Les Petites Affiches de Vaucluse depuis 1839

Ecrit par le 23 novembre 2024

Piratages des collectivités : à qui le tour ?

Le groupe Veolia et l'AMV (Association des maires de Vaucluse) ont organisé une table-ronde sur le thème : 'Cybersécurité et eau : collectivités, services publics, entreprises… Tous concernés'. Cette matinale, qui s'est tenue à l'Isle-sur-la-Sorgue, a été notamment l'occasion de rappeler les enjeux majeurs liés à la cybersécurité et de donner les clés pour pouvoir faire face à cette menace qui ciblent de plus en plus des collectivités de plus en plus en première ligne.

« Toutes les organisations, quelles que soient leurs tailles et leurs domaines d'activité sont potentiellement concernées par les menaces de cyberattaques, expliquait Olivier Campos, directeur

Les Petites Affiches de Vaucluse depuis 1839

Ecrit par le 23 novembre 2024

Veolia eau Provence-Alpes en préambule de cette 4e matinale climat organisé dans la Région Sud. Il est désormais essentiel pour les entreprises et les collectivités, dans le domaine de l'eau notamment, de prendre la pleine mesure cyber et se protéger. Ces rendez-vous, à destination des acteurs de premières lignes ont pour objectifs de favoriser les échanges, les interrogations, les retours d'expériences entre les différents experts qui interviennent sur le sujet mais également avec les élus et les représentants des collectivités présents. »

> « Les cyberattaquants s'en prennent à ceux qui sont le moins bien protégés. »
>
> *Célia Nowak, déléguée régionale Paca de l'ANSSI*

Données compromises pour 1 français sur 2

Après un mot d'accueil de Pierre Gonzalvez, maire de l'Isle-sur-la-Sorgue et président de l'AMV, sur la nécessité pour les collectivités de se prémunir contre les cyberattaques et leurs conséquences, les six intervenants ont dressé un état des lieux complet de la menace.

A une période où selon la CNIL (Commission nationale de l'informatique et des libertés) 1 français sur 2 a vu ses données personnelles compromises à la suite d'attaque et où plus de 2 500 actions de suspension de sites illicites utilisés pour de vastes campagnes d'hameçonnage ont été réalisées contre le cybersquattage de noms de domaines des collectivités, Célia Nowak, déléguée régionale Paca à la sécurité numérique pour l'Agence nationale de la sécurité des systèmes d'information (ANSSI) a rappelé la réglementation actuelle ainsi que les techniques des cyberpirates. Des méthodes que l'on pourrait assimiler à « une logique de la pêche au chalut » afin de ratisser le plus large possible pour s'attaquer aux plus 'faibles', c'est-à-dire ceux qui sont le moins bien protégés. Avec un souci de rentabilité, en jouant sur la masse des attaques, qui a pour conséquence qu'il n'est nul besoin d'être une cible directe pour en être la victime.

> « On n'est jamais assez préparé »,
>
> *Jérôme Poggi, Responsable de la sécurité des systèmes d'information à la ville de Marseille*

Le coût de la cybercriminalité explose en France

Epée de Damoclès 2.0 ?

Un risque permanent, sorte de d'épée de Damoclès 2.0, que confirme le commandant Nidhal Ben Aloui, conseiller cyber du commandant de région de gendarmerie Paca, chef de la section cyber et anticipation

Les Petites Affiches de Vaucluse depuis 1839

Ecrit par le 23 novembre 2024

cyber de la division régionale des réserves : « Au niveau financier le ransomware est le plus rentable. La France a versé 888 M€ de rançon en 2022. »
Dans tous les cas, le commandant de gendarmerie assure qu'il est impératif de prévenir les autorités, que ce soit pour mieux se défendre ou tenter d'identifier les attaquants pour les mettre hors d'état de nuire ou limiter les effets. « Il est très important de réagir vite », explique le militaire.

