être d'origine israélienne, pilotée par les services secrets du Mossad. Des sources interrogées par News Today ont indiqué que les dommages causés à l'installation iranienne sont plus importants que ceux indiqués par l'Iran et de nombreuses centrifugeuses de différents types ont été affectés.

DOCUMENT 3

« Les compétences "eau et assainissement" » - *collectivites-locales.gouv.fr* – consulté le 14 décembre 2021 -

Le service public d'eau potable

En application de l'article L. 2224-7 du code général des collectivités territoriales (CGCT), constitue un service public d'eau potable *« tout service assurant tout ou partie de la production par captage ou pompage, de la protection du point de prélèvement, du traitement, du transport, du stockage et de la distribution d'eau destinée à la consommation humaine »*.

La compétence obligatoire des communes : la distribution d'eau potable

L'article L. 2224-7-1 du CGCT pose le principe d'une compétence obligatoire des communes en matière de distribution d'eau potable.

Ce principe a été assorti de l'obligation d'arrêter un schéma de distribution d'eau potable en vue de délimiter les zones desservies par le réseau de distribution et donc *in fine* les zones dans lesquelles une obligation de desserte s'applique. Dans ces zones, la commune ne peut refuser le branchement sauf dans des cas très particuliers tels qu'une construction non autorisée ou de façon plus générale en méconnaissance des règles d'urbanisme.

Par ailleurs, les distributions municipales d'eau potable doivent s'assurer du respect des exigences fixées par l'article R. 1321-2 du code de la santé publique pour les eaux destinées à la consommation humaine (limites de qualité, etc.).

Par ailleurs, sauf dispositions contraires du code de l'urbanisme ou du règlement sanitaire départemental, aucune règle générale n'impose aux propriétaires le raccordement des immeubles au réseau public de distribution d'eau potable. Une habitation peut donc disposer d'une alimentation propre (régime de déclaration auprès du maire de la commune).

Les compétences facultatives des communes : la production, le transport et le stockage d'eau potable

La production d'eau potable, son transport et son stockage sont des compétences facultatives des communes.

Les autres acteurs éventuellement compétents en matière d'eau potable

L'article L. 2224-7-1 du CGCT précise que « les compétences en matière d'eau potable assurées à la date du 31 décembre 2006 par des départements ou des associations syndicales créées avant cette date ne peuvent être exercées par les communes sans l'accord des personnes concernées ».

Le service public d'assainissement

En amont de l'exercice de la compétence assainissement, les communes ou les EPCI délimitent :

- les zones relevant de l'assainissement collectif ;
- les zones relevant de l'assainissement non collectif ;

- les zones où des mesures doivent être prises pour limiter l'imperméabilisation des sols et pour assurer la maîtrise du débit et de l'écoulement des eaux pluviales et de ruissellement ;

- les zones où il est nécessaire de prévoir des installations pour assurer la collecte, le stockage éventuel et, en tant que de besoin, le traitement des eaux pluviales et de ruissellement lorsque la pollution qu'elles apportent au milieu aquatique risque de nuire gravement à l'efficacité des dispositifs d'assainissement.

Article L. 2224-10 du CGCT

Les compétences obligatoires des communes

L'article L. 2224-8 du CGCT pose le principe d'une compétence obligatoire des communes en matière d'assainissement. Cette compétence comprend :

- Au titre de l'assainissement collectif, la mission de « contrôle des raccordements au réseau public de collecte, la collecte, le transport et l'épuration des eaux usées, ainsi que l'élimination des boues produites ».

L'article L. 1331-1 du code de la santé publique impose le raccordement des immeubles aux réseaux publics de collecte disposés pour recevoir les eaux usées domestiques dans un délai de deux ans à compter de la mise en service du réseau.

- Au titre de l'assainissement non collectif, une mission de contrôle des installations d'assainissement non collectif à travers les services publics d'assainissement non collectif (SPANC) :

Pour les installations existantes, le service devait procéder à la vérification du fonctionnement et de l'entretien de toutes les installations d'assainissement non collectif avant le 31décembre 2012 puis mettre en place un contrôle de ces installations selon une périodicité maximale de 10 ans ;

Pour les installations neuves ou à réhabiliter, le SPANC doit procéder à un examen préalable de la conception de l'installation puis à la vérification de l'exécution (arrêté du 7 mars 2012 modifiant l'arrêté du 7 septembre 2009 fixant les prescriptions techniques applicables aux installations d'assainissement non collectif recevant une charge brute de pollution organique inférieure ou égale à 1.2 kg/j de DBO5) ;

Délivrer au demandeur d'un permis de construire un document attestant de la conformité du projet d'installation d'assainissement non collectif au regard des prescriptions réglementaires.

Les compétences facultatives des communes en matière d'assainissement non collectif

En matière d'assainissement non collectif, les communes peuvent, à titre facultatif et sur demande du propriétaire, assurer l'entretien, les travaux de réalisation et de réhabilitation des installations, le traitement des matières de vidange et fixer des prescriptions techniques pour les études des sols ou le choix de la filière, en vue de l'implantation ou de la réhabilitation d'une installation.

La mise en œuvre des services publics d'eau et d'assainissement

Mode de gestion

Le choix du mode de gestion relève du principe de libre administration des collectivités territoriales.

La commune ou l'EPCI peut exploiter le service en régie, c'est-à-dire le gérer directement par ses propres moyens en personnel et en matériel, et passer, le cas échéant, un ou plusieurs marchés publics pour l'exécution du service.

La commune peut aussi opter pour la gestion indirecte, c'est-à-dire confier la globalité de l'exécution du service à un tiers sous la forme d'une convention de délégation de service public (concession, affermage, régie intéressée).

Article L. 1411-1 et suivants et articles L. 2224-11-3 et suivants du CGCT

Le règlement de service

"Les communes et les groupements de collectivités territoriales, après avis de la commission consultative des services publics locaux, établissent, pour chaque service d'eau ou d'assainissement dont ils sont responsables, un règlement de service définissant, en fonction des conditions locales, les prestations assurées par le service ainsi que les obligations respectives de l'exploitant, des abonnés, des usagers et des propriétaires".

Article L. 2224-12 du CGCT

Le règlement du service régit les relations entre les différents acteurs du service public de l'eau ou de l'assainissement, et ceci dans le respect des dispositions législatives applicables.

C'est un acte administratif, composé d'un ensemble de dispositions à caractère réglementaire. Il est également considéré comme faisant partie intégrante du contrat d'abonnement dont il constitue des conditions générales.

Le rapport annuel sur le prix et la qualité du service public d'eau potable et du service public d'assainissement

Le rapport sur le prix et la qualité du service public (RPQS) est un document produit tous les ans permettant de rendre compte aux usagers du prix et de la qualité du service rendu pour l'année écoulée. C'est un élément clé dans la mise en œuvre locale de la transparence et de la gouvernance des services d'eau et d'assainissement.

Le maire présente au conseil municipal, ou le président de l'établissement public de coopération intercommunale présente à son assemblée délibérante, des rapports annuels sur le prix et la qualité des services publics d'eau potable et d'assainissement destinés notamment à l'information des usagers Il comprend des indicateurs techniques, financiers et de performance.

Articles L. 2224-5 et D. 2224-1 à D. 2224-5 du CGCT

Le maire d'une commune ou le président d'un EPCI qui exerce à la fois les compétences en matière d'eau potable et d'assainissement peut présenter un rapport annuel unique.

Ce rapport est présenté au plus tard six mois après la clôture de l'exercice concerné.

Dans les communes de 3 500 habitants et plus, le rapport annuel est mis à la disposition du public. En outre, un exemplaire est adressé au préfet, pour information.

Le maire doit communiquer le rapport à la commission consultative des services publics locaux (CCSPL), pour examen.

Article L. 1413-1 du CGCT

Par ailleurs, la commune a la possibilité de saisir les données du RPQS sur le portail de l'observatoire national des services publics d'eau et d'assainissement. Il s'agit d'une base de données nationale des prix de l'eau et des performances des services publics d'eau et d'assainissement alimentée par les collectivités après contrôle et validation par les services de l'État. Cet observatoire est un outil de pilotage destiné aux communes et à leurs groupements, permettant de suivre l'évolution de leurs services d'une année sur l'autre, et de comparer leurs performances avec d'autres services. En outre, à l'issue de la saisie des données, la commune peut éditer un RPQS pré-renseigné.

Le descriptif détaillé des réseaux d'eau et d'assainissement

La commune devait établir avant la fin de l'année 2013 un descriptif détaillé des ouvrages de transport et de distribution d'eau potable, qui est intégré au schéma de distribution d'eau potable. Il s'agit d'inciter la commune à adopter une gestion patrimoniale des réseaux, et notamment de limiter les pertes d'eau dans les réseaux de distribution.

La commune devait également établir avant la fin de l'année 2013 un schéma d'assainissement collectif comprenant un descriptif détaillé des ouvrages de collecte et de transport des eaux usées.

Ces descriptifs doivent être régulièrement mis à jour.

Articles L. 2224-7-1, L. 2224-8 et D. 2224-5-1 du CGCT

Lorsque les pertes d'eau dans les réseaux de distribution dépassent les seuils fixés par décret, un plan d'actions et de travaux doit être engagé (décret n° 2012-97 du 27 janvier 2012 relatif à la définition d'un descriptif détaillé des réseaux des services publics de l'eau et de l'assainissement et d'un plan d'actions pour la réduction des pertes d'eau du réseau de distribution d'eau potable). A défaut, une majoration de la redevance pour prélèvement sur la ressource en eau est appliquée.

Article D. 2224-5-1 du CGCT et articles D213-48-14-1, D213-74-1 et D213-75 du code de l'environnement

La possibilité de verser une subvention au fonds de solidarité pour le logement (FSL)

Les services publics d'eau et d'assainissement peuvent attribuer une subvention au FSL afin de contribuer au financement des aides relatives au paiement des fournitures d'eau ou des charges collectives, dans la limite de 0,5% des montants hors taxes des redevances d'eau ou d'assainissement perçues.

Fuites anormales d'eau potable

Le III *bis* de l'article L. 2224-12-4 prévoit que le service d'eau potable informe l'occupant d'un local d'habitation de l'augmentation anormale du volume d'eau consommé.

L'abonné n'est pas tenu au paiement de la part de la consommation anormale s'il présente au service une attestation d'une entreprise de plomberie indiquant qu'il a fait procéder à la réparation d'une fuite sur ses canalisations.

Par ailleurs, à défaut de l'information de la part du service, l'abonné n'est pas tenu au paiement de la part de la consommation anormale.

Il convient de se référer également à l'article R. 2224-20 du CGCT.

Le financement des services publics d'eau et d'assainissement

Les services publics d'eau potable et les services publics d'assainissement sont des services publics industriels et commerciaux (SPIC) dont le financement est assuré par les redevances perçues auprès des usagers pour le service rendu

Articles L. 2224-11 et L. 2224-12-3 du CGCT

Un budget spécialisé et équilibré

Un financement par un système de redevance implique d'équilibrer le budget en recettes et en dépenses et de spécialiser le budget du service. Les recettes générées pour l'activité devant en couvrir les dépenses, aucune subvention du budget général de la commune ne doit venir abonder le service (article L. 2224-1 et suivants et article L. 2224-12-3 du CGCT). Toute subvention est en effet interdite au profit des SPIC. Toutefois :

- il existe trois exceptions, vérifiées de façon stricte par le juge, comme celle visant à éviter une augmentation excessive des tarifs liée à la réalisation d'investissements massifs ;
- cette règle ne s'applique pas aux services d'eau et d'assainissement des communes de moins de 3 000 habitants et des établissements publics de coopération intercommunale (EPCI) dont aucune commune membre n'a plus de 3 000 habitants.

Par ailleurs, le service de distribution d'eau et le service d'assainissement constituent deux activités distinctes qui sont retracées chacune dans un budget distinct. Toutefois, les communes de moins de 3 000 habitants et les EPCI dont aucune commune membre n'a plus de 3 000 habitants peuvent établir un budget unique de ces services s'ils sont soumis aux mêmes règles d'assujettissement à la taxe sur la valeur ajoutée et si leur mode de gestion est identique.

La fixation des redevances

Les redevances d'eau

Toute fourniture d'eau potable fait l'objet d'une facturation, à l'exception des consommations d'eau des bouches et poteaux d'incendie placés sur le domaine public.

Article L. 2224-12-1 du CGCT

Le montant de la redevance est fixé par le conseil municipal ou l'organe délibérant de l'EPCI compétent.

La redevance comprend une part proportionnelle et *peut* comprendre une part fixe.

Article L. 2224-12-4 du CGCT

La part proportionnelle est déterminée en fonction du volume réellement consommé par l'abonné, soit sur la base d'un tarif uniforme au mètre cube, soit sur la base d'un tarif progressif.

A titre exceptionnel, la commune peut fixer une tarification forfaitaire, après autorisation du préfet de département. Elle peut également, sous certaines conditions, établir un tarif dégressif.

La part fixe, facultative, correspond aux charges fixes du service et aux caractéristiques du branchement, notamment du nombre de logements desservis. En application de l'arrêté interministériel du 6 août 2007 relatif à la définition des modalités de calcul du plafond de la part de la facture d'eau non proportionnelle au volume d'eau consommé, le montant maximal de cet abonnement ne peut dépasser, par logement desservi et pour une durée de douze mois, tant pour

l'eau que pour l'assainissement, 30 % du coût du service pour une consommation d'eau de 120 mètres cubes, et 40 % pour les communes touristiques.

La commune peut définir des tarifs de l'eau par catégories d'usagers telle que celle des *« ménages, occupants d'immeubles à usage principal d'habitation »* (article L. 2224-12-1du CGCT). Par ailleurs, les différenciations tarifaires par catégories d'usagers sont admises dans les limites définies par la jurisprudence relative au principe d'égalité des usagers devant le service public (différence de situation ou motif d'intérêt général). Toutefois, les discriminations tarifaires entre résidents permanents et résidents secondaires sont jugées illégales, dès lors qu'elles ne trouvent leur justification ni dans la différence de situation existant entre ces deux catégories d'usagers ni dans aucune nécessité d'intérêt général en rapport avec les conditions d'exploitation du service.

CE, 28 avril 1993, Commune de Coux

En revanche, des tarifs différents peuvent être définis selon les périodes de l'année dans les communes où l'équilibre entre la ressource et la consommation d'eau est menacé de façon saisonnière.

IV de l'article L. 2224-12-4 du CGCT

Les redevances d'assainissement

Tout service public d'assainissement, quel que soit son mode d'exploitation, donne lieu à la perception d'une redevance.

Article R. 2224-19 et suivants du CGCT

Le conseil municipal ou l'organe délibérant de l'établissement public compétent institue la redevance pour la part du service qu'il assure et en fixe le tarif.

Lorsque le service d'assainissement concerne à la fois l'assainissement collectif et l'assainissement non collectif, deux redevances distinctes sont instituées.

La redevance d'assainissement collectif

La redevance d'assainissement collectif comprend une partie variable et, le cas échéant, une partie fixe.

Article R. 2224-19-2 et suivants du CGCT

La partie variable est déterminée en fonction du volume d'eau prélevé par l'usager sur le réseau public de distribution ou sur toute autre source, dont l'usage génère le rejet d'une eau usée collectée par le service d'assainissement.

Toutefois, lorsque la consommation d'eau est calculée de façon forfaitaire, la redevance d'assainissement peut également être calculée forfaitairement ;

La partie fixe est calculée pour couvrir tout ou partie des charges fixes du service d'assainissement. En application de l'arrêté interministériel du 6 août 2007 relatif à la définition des modalités de calcul du plafond de la part de la facture d'eau non proportionnelle au volume d'eau consommé, le montant maximal de cet abonnement ne peut dépasser, par logement desservi et pour une durée de douze mois, tant pour l'eau que pour l'assainissement, 30 % du coût du service pour une consommation d'eau de 120 mètres cubes, ou 40 % pour les communes touristiques.

La redevance d'assainissement non collectif

La redevance d'assainissement non collectif comprend une part destinée à couvrir les charges de contrôle (compétence obligatoire de la commune) et, le cas échéant, une part destinée à couvrir les charges d'entretien des installations (compétence facultative de la commune).

Article R. 2224-19-5 du CGCT

La part représentative des opérations de contrôle est calculée en fonction de critères tenant compte notamment de la situation, de la nature et de l'importance des installations. Ces opérations peuvent donner lieu à une tarification forfaitaire ;

La part représentative des prestations d'entretien n'est due qu'en cas de recours au service d'entretien par l'usager. Les modalités de tarification doivent tenir compte de la nature des prestations assurées.

Par ailleurs, l'article R. 2224-19-11 du CGCT dispose que *« le produit des sommes exigibles au titre du troisième alinéa de l'article L. 1331-1* (somme perçue auprès des propriétaires des immeubles raccordables mais non raccordés) *et des articles* L. 1331-2 (remboursement des frais de branchement), L. 1331-3, L. 1331-6, L. 1331-7 (participation pour le financement de l'assainissement collectif), L. 1331-8 *et* L. 1331-10 *du code de la santé publique s'ajoute au produit des redevances ainsi qu'aux autres recettes du service d'assainissement, notamment celles correspondant aux aides et primes d'épuration versées par les agences de l'eau, pour être affecté au financement des charges de ce service »*.

L'exercice intercommunal des compétences "eau et assainissement"

L'eau et l'assainissement constituent des compétences majeures des EPCI à fiscalité propre qui interviennent soit dans le cadre de leur propre périmètre, soit en s'associant à d'autres partenaires publics (communes, EPCI) au sein de syndicats mixtes.

L'eau est une compétence obligatoire des métropoles (article L. 5217-2 du CGCT) et des communautés urbaines (article L. 5215-20 du CGCT) et une compétence optionnelle des communautés d'agglomération (article L. 5216-5 du CGCT).

L'assainissement est une compétence obligatoire des métropoles (article L. 5217-2 du CGCT) et des communautés urbaines (article L. 5215-20 du CGCT) et une compétence optionnelle des communautés d'agglomération (article L. 5216-5 du CGCT). Les communautés de communes peuvent choisir à titre optionnel d'exercer *"tout ou partie de l'assainissement"* (article L. 5214-16 du CGCT), contrairement aux communautés de communes éligibles à la DGF bonifiée qui sont pour leur part tenues d'exercer intégralement l'assainissement collectif et non collectif lorsque ce bloc de compétences est choisi à titre optionnel (article L. 5214-23-1 du CGCT).

Les fichiers d'état civil - *Cnil.fr*

02 octobre 2019

La tenue des registres d'état civil constitue une obligation pour les maires. La CNIL rappelle les bonnes pratiques indispensables pour protéger au mieux les données personnelles des citoyens.

Suivant le mouvement de dématérialisation de l'état civil, la plupart des communes recourent à des applications informatiques pour traiter les données de l'état civil, en particulier dans le cadre de la numérisation des actes ou la mise en place de téléservices permettant aux administrés d'effectuer en ligne certaines démarches administratives.

Une utilisation des données strictement limitée

Les données personnelles enregistrées par les services d'état civil, à l'occasion de l'établissement ou de l'actualisation d'un acte, ne doivent être utilisées **que pour l'accomplissement des missions dont sont investis les maires en leur qualité d'officier de l'état civil**. Ces données ne peuvent être communiquées qu'aux destinataires habilités à en connaître (administrations, délégataires ou particuliers qui en font la demande) en vertu de dispositions légales, dans les conditions et pour les finalités prévues par celles-ci.

La publication dans la presse des naissances, mariages et décès

Les données personnelles enregistrées aux fins d'inscription d'un acte sur le registre de l'état civil ne peuvent être utilisées par les élus municipaux à des fins de message de félicitations ou de condoléances ou publiées dans la presse que si, au moment de l'établissement de l'acte, **les personnes concernées ont donné leur accord** à ce message personnalisé ou à cette publication. Les informations collectées pour ces seules fins ne peuvent être ni conservées ni alimenter un fichier permanent.

La formule suivante peut être adoptée pour figurer sur les documents distribués aux personnes accomplissant des démarches relatives à l'état civil :

> « *La mairie de […] vous propose de faire part de la naissance de votre enfant, de votre mariage, ou du décès de votre proche dans le bulletin municipal. Afin de respecter votre vie privée, cette diffusion nécessite votre accord.*
>
> *M., Mme […]* (Nom, Prénom) *accepte qu'une information relative à l'événement d'état civil déclaré ce jour soit publiée dans le bulletin municipal.*
>
> *Le […]* (date) »

L'information des personnes et le respect de leurs droits

Les administrés doivent être informés des traitements de leurs données d'état civil. Le RGPD renforce l'obligation d'information à l'égard des personnes dont les données sont traitées. Doivent ainsi être portés à leur connaissance :

- le nom et les coordonnées de la commune qui traite les données ;
- la finalité du traitement des données (établissement, conservation, mise à jour et délivrance des actes de l'état civil) et sa base juridique (dispositions du code civil relatif aux actes de l'état civil, en particulier l'article 40) ;
- le caractère obligatoire du recueil des données ;
- les destinataires du traitement tels que prévus par les textes (service municipal de l'état civil, INSEE, etc.) ;
- la durée de conservation des données ;
- les droits de l'administré ;
- les coordonnées du délégué à la protection des données ;
- le droit d'introduire une réclamation auprès de la CNIL.

De plus, les collectivités doivent garantir aux personnes concernées l'exercice facile et effectif de leurs droits d'accès et de leur droit de rectification, exercé dans les conditions définies par les textes en vigueur en matière d'état civil.

Les fichiers d'état civil répondant à une obligation légale, **le droit d'opposition ne s'applique pas**.

La sécurité des données

Les actes de l'état civil sont établis sur papier, selon des procédés manuels ou informatisés (mais obligatoirement signés de façon manuscrite). Ils sont inscrits, dans chaque commune, sur un ou plusieurs registres tenus en double exemplaire.

Ces registres et les données qu'ils contiennent doivent être conservés dans des conditions **garantissant leur sécurité** (confidentialité, intégrité et disponibilité) **et le respect des dispositions légales applicables** (par ex. celles du décret du 6 mai 2017 relatif à la gestion informatique de l'état civil).

Ainsi, lorsqu'une commune met en place un traitement automatisé pour l'établissement, la mise à jour ou la numérisation des actes, elle peut déléguer l'hébergement de ses données ou d'une sauvegarde de celles-ci à tout organisme public (département, région, EPCI…). Hormis les cas des communes nouvelles, des communes fusionnées et des communes comportant des divisions administratives, toute utilisation mutualisée du traitement doit garantir que **chaque commune n'a accès qu'aux données des actes dont elle est responsable**.
La commune, ou le délégataire avec l'accord de la commune, peut également faire appel à un organisme privé **à la condition que celui-ci soit établi en France** et que **l'hébergement et la sauvegarde des données soient réalisés sur le territoire national**. Dans ce cas, seule la commune, ou son délégataire, a accès au traitement, aux données associées et à leurs infrastructures d'hébergement.

Enfin, en application du RGPD, en cas de recours à un sous-traitant, notamment pour une prestation d'hébergement, un contrat précisant les conditions de la mise en œuvre des traitements de données personnelles faisant l'objet de cette sous-traitance, ainsi que les obligations de chacune des parties, doit être établi.

La durée de conservation des données

Les registres sont clos et arrêtés par l'officier de l'état civil à la fin de chaque année. Un des exemplaires est déposé aux archives de la commune, l'autre est versé au greffe du tribunal de grande instance dans le mois de leur clôture, sauf en cas de mise en place d'une gestion informatisée répondant aux caractéristiques fixées par le décret de 2017, qui dispense d'élaborer les registres en double exemplaire.

L'exemplaire déposé aux archives de la commune est conservé dans les conditions prévues par le code du patrimoine, comme pour les tables décennales (articles L.212-11 et L.212-12). L'exemplaire déposé au greffe du tribunal de grande instance est **conservé pendant un délai de soixante-quinze ans** avant versement aux archives départementales.

Effectuées sur place, par courrier ou par téléservice, les demandes d'actes (dont le contenu est également précisé par le décret de mai 2017), ainsi que les pièces justificatives pouvant être légitimement sollicitées en cas de doute quant à l'identité ou la qualité du demandeur, sont pour leur part **conservées pendant une durée d'un an** à des fins de gestion d'un éventuel contentieux.

La communication des données de l'état civil

Les actes de naissance, les actes de reconnaissance et les actes de mariage, ainsi que les registres de l'état civil qui les contiennent, datant de moins de soixante-quinze ans, ne peuvent être directement consultés que par les agents de l'État habilités à cet effet et les personnes munies d'une autorisation écrite de l'administration des archives. Au-delà de ce délai de soixante-quinze ans, l'accès de toute personne à ces actes et registres est régi par le code du patrimoine.

Le contenu et les conditions de délivrance de copies intégrales et d'extraits d'actes sont fixés par le décret de mai 2017. **Toute personne peut obtenir communication d'extraits d'actes de naissance et de mariage sans indication de la filiation, ainsi que des copies intégrales des actes de décès**, sauf lorsque la communication des informations y figurant est de nature à porter atteinte, compte tenu des circonstances du décès, à la sécurité des personnes désignées dans l'acte.

Ce décret prévoit également que des copies intégrales de ces actes puissent par ailleurs être délivrées à certains professionnels ou administrations (par exemple les généalogistes, l'INSEE ou les services de protection maternelle et infantile du conseil départemental), en vertu de réglementations spécifiques et dans le respect de certaines conditions.

En application du CRPA, les tables annuelles et décennales d'état civil sont, dès leur élaboration, librement communicables à toute personne qui les demande, à condition qu'elles ne comprennent pas d'autres données personnelles que le nom des personnes concernées et la date ou le numéro de l'acte (articles L311-1 et L311-6). Les autres mentions, s'il en existe, qui relèvent de la vie privée des personnes intéressées (ex. : noms et prénoms des parents pouvant figurer dans les tables décennales de naissance), ne sont communicables qu'à ces dernières et devront donc, jusqu'à l'expiration d'un délai de 50 ans à compter du dernier acte qui y est transcrit (article L213-2 du code du patrimoine), être occultées avant toute communication des tables à des tiers.

Les textes de référence

> Article 40 du Code civil

> Décret n° 2017-890 du 6 mai 2017 relatif à l'état civil - sur Légifrance

> Article L.212-11 du code du patrimoine - sur Légifrance

> Article L.212-12 du code du patrimoine - sur Légifrance

DOCUMENT 5

« Floride : le piratage d'un réseau d'eau potable tourne court grâce à la vigilance d'un employé » - *Ici.fr* - 9 février 2021

iStock

FRAYEUR - Aux États-Unis, les autorités sont sur le qui-vive après le piratage, vendredi, d'une usine d'approvisionnement en eau en Floride. S'infiltrant dans le réseau d'ordinateurs, le hacker est parvenu à modifier l'équilibre chimique de l'eau, la rendant dangereuse pour la consommation.

Le pire a été évité de justesse. Vendredi, à la veille du Superbowl qui se jouait à quelques kilomètres de là, à Tampa, un pirate informatique est parvenu à entrer de façon illégale dans le réseau d'ordinateurs d'une usine d'approvisionnement en eau en Floride, donnant des instructions pour augmenter à un niveau dangereux la concentration d'un additif chimique. Immédiatement remarquée, la modification des données a été corrigée de façon à ce qu'aucun consommateur local n'ait été en danger.

La teneur en hydroxyde de sodium multipliée par 1000

Les 15.000 personnes qui dépendent de l'usine de traitement d'eau d'Oldsmar, dans la banlieue de Tampa, doivent leur santé à un technicien informatique. Dans la salle des opérations vendredi matin, il remarque tout d'abord le déplacement inopiné de son curseur de souris. L'incident en reste là, mais se reproduit quelques heures plus tard. Là, l'employé de l'usine voit que quelqu'un, derrière son écran, est en train de multiplier par 1000 la teneur de l'eau en hydroxyde de sodium. La substance,

cruciale pour le contrôle d'un milieu alcalin ou la régulation d'acidité de l'eau, est corrosive et dangereuse à teneur élevée.

L'alerte donnée immédiatement fait échapper au pire

L'opérateur réduit immédiatement la teneur et donne l'alerte aux autorités locales. Le shérif met alors en garde toutes les infrastructures sensibles du secteur. *"Quand on passe de 100 à 11.100 parties par million, ce n'est pas juste un accident. C'est potentiellement grave"*, souligne-t-il auprès de Fox 13 News. Interviewée par la chaîne de télévision, Katherine Alfredo, professeur de génie civil à l'Université de Floride du Sud, indique qu'une telle concentration en hydroxyde de sodium n'est pas mortelle, mais est surtout dangereuse pour la peau. Si le dénouement de cette cyberattaque est heureux, celle-ci est venue illustrer le danger que les piratages informatiques peuvent faire courir à d'importantes infrastructures. Le FBI a ouvert une enquête.

DOCUMENT 6

« Après le piratage informatique de la mairie de Douai, des données personnelles des habitants volées ? » - *francebleu.fr* - 14 avril 2021

Vendredi dernier, des hackers ont piraté les serveurs de la ville de Douai par le biais d'un rançongiciel, un logiciel malveillant qui bloque les données informatiques en échange d'une rançon. Les services sociaux ont été touchés, faisant craindre la perte de certaines données personnelles.

Des données personnelles de Douaisiens volées par des hackers ? La question se pose après le piratage informatique subi vendredi dernier par la ville de Douai. Un piratage par le biais d'un "rançongiciel" ou "ransomware" en anglais. Il s'agit en fait d'un logiciel malveillant qui bloque l'accès aux données en échange d'une rançon. Les téléphones et les mails des agents de la ville ont été rendus inaccessibles, tout comme plusieurs services en ligne.

Ce mercredi, les services en ligne fonctionnent à nouveau, mais les mails de tous les agents de la ville sont toujours inutilisables. Les serveurs informatiques de la municipalité avaient été mis hors service dès la découverte de l'attaque vendredi dernier et la plupart des données faisaient l'objet d'une sauvegarde régulière. Mais des données personnelles de Douaisiens pourraient avoir été perdues, notamment celles dont disposent les services sociaux. Et donc volées par les hackers.

Le maire rassure

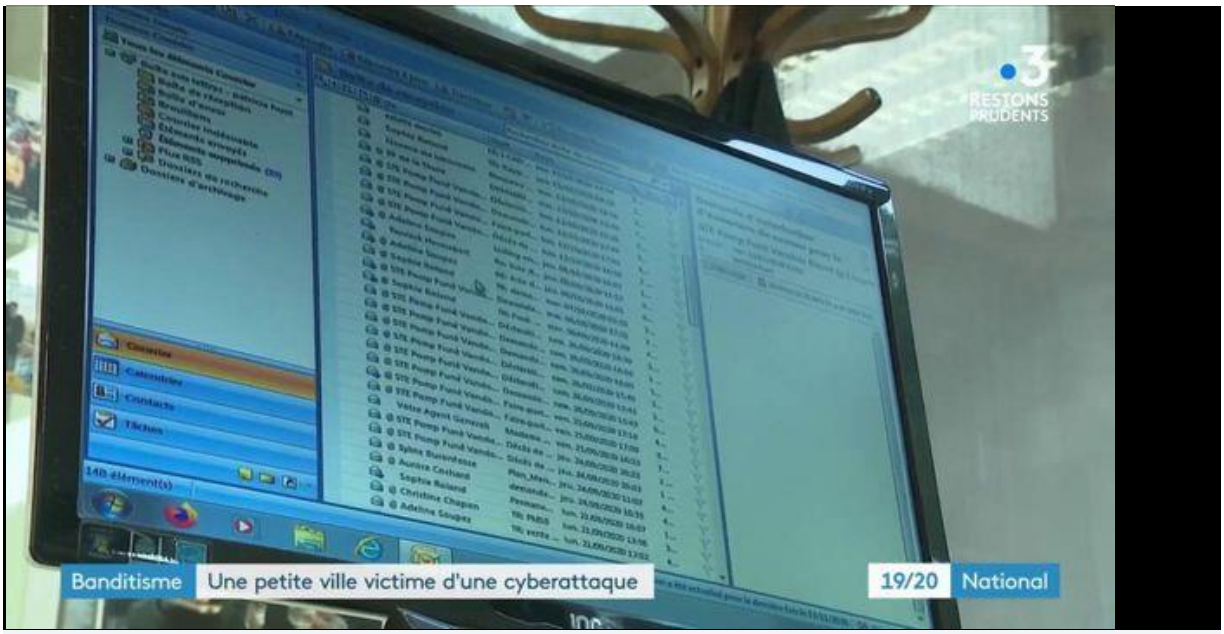
"Ces données personnelles peuvent amener les hackers à faire de l'usurpation d'identité", s'inquiète Coline Craeye, conseillère municipale d'opposition. Elle demande au Maire de Douai, Frédéric Chéreau, *"de dire quelles sont les données que les pirates informatiques ont dans les mains et quelles sont les familles concernées."*

Frédéric Chéreau se veut rassurant. Le maire de Douai explique que des analyses sont toujours en cours avec l'agence nationale de sécurité des systèmes d'information (ANSSI) pour définir les données perdues et les personnes touchées. *"Il ne faut pas paniquer, les données dont nous disposons ne sont pas utilisables tel quel."*, explique Frédéric Chéreau. *"Nous sommes en train de recenser les personnes concernées pour les contacter"*, poursuit l'édile.

Douai n'est pas la première commune du Nord à avoir été touchée par ce type de piratage. En novembre dernier, la mairie d'Aulnoye-Aymeries en avait également été victime.

DOCUMENT 7

« Cyberattaques : les communes de plus en plus victimes du rançonnage » - *Francetvinfo.fr* - 23 novembre 2021



Dans le Nord, une commune de 9 000 habitants a vu son système informatique sclérosé par une attaque au logiciel de rançonnage. Une pratique devenue répandue face au système vulnérable des collectivités locales.

Il y a quelques jours, le patron français de la sécurité informatique alertait sur la vulnérabilité des collectivités locales face aux cyberattaques. Les communes sont de plus en plus ciblées. À Aulnoye-Aymeries, dans le Nord, les systèmes informatiques de la ville de 9 000 habitants sont hors service depuis mercredi 18 novembre. *"Tout apparaît sur le bureau, mais on ne peut rien ouvrir"*, explique Patricia Huet, employée de mairie. Les données d'état civil et les sauvegardes ont été piratées.

Sécuriser l'Ehpad, une priorité

Tout doit être fait à la main pour le moment. En pleine crise sanitaire, la sécurité des résidents de l'Ehpad de la commune est aussi au centre des préoccupations. *"Les appels malades ne fonctionnent plus"*, indique Sabine Cambreleng, directrice du centre communal d'aide sociale (CCAS). Les soignants ne reçoivent donc plus sur leur smartphone l'appel d'une personnes âgée. La municipalités a été victime d'un logiciel de rançon. Une demande de 150 000 euros a été faite, refusée par les autorités.

DOCUMENT 8

« Cyberattaque à Angers : deux mois après, la police ne peut toujours pas dresser de PV » - *Ici.fr* - 25 mars 2021

BUGS – Le 16 janvier dernier, la ville d'Angers a été touchée par une cyberattaque. Depuis, la police municipale ne peut plus mettre de PV. La bibliothèque et la clinique d'Anjou sont, elles aussi, touchées.

"Ça aurait été sympa de nous prévenir." C'est une nouvelle qui laisse un goût amer aux Angevins. Depuis le 16 janvier dernier, la police municipale ne peut plus dresser de PV. Les horodateurs, eux, fonctionnent toujours. *"Ce n'est pas normal de ne pas nous le dire, je trouve qu'il faut être assez honnête avec les gens"*, affirme un automobiliste. *"On aurait pu économiser un petit peu de sous"*, poursuit une autre.

Ce piratage informatique bloque encore les sites internet de la bibliothèque et de la garderie. Dans le reportage en tête de cet article, une maman a des difficultés pour réserver le centre aéré. *"Normalement, on fait ça tranquillement dans notre salon sans avoir rien à demander à personne, là il a fallu appeler la mairie",* explique-t-elle.

Une cyberattaque qui touche toute la ville

La cyberattaque a visé la clinique d'Anjou également. Aujourd'hui encore, tous les services n'ont pas retrouvé leur système informatique, un retour au papier pas toujours simple. *"Au départ, ça a pris plus de temps parce qu'il faut se remettre au papier"*, déclare une infirmière. Un *"plan blanc"* a été déclenché pour mobiliser le personnel plus longtemps et stabiliser la situation. *"Ça nous a surpris, on ne s'attendait pas à ça à ce moment-là. On était déjà en pleine crise Covid donc cette crise s'est rajouté à la crise"*, témoigne un infirmier.

Pour que cela ne se reproduise plus, les données seront à l'avenir hébergées sur un serveur extérieur à la clinique, nous assure le directeur. Les services de la ville et de la clinique devraient revenir à la normale autour du mois de juin. En ce qui concerne les PV, ne vous faites pas de fausses joies, le système devrait fonctionner à nouveau d'ici quelques jours.

DOCUMENT 9

« Comment Colonial Pipeline a géré une attaque de ransomware » - *kaspersky.fr* - 17 Mai 2021

La récente attaque par ransomware contre Colonial Pipeline, l'entreprise qui contrôle le réseau d'oléoducs qui fournit du carburant à une grande partie de la côte Est des États-Unis est l'une des plus grandes de toute l'histoire. Naturellement, les détails concernant l'attaque n'ont pas été rendus publics, mais certaines bribes d'informations ont été partagées par les médias, ce qui nous permet d'en tirer une conclusion : informer rapidement les forces de l'ordre aide à réduire les dégâts. Bien entendu, tout le monde n'a pas ce choix-là car dans certains états, les victimes sont obligées d'informer les organismes de réglementation. Cependant, même si ce n'est parfois pas nécessaire, cela peut vraiment aider.

Attaque

Le 7 mai, le ransomware a touché Colonial Pipeline, une entreprise qui gère le plus long oléoduc destiné au transport d'hydrocarbures sur la côte Est des États-Unis. Les employés ont dû déconnecter certains systèmes d'informations car certains ordinateurs étaient chiffrés et afin que l'infection ne se propage pas. Cet incident a causé des retards dans l'approvisionnement en carburant de la côte Est, ce qui a provoqué une hausse de 4 % des contrats à terme sur l'essence. Afin de limiter les dégâts, l'entreprise prévoit d'augmenter les livraisons de carburant.

L'entreprise continue de restaurer son réseau, mais selon des informations du blog de Zero Day, le problème ne se trouve pas dans le réseau de services mais plutôt dans le système de facturation.

Fermeture fédérale

Les opérateurs de ransomwares modernes non seulement chiffrent les données et demandent une rançon pour les déchiffrer, mais ils volent également ces informations pour s'en servir comme moyen de pression afin d'extorquer les victimes. En ce qui concerne Colonial Pipeline, les pirates informatiques se sont emparés d'environ 100 Gb de données de l'entreprise.

Cependant, selon *Washington Post*, des enquêteurs externes ont vite su ce qu'il s'était passé et où se trouvaient les données volées et ils ont par la suite contacté le FBI. Les fédéraux, à leur tour, ont contacté le fournisseur d'accès Internet qui possède le serveur où se trouvaient les données téléchargées, et l'ont isolé. Par conséquent, les cybercriminels ne devraient plus avoir accès aux données qu'ils ont volées à Colonial Pipeline. Cette rapidité d'action a au moins aidé à limiter les dégâts.

Le fait de savoir ce qui est arrivé ne remettra pas les principaux oléoducs en service, mais les dégâts, assez conséquents, auraient pu être bien pires.

Origine

Il semblerait qu'il s'agisse d'une attaque du ransomware DarkSide qui peut être distribué à la fois sur Windows et Linux. Les produits de Kaspersky détectent ce malware en tant que Trojan-Ransom.Win32.Darkside et Trojan-Ransom.Linux.Darkside. Ce malware utilise de puissants algorithmes de cryptage, ce qui rend impossible la restauration des données sans une clé.

À première vue, le groupe DarkSide ressemble à un fournisseur de services en ligne doté d'un support technique, d'un service de communication et d'un centre de presse. Un message laissé par les

responsables sur leur site Web laisse entendre que leur motivation était purement financière et non politique.

Ce groupe utilise un modèle d'abonnement RaaS (ransomware-as-a-service) et fournit à leurs partenaires un logiciel ainsi qu'une infrastructure connexe pour mener une attaque. Un de ces partenaires est l'auteur de l'attaque ciblant Colonial Pipeline. Selon DarkSide, le groupe n'avait pas pour objectif d'engendrer de telles répercussions sociales, et dorénavant, il surveillera de près quelle victime leurs « intermédiaires » choisissent. Cependant, il est difficile de prendre au sérieux une seule déclaration parmi les nombreux tours de passe-passe de relations publiques.

Comment se protéger

Afin de protéger votre entreprise des ransomwares, nos experts recommandent ce qui suit :

- Interdisez les connexions superflues aux *Remote Desktop Services* (Services Bureau à distance) comme par exemple un RDP à partir d'un réseau public, et utilisez toujours un ou des mots de passes forts pour ce genre de services ;
- Installez tous les correctifs disponibles pour les solutions VPN que vous utilisez pour que les employés qui travaillent à distance se connectent au réseau de l'entreprise ;
- Mettez à jour les logiciels et tous les appareils connectés afin d'empêcher l'exploitation d'une vulnérabilité ;
- Centrez votre stratégie de défense sur la détection des mouvements latéraux et sur l'exfiltration des données en prêtant une attention particulière au trafic sortant ;
- Sauvegardez régulièrement vos données et assurez-vous que vous avez rapidement accès aux sauvegardes lors d'une urgence ;
- Tirez profit des renseignements sur les menaces afin d'être toujours au courant des tactiques d'attaques, des techniques ainsi que des procédures ;
- Utilisez des solutions de sécurité comme Kaspersky Endpoint Detection and Response et Kaspersky Managed Detection and Response qui aident à bloquer rapidement les attaques ;
- Formez vos employés afin de les sensibiliser à la sécurité au sein de l'entreprise ;
- Utilisez une solution de sécurité fiable pour la protection des terminaux qui empêche les exploits, détecte les comportements suspects et qui peut annuler les changements malveillants et restaurer le système.

Le cas de Colonial Pipeline montre l'avantage de contacter les autorités et sans tarder. Rien ne garantit qu'elles pourront aider, mais elles pourront minimiser les dégâts.

DOCUMENT 10
« Les données personnelles d'agents du Grand Annecy diffusées cinq mois après la cyberattaque » - *Lagazettedescommunes.com* - 19 mai - 2021

ADOBESTOCK/Oleksii

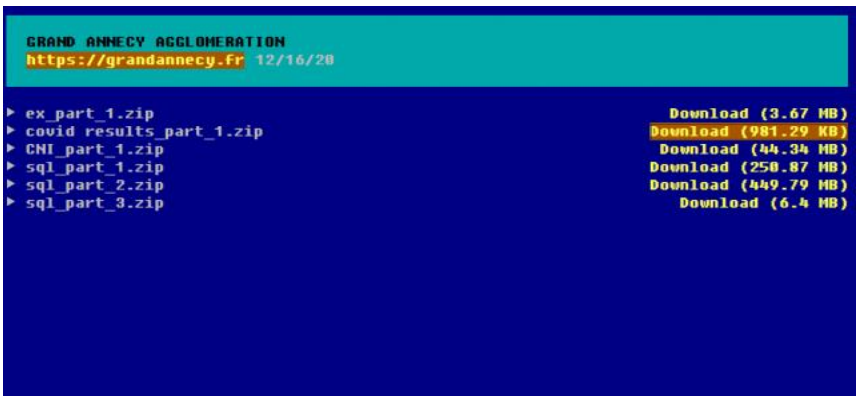
Tests « Covid-19 » ou coordonnées personnelles de plus de 1000 agents de la communauté d'agglomération ont été diffusées sur le web alternatif. Une attaque par rançongiciel avait ciblé le Grand Annecy à la fin de l'année 2020.

Les usagers avaient d'abord payé les pots cassés, avec la suspension de certains services distants, comme le paiement des factures d'eau ou tout simplement la consultation du site du Grand Annecy (Haute-Savoie, 34 communes, 200 000 hab.), seulement rétabli à la mi-mars.
Près de cinq mois après la découverte de l'intrusion, à la fin décembre 2020, les cybercriminels de Pysa viennent de se rappeler aux bons souvenirs des Haut-Savoyards, en publiant les informations personnelles de plusieurs agents, conservées par la collectivité.

Un mode opératoire déjà expérimenté contre la métropole d'Aix-Marseille-Provence. Les pirates informatiques(1) avaient alors attendu six mois pour, faute de paiement d'une rançon, faire fuiter des données. Si la collectivité du sud de la France avait déploré une fuite d'environ 20 gigaoctets, celui qui affecte le Grand Annecy, d'environ 750 mégaoctets pour le moment, est d'une ampleur moindre.

Un millier de personnes touchées

Mais si le volume de données divulguées est plus faible, cette fuite est pourtant d'une autre envergure. Dans les six archives publiées, repérées par le blog spécialisé Zataz.com et consultées par La Gazette des communes, on retrouve en effet plusieurs dizaines de cartes d'identité ou d'autres documents d'identités scannés. Un autre dossier contient des résultats de tests « Covid-19 », avec 55 résultats nominatifs. Enfin, un dernier fichier comporte une liste d'agents avec leur date de naissance, leur adresse et leurs numéros de téléphones mobiles.



Capture d'écran du site proposant des données personnelles d'agents du Grand Annecy sur le web alternatif

Alors que la collectivité compte environ 1300 agents, elle a dû informer plus de 1000 personnes – essentiellement des agents ou anciens salariés, mais aussi quelques élus et des résidents d'Ehpad – de cette violation de données personnelles, également notifiée à la Cnil.
Ils peuvent tous se tourner vers le délégué à la protection des données. L'agglomération n'a su quelles données avaient été volées qu'après leur publication.

De manière générale, « nous invitons toutes les victimes à être particulièrement vigilantes », complète Véronique Bonnard, la directrice de la communication du Grand Annecy. L'accès à des documents d'identité peut devenir une mine d'or pour des escrocs, en facilitant des tentatives d'usurpation d'identité, par exemple pour prendre le contrôle d'un compte bancaire.

« Une collègue vient de recevoir le courrier de la direction générale l'appelant à faire attention à ses comptes bancaires », signale ainsi Jean-Claude Davat, représentant du personnel Unsa-Territoriaux. « Alors que la première communication de la direction était assez rassurante dans un premier temps, on sent une différence, ajoute-t-il. C'est plus inquiétant, sans que l'on ait vu de conséquences néfastes pour l'instant. »

Des conséquences déjà lourdes

Pour les agents, les conséquences du piratage avaient déjà été lourdes cet hiver. Privés de messagerie, des employés ont perdu le décompte de certains de leurs congés. Des comptes épargne temps d'agents ont également été perdus. "Il y a eu beaucoup de saisies à opérer pour reconstruire des bases de données dont on avait besoin de suite", poursuit Jean-Claude Daval.

Au lendemain du piratage, des aides à domicile avaient dû faire leur tournée de mémoire, tout comme les éboueurs, privés de leur GPS, relate enfin la direction de la communication de la communauté d'agglomération. Et faute de site internet, l'agglomération avait été obligée de publier en commentaire de son post Facebook le plan de ramassage des sapins de Noël. Un réveillon au goût toujours amer, cinq mois après.

DOCUMENT 11

« Comment se prémunir contre les rançongiciels »
Lagazettedescommunes.com - 5 novembre 2020

Hasselblad H5D

De nombreuses collectivités ont été attaquées par des rançongiciels ces derniers mois, immobilisant parfois leurs services pendant plusieurs semaines. Des entités de toutes tailles ont été ciblées, montrant l'importance de prendre en compte ce risque d'attaque à tous les échelons. Outre une hygiène numérique primordiale et un soin quotidien à la sécurité informatique avec un budget conséquent, l'anticipation en cas d'attaque est importante.

DoppelPaymer, Sodinokibi, Mespinoza : les rançongiciels prolifèrent mais leur fonctionnement de base est identique. Ils chiffrent les données des ordinateurs attaqués et demandent une rançon en échange d'une clé de déchiffrement. La crise sanitaire, avec ses multiples postes à distance ouverts, a créé de nombreuses vulnérabilités dont ont su profiter les assaillants. « La numérisation de services et la dématérialisation s'accroissent dans les collectivités, donc les risques aussi, constate Jean-Jacques Latour, expert à cybermalveillance.gouv.fr, plateforme gouvernementale de sensibilisation aux risques cyber. On veut numériser sans forcément prendre en compte les risques, c'est comme sauter d'un avion sans parachute. »

Les signalements sur la plateforme pour des attaques par rançongiciels ont explosé par rapport à l'an dernier. Ces attaques sont le fait de réseaux de criminels, organisés en ligne. « Ce n'est pas un groupe criminel unique qui contrôle tout, explique François-Xavier Masson, directeur de l'Office central de lutte contre la criminalité liée aux technologies de l'information et de la communication. Les pirates sont en contact entre eux grâce aux réseaux sociaux et se complètent en mettant à la disposition des autres leurs savoir-faire : préparation du logiciel, envoi des messages, identification des failles, captation des données, blanchiment des données et de l'argent… »

Plusieurs collectivités ont accepté de faire un retour d'expérience, pour que leur mésaventure serve à en empêcher d'autres. Elles y ont mis une condition : leur anonymat. « Nous voulons éviter de nous retrouver exposés et donc de donner des billes aux attaquants », explique le directeur des systèmes d'information (DSI) d'une collectivité de l'Est de la France, attaquée il y a quelques mois. Ces offensives ont souvent eu lieu le vendredi soir, ou le week-end. « Une fois que les pirates ont réussi à entrer dans le réseau, ils restent des jours, voire des semaines, explique Jean-Jacques Latour. Ils repèrent les actifs, détruisent les sauvegardes s'ils y parviennent et choisissent le moment pour l'attaque : quand la pression est maximale. »

Traces laissées par les pirates

Une fois l'attaque constatée, faire une revue des dégâts est important. « Ils ont trouvé les serveurs de sauvegarde et les ont explosés », se souvient le DSI dans l'Est. « On a perdu toutes nos données de travail, notre serveur de fichiers, les tableaux de bord. Heureusement, on a pu récupérer une partie

des données chez nos prestataires », constate de son côté un directeur général adjoint (DGA) d'une agglomération attaquée en 2019. En parallèle, il faut faciliter l'identification des traces laissées par les pirates qui seront transmises à l'Agence nationale de la sécurité des systèmes d'information (Anssi) et aux autorités, en cas de plainte. « Il faut récupérer un maximum d'informations et de journaux de connexion pour les analyser », se souvient un responsable de la sécurité informatique (RSSI) d'une grande ville. Alors que le message garantissant que « tout serait plus simple contre quelques bitcoins » s'affiche sur tous les écrans, aucune collectivité n'a payé de rançon. « Il est recommandé de ne jamais payer », note l'Anssi dans un guide sur le sujet. « En payant, vous alimentez le système criminel ; surtout, vous n'êtes pas garantis de retrouver vos données », confirme François-Xavier Masson.

Les priorités – paie des agents, versement du revenu de solidarité active (RSA) pour les départements – ont ensuite dû être rapidement gérées. « On savait quelles étaient les applications les plus sensibles ou importantes. Mais il y a des choses que l'on n'a pas pu anticiper, note-t-on dans une grande ville. Nous étions en pleine crise sanitaire et la direction des opérations funéraires nous appelle pour une urgence : il a fallu remonter en 48 heures le système d'information pour gérer les concessions dans les cimetières… »

Numéro d'équilibriste

Une petite ville attaquée à quelques jours des élections a dû reconstituer à la hâte des listes d'émargement grâce à la mobilisation de plusieurs agents. Alors que les systèmes d'information sont paralysés, prévoir une communication efficace peut ressembler à un numéro d'équilibriste. « Il faut faire attention à ne pas donner d'informations contre-productives », prévient la directrice générale des services (DGS) d'un département attaqué. Les premiers jours, elle a privilégié les SMS pour communiquer avec les agents. D'autres ont dû se passer de courriels pendant plusieurs semaines. Un retour en arrière technologique imposé. « Le papier n'est pas prêt de disparaître », ironise un DGS attaqué.

Les attaques sont l'occasion de se montrer résilient, notamment par la fortification des systèmes informatiques. « On a fait intervenir un prestataire très rapidement pour nous aider à reconstituer le réseau, se souvient un directeur général adjoint, mais la procédure d'urgence dans les marchés publics ne fait pas apparaître le "risque cyber", il faudrait que ça soit modifié. » Dans une commune attaquée en 2019, « les supports de sauvegarde ne restent pas allumés en permanence ».

Un travail de longue haleine

Le DGA d'une autre ville ciblée confirme : « Il est important d'avoir des sauvegardes dignes de ce nom et, surtout, de ne pas mettre tous les œufs dans le même panier. » Selon Jean-Jacques Latour, « avec des mises à jour, des mots de passe solides et une sauvegarde hors ligne, 90 % des attaques pourraient être réglées ». La mise à niveau des systèmes de sécurité ne se fait pas sans impact. La double authentification, qui consiste à demander confirmation d'une connexion par un code reçu sur le téléphone, adopté par le service technique d'une agglomération et l'ensemble des agents d'un département obère la fluidité du travail.

« Il y a des actions de sensibilisation à mener régulièrement sur le "phishing" [hameçonnage], le changement fréquent des mots de passe. C'est un travail de longue haleine qu'il faut reprendre régulièrement », détaille la DGS d'une collectivité attaquée pendant l'été. « Nous avons instauré de nouvelles recommandations et commandé la prestation d'Avant de cliquer, une société spécialisée dans la prévention des risques de "phishing" et d'intrusion auprès des agents », explique de son côté

un DSI. Mais ces actions coûtent cher. Le Club de la sécurité de l'information français (Clusif) a publié un rapport, « Menaces informatiques et pratiques de sécurité en France », selon lequel, une communauté de communes a estimé à 400 000 euros l'impact financier d'une attaque. « La sécurité informatique, ça coûte cher, prévient un DGA, mais tout remettre en place après une attaque, ça coûte encore plus cher. Nous avons dû changer plusieurs machines parce qu'elles ne supportaient pas les antivirus nouvelle génération. »

Lorsque les systèmes sont remis en place, tout n'est pas pour autant terminé. Les attaquants publient régulièrement des données pour remettre la pression, plusieurs semaines après les attaques. « Il faut prendre en compte ce nouveau risque sur la confidentialité des données », note l'Anssi dans son « Etat de la menace rançongiciel », paru en février 2020. La communication est primordiale, pour ne pas dégrader la confiance, avec parfois des données personnelles d'administrés qui traînent en ligne. Dans le rapport du Clusif pourtant, 53 % des collectivités attaquées interrogées disent ne pas avoir communiqué sur l'attaque. Alors que cela sert aussi de prévention. « J'ai fait un retour de ce qui nous est arrivé à tous les collègues des hôpitaux, départements et communes que je côtoie », explique le DSI d'une commune. Parfois, l'attaque est un lointain souvenir. Le même DSI se désole : « Malgré l'attaque, j'ai encore un peu de mal à trouver un budget. Il faut pourtant des gens spécialisés qui aient le temps de travailler. »

FOCUS

« L'une des solutions est la mutualisation »

Cyril Bras, responsable de la sécurité des services informatiques (RSSI) de Grenoble – Alpes métropole, 49 communes, 443 100 hab.

« La cybersécurité doit être prise en compte au plus haut niveau, c'est stratégique. Il est important de respecter l'hygiène numérique en général, mais pas seulement sous le prisme technique. La prise de conscience pour les collectivités est douloureuse parce qu'auparavant le sujet a été malmené. On le voit au positionnement du RSSI dans la hiérarchie. La solution est notamment la mutualisation, le levier se situant au niveau des intercommunalités. Il ne faut pas forcément mutualiser les systèmes informatiques, mais la compétence de sécurité des services informatiques. On est d'ailleurs en train de créer un réseau de RSSI pour s'aider et partager entre les collectivités rapidement. »

FOCUS

« Il faut de la transparence»

Jérôme Poggi, responsable des services informatiques de Marseille, 863 300 hab.

« A cause de la cyberattaque [les 13 et 14 mars], on ne pouvait plus accéder aux mails, échanger avec les citoyens était impossible. Il fallait donc communiquer en interne comme en externe, surtout que nous n'étions pas les seuls touchés, la métropole l'était aussi. Il faut de la transparence. Je pense qu'en termes de communication, on a fait au mieux. On s'est exprimé assez tôt et on a bien fait : plus on attend, plus les gens se posent des questions. Surtout, c'était la veille des élections [premier tour des municipales] et il était impossible de laisser les complots prospérer. A Marseille, on a toujours été vigilants au sujet des élections : le système qui centralise les résultats a un réseau dédié, qui n'a pas été impacté. La communication permet aussi de sensibiliser au-delà de sa collectivité : j'ai été en contact avec d'autres RSSI qui nous ont remerciés d'avoir été transparents. »

DOCUMENT 12

« Une cyberattaque coûte 550 000 euros à la ville de Chalon-sur-Saône » - Lagazettedescommunes.com - 29 juillet 2021

Momius / Adobestock

Lors du conseil municipal du 20 juillet, le maire de Chalon-sur-Saône a annoncé le coût de la cyberattaque subie par la ville et la communauté d'agglomération en février dernier. Plusieurs embauches sont en cours.

En février, la communauté d'agglomération, la ville et le CCAS de Chalon-sur-Saône ont été victimes d'une attaque par rançongiciel. En réponse à une question lors du conseil municipal du 20 juillet, le maire de la ville a donné quelques éléments sur le coût de la remise en état de marche des systèmes informatiques, ainsi que le notait le Journal de Saône-et-Loire.

Des embauches en cours

550 000 euros ont été engagés par la collectivité pour remettre d'aplomb le système informatique et plusieurs embauches sont en cours, dont celle d'un responsable de la sécurité des services informatiques (RSSI).
« On en sort grandi, s'est félicité le maire. Cette reconstruction a permis d'améliorer de manière substantielle la sécurité de notre système d'information. »

Les 550 000 euros ont été réglé en partie à Orange Cyberdéfense qui a accompagné les collectivités lors de l'attaque, ainsi que plusieurs prestataires. Le maire a également annoncé un soutien de l'Anssi, de l'ordre de 100 000 euros, pour l'amélioration de la sécurité de ses systèmes.

« Les systèmes informatiques de la Ville de Chalon-sur-Saône et du Grand Chalon ont été victimes d'une cyberattaque », indiquait le 21 février le Grand Chalon sur sa page Facebook. Le maire avait rapidement communiqué pour indiquer qu'il ne paierait pas la rançon demandée par le groupe criminel qui paralysait les systèmes informatiques des collectivités. « Nos amis destructeurs peuvent attendre, nous ne donnerons pas un seul centime du contribuable », a-t-il déclaré au micro de France 3.

Dégâts moindres mais coût important

Le coût est important, alors que l'attaque n'a fait que très peu de dégâts. Aucune fuite de données personnelles n'a pour l'instant été constatée et aucune donnée administrative n'a été perdue. « On n'a pas perdu de données administratives. On avait un système de sauvegarde qui existait et on a pu récupérer des données de la veille de la cyberattaque. C'est une chance extraordinaire », s'est réjoui le maire.

Ce n'est pas le cas pour toutes les villes cyberattaquées. La ville de Bondy, en Seine-Saint-Denis avait dû reconstruire l'intégralité des dossiers RH de ses agents, faute de sauvegarde.
Et les villes d'Annecy et Marseille avaient vu les données personnelles de certains de leurs administrés être mises en ligne sur le web alternatif plusieurs semaines après avoir subi des attaques par rançongiciel.

Après la cyberattaque subie en janvier par la ville d'Houilles, dans les Yvelines, le maire avait annoncé un coût de 350 000 euros. Depuis le début de l'année, plus d'une dizaine de collectivités ont annoncé avoir été victimes de cyberattaque par rançongiciel.

DOCUMENT 13

« Les RSSI des collectivités territoriales créent un réseau de partage » - *lemondeinformatique.fr* - 16 Février 2021

Constatant un manque et avec le soutien de l'Anssi, un réseau regroupant une centaine de RSSI de collectivités territoriales vient de voir le jour. Un lieu d'échanges et d'entraide particulièrement utile en cette période de vague de cyberattaques.

A l'occasion du Panocrim du Clusif, le RSSI de la ville de Marseille Jérôme Poggi avait déjà vendu la mèche sur l'existence d'un réseau regroupant des RSSI des collectivités territoriales. Il restait néanmoins à officialiser cette structure et c'est chose faite par la voix de son pilote, Cyril Bras, RSSI de la métropole de Grenoble. « Le réseau comprend aujourd'hui une centaine de membres venant de différents horizons, villes, métropoles, départements, régions réparties sur l'ensemble du territoire », précise le responsable. Les admissions se déroulent par cooptation et excluent les fournisseurs de solutions. Le réseau comprend un comité de coordination composé d'une dizaine de personnes.

Ayant le soutien de l'Anssi, ce réseau a pour vocation d'être « un lieu de partage d'informations, de bonnes pratiques et d'expérience ». Bien évidemment, ce groupe est particulièrement actif pendant cette période où les collectivités locales sont de plus en plus frappées par des cyberattaques et notamment des ransomwares. « Nous partageons notamment des rapports d'IOC (indices de compromission) pour améliorer la réponse à incident », glisse Cyril Bras. Et de prodiguer aussi des conseils autour « de la sauvegarde et de l'hygiène informatique ».

Une meilleure écoute et une structuration en réflexion

Si les questions de cybersécurité focalisent les discussions pour des raisons évidentes d'actualité, le groupe entend bien discuter d'autres sujets (RGS, retour d'expérience, sensibilisation). Un échange nécessaire selon Cyril Bras, « en discutant avec les RSSI, on constate qu'il y a un manque d'écoute des RSSI de la part des collectivités ». Et pourtant, le responsable de la sécurité est « le garant de la confiance des usages du numérique », rappelle-t-il. Un autre axe de la création de ce réseau est de montrer un front commun vis-à-vis des éditeurs de solutions de sécurité qui proposent parfois « des produits non conformes ». Il s'agit d'un marché de niche et les collectivités sont un peu démunies pour négocier avec les fournisseurs.

Maintenant que la création de ce réseau est actée, quelles sont les prochaines étapes ? « Nous sommes en pleine réflexion pour savoir quelle forme prendra ce réseau : association ou autre avec un rattachement ou pas », admet Cyril Bras. Cette formalisation devrait intervenir dans les prochains mois pour une initiative essentielle dans cette période de forte intensité cyber autour des collectivités locales.

DOCUMENT 14

« Le service d'assainissement des eaux d'Oloron-Sainte-Marie a été pris pour cible par des hackers » - *usine-digitale.fr* - 30 Septembre 2021

Le service d'assainissement des eaux de la commune d'Oloron-Sainte-Marie a été victime d'un ransomware. Les hackers ont profité de la phase de maintenance du site pour pénétrer dans le système d'information. Une plainte a été déposée.

Après l'hôpital, c'est le service d'assainissement des eaux d'Oloron-Sainte-Marie dans les Pyrénées-Atlantiques qui a été visé par un ransomware en juin 2021. L'incident a été révélé par Patrick Maillet, adjoint en charge de la politique budgétaire et de la police municipale, lors du Conseil municipal du 27 septembre, d'après *Sud Ouest*.

LORS DE LA PHASE DE MAINTENANCE

Les cyberattaquants ont profité d'une faille dans le système de gestion automatisée des pompes de relevage de la station d'épuration, détaille *20 Minutes*. C'est au moment de la maintenance par la PME ASCII, spécialisée en automatisme et informatique industrielle, qu'ils ont réussi à pénétrer dans le système d'information. "*Tous les écrans se sont éteints et un message est apparu avec une demande de rançon*", a raconté Patrick Maillet.

Une partie des données a été détruite mais les criminels n'ont pas réussi à prendre le contrôle du service d'assainissement. La commune a refusé de payer la rançon, dont le montant est inconnu. La facture de 12 000 euros est tout de même salée pour ce territoire de 10 000 habitants.

UNE PISTE VERS LA RUSSIE ET L'AFRIQUE DU SUD

Une plainte a été déposée pour faire la lumière sur cette attaque. Pour l'instant, le traçage des hackers et des données piratées a permis de remonter jusqu'en Russie et en Afrique du Sud, précise *20 Minutes*.

Cette attaque montre, une nouvelle fois, la manque de sécurité informatique des infrastructures critiques. L'Union européenne souhaite d'ailleurs renforcer les règles en la matière en élargissant le nombre de secteurs concernés par des obligations strictes, dont les eaux usées ou encore les infrastructures des marchés financiers font partie.

DOCUMENT 15

« LOI DE PROGRAMMATION MILITAIRE 2019/2025 : UNE PROTECTION ACCRUE CONTRE LES ATTAQUES INFORMATIQUES » - *datalegaldrive.com*

6 mars 2019

Une défense efficace de la sécurité, qu'elle soit privée, ou étatique et souveraine, passe aujourd'hui irrémédiablement et prioritairement par une protection accrue des systèmes informatiques. C'est la raison pour laquelle la **loi n°2018-607 du 13 juillet 2018 relative à la programmation militaire pour les années 2019-2025** et portant diverses dispositions intéressant la défense (« **LPM** ») procède à un renforcement significatif des capacités de détection, de caractérisation et de prévention des attaques opérées sur les systèmes informatiques.

Modifiant à la fois le Code des postes et des communications électroniques et le Code de la défense, **l'article 34 de la LPM** ajoute une nouvelle pierre à l'édifice de la lutte contre les attaques informatiques en France. Publié le 14 décembre dernier et entré en vigueur le 1er janvier 2019, **le décret n°2018-1136** apporte des précisions sur les modalités d'application des nouvelles compétences accordées aux différents acteurs du secteur et que nous allons expliciter ci-dessous.

1. Une prévention accrue de la sécurité des systèmes d'information par la consécration de nouveaux pouvoir

Le nouveau dispositif juridique implique désormais l'ensemble des opérateurs de communications électroniques (OCE) – et non plus seulement les opérateurs d'importance vitale (OIV) – ainsi que les fournisseurs de services de communication au public en ligne.

Instaurant une étroite collaboration entre les opérateurs de communications électroniques et l'autorité nationale de sécurité des systèmes d'information (« **ANSSI** »), le nouvel **article L 33-14 du Code des postes et des communications électroniques** dessine en effet les nouveaux contours d'une défense renforcée des systèmes d'information.

Est ainsi autorisée la mise en place par **les opérateurs de communications électroniques** de **« *dispositifs mettant en œuvre des marqueurs techniques* *aux seules fins de détecter des événements susceptibles d'affecter la sécurité des systèmes d'information de leurs abonnés* ». Le recours à ces dispositifs pourra être exercé soit à l'initiative des opérateurs de communications électroniques eux-mêmes – ils devront alors en informer l'ANSSI – ou encore à la requête de l'ANSSI elle-même.

Outre demander aux opérateurs de communications électroniques de mettre en place ces dispositifs de détection d'attaques informatiques, **l'article L 2321-2-1 du Code de la défense** permet désormais à l'ANSSI elle-même de mettre en œuvre directement sur le réseau d'un opérateur ces mêmes dispositifs. Cette possibilité lui est plus précisément ouverte lorsqu'elle a connaissance d'une menace grave et imminente sur les systèmes d'une autorité publique, d'un opérateur d'importance vitale (« **OIV** ») ou encore d'un opérateur de services essentiels (« **OSE** »).

La LPM fait donc directement et inéluctablement écho à la **directive 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 NIS »**. En effet la directive NIS tend au renforcement des capacités nationales de cybersécurité, par exemple au travers de l'obligation faite aux OSE de notifier les incidents ayant un impact sur la continuité de leurs services essentiels ou encore à l'injonction faite aux Etats membres de définir au niveau national des règles de cybersécurité auxquelles lesdits OSE devront se conformer.

Une protection des libertés fondamentales par la mise en place de garde-fous

Si le législateur a renforcé les compétences de plusieurs acteurs essentiels au maintien de la sécurité des systèmes informatiques, il a aussi corrélativement pris soin d'introduire plusieurs limites à l'exercice de ces facultés.

En effet seules les « ***données techniques*** *pertinentes* » peuvent être recueillies, analysées et conservées, étant entendu qu'elles ne peuvent pas être **conservées** pendant une durée supérieure à **six mois** par les opérateurs de communications électroniques (régime de l'article **L 33-14 du Code des postes et des communications électroniques**), et pendant une durée supérieure à **dix ans** par l'ANSSI (régime de **l'article L 2321-2-1 du Code de la défense**). Si ces données dites techniques ne comprennent pas le contenu des correspondances, elles sont toutefois diverses et comprennent par exemple les données permettant d'identifier « *l'origine de la communication et l'utilisateur ou le détenteur du système d'information affecté par l'événement détecté* », le « *routage* », le « *protocole utilisé* », mais aussi « *la date, l'horaire, le volume et la durée de chaque communication* ».

A cet égard, un parallèle peut certainement être dressé **avec l'article L 34-1 du Code des postes et des communications électroniques** relevant de la section « Protection de la vie privée des utilisateurs de réseaux et services de communication électroniques ». En effet après avoir posé le principe de l'effacement ou de l'anonymisation des données relatives au trafic par les opérateurs de communication électroniques, le législateur français autorise ces derniers « pour les besoins de la recherche, de la constatation et de la poursuite des infractions pénales » (notamment en matière de contrefaçon de droit d'auteur) à différer « les opérations tendant à effacer ou à rendre anonymes certaines catégories de données ». Cette durée de conservation exceptionnelle est alors limitée à un an par **l'article R10-13 du Code des postes et des communications électroniques**.

Il est important de noter que cette durée d'un an risque d'être invalidée par la Cour de Justice de l'Union européenne. En effet, cette dernière, après avoir invalidé dans son arrêt **« Digital Rights Ireland »** de 2014 la Directive 2006/24/CE (du Parlement européen et du Conseil du 15 mars 2006 sur la conservation de données générées ou traitées dans le cadre de la fourniture de services de communications électroniques accessibles au public ou de réseaux publics de communications), a dans ses arrêts **« Tele2 Sverige AB » et « Watson »** de 2016 invalidé respectivement les législations suédoise et britannique prises sur le fondement de cette directive, notamment au motif que la durée de conservation de ces données était disproportionnée par rapport au but poursuivi. Or en l'espèce, la durée de conservation choisie par le législateur suédois était de six mois. Par conséquent se pose légitimement la question de savoir si les dispositions adoptées par la LPM risquent ou non d'être invalidées, et celle de leur combinaison voire enchevêtrement dans la pratique, du moins en ce qui concerne la conservation des données.

Pour en revenir aux limitations apportées, le dispositif de détection d'attaques informatiques mis en place doit en outre l'être pour **une durée et un périmètre nécessairement limités.** A titre d'illustration, le dispositif de détection relevant de **l'article L 2321-2-1 du Code de la défense** doit être mis en œuvre pour une période maximale de trois mois, prorogeable en cas de persistance de la menace pour trois mois supplémentaires (**article R 2321-1-2 du Code de la défense**).

En effet cette limitation s'illustre enfin à travers le contrôle exercé par l'autorité de régulation des communications électroniques et des postes (« **ARCEP** ») sur l'ANSSI. Ainsi, cette dernière doit notifier à l'ARCEP toute décision de mettre en œuvre des dispositifs de détection d'attaques informatiques, en lui communiquant notamment un cahier des charges précisant les conditions techniques d'organisation et de fonctionnement, ainsi que le délai de mise en œuvre (**article R 2321-1-1 du Code de la défense**). Par ailleurs, la décision de proroger le dispositif de détection au-delà de trois mois doit également être notifiée à l'ARCEP (**article R 2321-1-2 du Code de la défense**). L'ARCEP se pose ainsi véritablement comme autorité de contrôle de l'ANSSI dans la mise en œuvre de ses nouveaux pouvoirs.

Il restera enfin à déterminer les interactions entre cette nouvelle législation, **la directive n°2016/680 du 27 avril 2016**, dite **directive « Police-Justice »** (relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel par les autorités compétentes à des fins de prévention et de détection des infractions pénales, d'enquêtes et de poursuites en la matière ou d'exécution de sanctions pénales, et à la libre circulation de ces données) d'une part, et le futur **règlement e-Privacy** (concernant le respect de la vie privée et la protection des données à caractère personnel dans les communications électroniques) d'autre part. Assurément, ces différentes réglementations tentent de mettre en balance les impératifs de sécurisation des réseaux de communication et de défense de la sécurité nationale d'un côté, avec les impératifs de protection de la vie privée et du secret des correspondances de l'autre.

A ce titre, tant la directive « Police-Justice » que le futur règlement e-Privacy contiennent des dispositions ayant trait à la possibilité de traiter des données à caractère personnel et corrélativement à l'obligation faite aux Etats membres de l'Union européenne de mettre en place les dispositifs et réglementations nécessaires afin que la durée de conservation de ces données ne soit pas excessive au regard de la finalité poursuivie (voir notamment les considérants 26, 41 et l'article 5 de la directive 2016/680 ; et l'article 6.1.b, 6.1.c et 6.2.a du dernier projet de règlement e-Privacy en date du 22 février 2019).

Ces nouveautés devront être suivies de près tant la sécurité informatique constitue l'un des thèmes d'actualité les plus brûlants. Ainsi, comme le souligne l'ARCEP, ce nouveau dispositif législatif risque d'impacter non seulement le bon fonctionnement des réseaux et des services de communications électroniques, mais aussi le respect de la neutralité du net ou encore le respect du secret des correspondances.

Dans l'expectative, c'est vers le recours en excès de pouvoir introduit devant le Conseil d'Etat par La Quadrature du Net, Franciliens.net et Fédérations des fournisseurs d'accès à Internet associatifs qu'il faut se tourner. Ces derniers mettent en cause en particulier l'absence d'information à l'égard des personnes concernées quant au traitement qui est fait de leurs données ainsi que la finalité poursuivie, leur déniant ainsi tout droit d'opposition et toute possibilité de recours juridictionnel, mais aussi l'imprécision et le manque de clarté caractérisant certains termes cruciaux tels que « marqueurs techniques » et « menace », ou encore les pouvoirs insuffisants de l'ARCEP qui ne dispose d'aucun pouvoir de sanction à proprement parler.

DOCUMENT 16

« 4 questions à vous poser pour bien choisir votre solution de gestion de crise » - *journaldunet.com* - 24 août 2021

Les gestionnaires de crise commencent à investir dans des solutions qui vont au-delà des systèmes de notification d'urgence, en vue de planifier, détecter, voire anticiper, et se remettre plus rapidement des évènements critiques menaçant les entreprises modernes.

Imaginez-vous allumer votre ordinateur professionnel et découvrir avec horreur ce message : "Oups ! Vous voulez récupérer vos fichiers ? Voici comment payer." Que feriez-vous ? En cas d'attaque par ransomware, l'IT et les dirigeants s'empressent de restaurer les versions précédentes du système via des solutions de cybersécurité avancées... ou songent à payer la rançon s'ils n'y arrivent pas.

Du côté des employés, les modules d'e-learning sur la prévention des cyberattaques ou les mots de passe sécurisés ne sont alors plus d'aucune utilité, car il est trop tard. Vos collaborateurs doivent continuer à servir les clients malgré l'indisponibilité complète des systèmes. Après la Covid, vous ne pouvez pas vous permettre de suspendre vos activités. Et qui protègera les emplois si votre entreprise perd de l'argent ? Les employés sont dans le noir, et le chaos est proche.

Malgré le caractère cauchemardesque de ces situations du point de vue managérial, il est surprenant de constater que les organisations ne font pas grand-chose pour éviter la confusion et les perturbations causées par ces incidents imprévus. Selon l'enquête 2019 de Gartner sur la gestion de la sécurité et du risque, 37% seulement des répondants indiquent qu'ils ont déployé un système de notification d'urgence de masse (emergency mass notification system, EMNS) complet au sein de leur organisation. Face à la diversité des défis rencontrés par toutes les entreprises en 2020, qu'il s'agisse d'incendies dévastateurs, de tensions civiles ou de la pandémie, les gestionnaires de crise commencent cependant à investir dans des solutions qui vont au-delà de ces EMNS, en vue de planifier, détecter, anticiper si possible ou gérer et se remettre plus rapidement des évènements critiques menaçant les entreprises modernes.

Beaucoup se rendent compte qu'une technologie appropriée pourrait aider à limiter toute perturbation supplémentaire lors du retour au bureau, mais, comme le montre l'exemple du ransomware, l'utilité de ces communications de crise ne se limitera pas au contexte post-Covid. Aucune organisation n'est à l'abri, quel que soit le lieu de travail de ses collaborateurs. Elles doivent déployer une solution de gestion des évènements critiques (critical event management, CEM) alignée sur les besoins de leur activité. **Pour faire le bon choix, les gestionnaires de crise doivent se poser les quatre questions suivantes :**

1. **Quelles sont vos principales préoccupations ?** En tant que chef d'entreprise, quels évènements sont susceptibles de perturber vos opérations ou de nuire à votre réputation ? S'il est possible d'élaborer des stratégies de gestion et de reprise pour les catastrophes naturelles ou autres incidents humains (par exemple, des fusillades, ou des incendies dans les locaux), il existe sans doute d'autres risques tout à fait imprévisibles. Dans ce cas, la première chose à faire sera probablement de contacter les principales parties prenantes, de les rassurer ou de leur transmettre des

consignes, et de leur demander d'en accuser bonne réception dans le cadre de votre stratégie de communication. En recensant vos employés, vous pourrez réfléchir plus efficacement ensemble à la marche à suivre pour faire face à la situation.

2. **De quels organismes réglementaires dépendez-vous ?** Certains secteurs d'activité peuvent être soumis à des exigences réglementaires spécifiques. Par exemple, les entreprises exploitant des infrastructures d'information critiques (critical information infrastructures, CII) peuvent être tenues de signaler leurs incidents de cybersécurité dans un délai donné à des autorités réglementaires sectorielles, en fournissant des détails pertinents comme la portée ou l'avancée des mesures d'endiguement et de résolution. Les équipes IT et cybersécurité de l'organisation sont alors sous pression : en parallèle à la rapidité demandée pour les remontées et le reporting aux autorités, elles doivent également fournir une vue complète sur l'état de l'incident et contribuer à la résolution rapide du problème. Compte tenu de la nature de ce type de menace, les responsables business qui s'appuient uniquement sur les communications par email et par SMS prennent des risques inutiles. Il serait plus judicieux d'opter pour une plateforme sécurisée capable de prendre en charge l'ensemble du cycle de réponse aux incidents via une vue opérationnelle commune, avec des alertes automatiques et une collaboration en direct avec les parties prenantes concernées.

3. **De qui êtes-vous responsable ?** En cas d'évènement critique susceptible d'entraîner des catastrophes, les entreprises ont un devoir de diligence envers leurs employés et les autres parties prenantes. Ici, il s'agit de recenser non seulement les personnes travaillant dans les locaux de l'organisation, mais aussi tous les professionnels sous contrat avec l'entreprise (y compris les collaborateurs en télétravail et les prestataires de services externes). Les entreprises qui s'appuient encore sur un système d'arborescence d'appels manuel devront laborieusement contacter chaque employé individuellement, ou attendre la réponse du "prochain responsable de niveau identifié". Par opposition, les plateformes de communication capables d'envoyer rapidement des alertes, d'enregistrer les accusés de réception et de faciliter l'échange d'informations critiques avec les premiers secours peuvent accélérer la réponse et donc la reprise de manière significative.

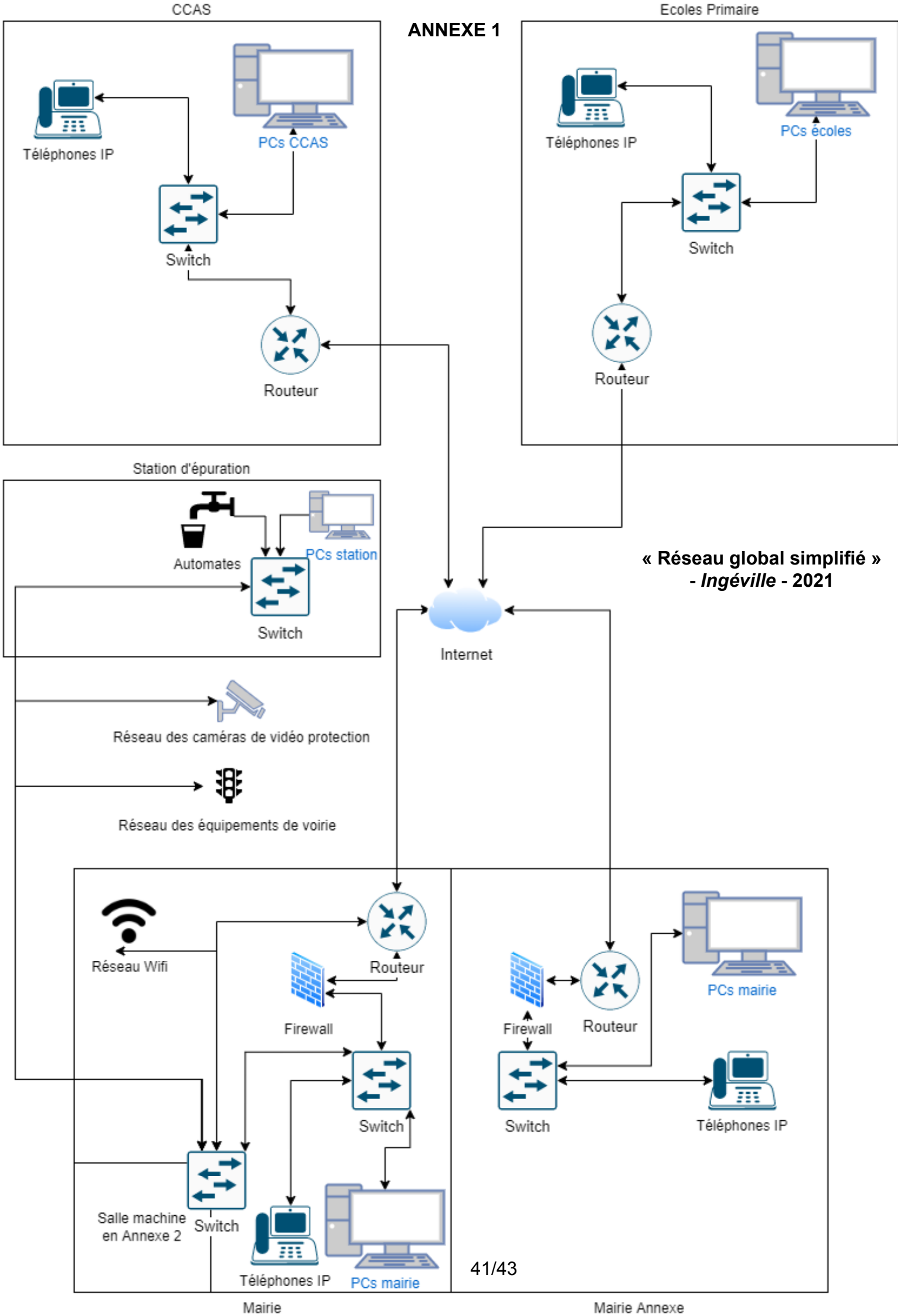
4. **Faut-il signaler les incidents à quelqu'un ?** En cas d'évènement critique (en cours ou imminent), faut-il informer directement l'équipe de management ou le conseil d'administration ? Faut-il aussi transmettre ces informations à d'autres collaborateurs et fournisseurs essentiels dans l'entreprise ? Les communications uniquement par email et SMS peuvent s'avérer problématiques, en particulier si l'évènement se produit en pleine nuit, pendant le weekend ou un jour férié. Si certaines mesures de réponse nécessitent une autorisation pour être lancées, il n'est pas question de devoir attendre le lendemain matin. Pour limiter ce risque, il serait judicieux d'opter pour une plateforme CEM fiable, robuste et capable de rassurer les parties prenantes tout en permettant des communications bidirectionnelles sécurisées, en vue de diffuser rapidement les informations et d'accélérer la réponse.

Quels sont les éléments non négociables pour les plateformes CEM ?

Quelle que soit la solution CEM choisie par les gestionnaires de crise, elle doit pouvoir prendre en charge des changements de stratégie de dernière minute "en direct", sur une plateforme accessible et sécurisée. Puisque les évènements perturbateurs évoluent constamment, les technologies doivent être en mesure de transmettre rapidement les informations. La plateforme doit pouvoir envoyer rapidement des notifications en cas d'activation, offrir des capacités de suivi des responsabilités, faciliter la collecte d'informations critiques et la gestion de la part des équipes de réponse stratégique et opérationnelles et, surtout, permettre à toutes les personnes contribuant au bon fonctionnement de l'entreprise de collaborer. Sans une plateforme sécurisée, ces mesures ne seront d'aucune utilité. Chaque plateforme doit reposer sur des normes de sécurité reconnues par le secteur et justifier d'une résilience éprouvée aux tentatives de piratage. Beaucoup de ces solutions sont aujourd'hui étayées par une équipe de services gérés capable d'offrir une assistance de confiance en cas d'urgence.

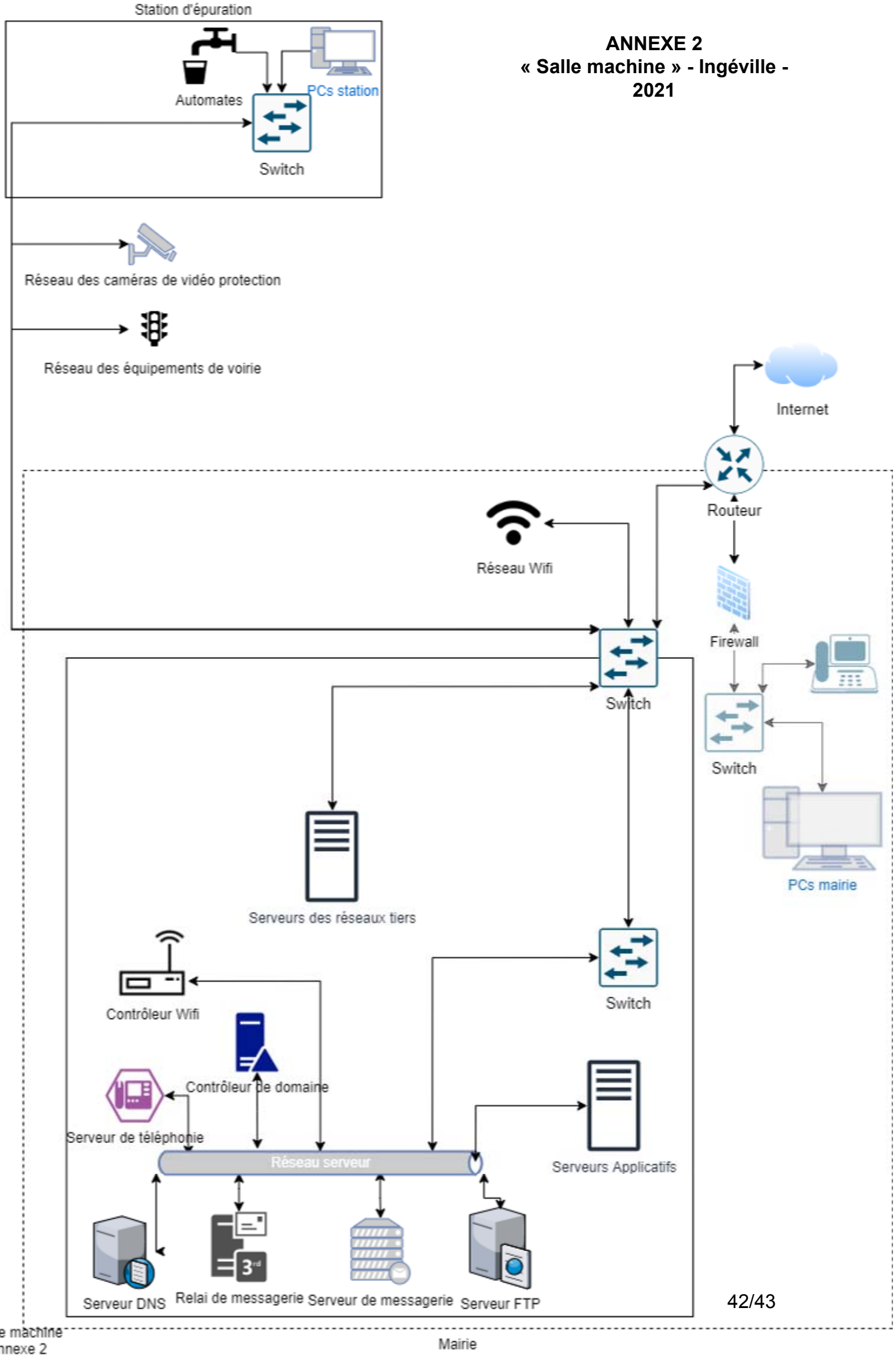
Le chaos ne provient pas de la source de la perturbation, mais des équipes qui cèdent à la panique. Avec une plateforme CEM, vous pouvez apaiser ce tumulte parmi vos parties prenantes en attendant de trouver une solution, ce qui réduira considérablement l'impact de l'évènement sur les opérations quotidiennes de votre entreprise.

ANNEXE 1



« Réseau global simplifié »
- *Ingéville* - 2021

ANNEXE 2
« Salle machine » - Ingéville - 2021



ANNEXE 3

« Le système d'Information de la commune » - *Ingéville* - 2021

La commune d'Ingéville compte 100 000 habitants. La mairie emploie environ 800 agents.

Le système d'information s'est construit pour répondre aux exigences réglementaires au fur et à mesure de leurs arrivées.

Une trentaine d'agents travaillent à la Direction des Systèmes d'information. Ils gèrent les 1 000 terminaux (postes de travail, équipements mobiles, IOT…) de la collectivité, répartis dans les sites et les écoles, ainsi que toute l'infrastructure technique. Il n'est fait appel à la prestation qu'en cas de difficulté majeure.

Les systèmes sont à jour et les PC disposent d'un antivirus.

Il n'existe pas de VLAN, mais les équipements réseau (de même marque) supportent ce type de segmentation.