> « Il faut pouvoir continuer à fonctionner en mode dégradé. »
>
> *Franck Galland, directeur général d'Environmental Emergency & Security Services*

Une rapidité de réaction que confirme Jérôme Poggi, RSSI (responsable de la sécurité des systèmes d'information) à la ville de Marseille dont les services ont été victime d'une cyberattaque le 14 mars 2020 à 7h31.
Après avoir témoigné de la difficulté de se remettre de telles attaques, plusieurs mois, il a insisté sur les conséquences parfois inattendues qu'elles pouvaient avoir sur la bonne marche de la collectivité (gestion des cimetières, Etat-civil, impact humain, sentiment de remise en cause…). « On n'est jamais assez préparé », prévient-il.
« Il faut effectivement prendre en compte le temps long d'une telle crise et donc anticiper pour pouvoir continuer à fonctionner en mode dégradé », estime pour sa part Franck Galland, directeur général d'Environmental Emergency & Security Services et président-fondateur d'Aqua Sûreté, expert en sécurité des infrastructures hydrauliques.
C'est avec cette volonté d'anticipation, qu'en vue des JO de Paris, cet expert de la sûreté dans le domaine de l'eau a participé à un exercice de crise d'une attaque cyber dans une station d'épuration Veolia en Île-de-France.

> « Nous proposons des mesures techniques de protection en faisant très attention aux accès à distance demandés par les clients. »
>
> *Meriem Riadi, directrice des systèmes d'information Veolia Eau France*

Sécuriser l'approvisionnement en eau
Chez Veolia, cette prévention de la menace passe notamment par un accompagnement des collectivités partenaires.
« Tout d'abord, nous mettons en place une forte sensibilisation aux aspects humains, insiste Meriem Riadi, directrice des systèmes d'information Veolia Eau France. Ensuite nous proposons des mesures techniques de protection en faisant très attention aux accès à distance demandés par les clients, car ouvrir des portes et créer des interconnexions a des conséquences. On protège aussi les systèmes informatiques dans l'usine via des antivirus. Il faut aussi détecter les incidents qui peuvent arriver et enfin, se préparer opérationnellement en ayant des sauvegardes, être capable de les restaurer, mener des exercices de crise… »

Les Petites Affiches de Vaucluse depuis 1839

Ecrit par le 23 novembre 2024

> « Cette connectivité expose ces systèmes à des cyberattaques potentielles. »
>
> *Olivier Campos, directeur Veolia eau Provence-Alpes*

« Les services d'eau et d'assainissement étant vitaux pour notre société, ils sont également vulnérables aux menaces cybernétiques, ce qui rend la cybersécurité d'une importance capitale pour Veolia, rappelle Olivier Campos, le directeur Provence-Alpes. Les systèmes de contrôle industriel utilisés pour gérer les infrastructures d'eau et d'assainissement sont de plus en plus connectés à internet pour des raisons d'efficacité et de commodité. Cependant, cette connectivité expose ces systèmes à des cyberattaques potentielles. Une attaque réussie pourrait perturber l'approvisionnement en eau ou l'assainissement, avec des conséquences potentiellement désastreuses pour la santé publique et l'environnement. Le sujet est également sensible car Veolia gère une grande quantité de données sensibles sur ses clients. »

> « Il ne viendrait jamais à l'idée pour un élu d'ouvrir un établissement qui n'est pas aux normes sans contrôle préalable. »
>
> *Léo Gonzales, PDG de Devensys cybersécurité*

Quelles sont les solutions et que faire en cas d'attaque ?
« Il faut responsabiliser et sensibiliser les dirigeants ou les élus aux risques cyber pour qu'ils prennent leurs responsabilités, mettent les moyens humains, techniques et financiers en face du risque, précise Léo Gonzales, PDG de Devensys cybersécurité à Montpellier. C'est exactement ce qu'il se passe pour le risque juridique, ou encore avec le risque sûreté (normes ERP pour les bâtiments, sécurité incendie, etc.) Il ne viendrait jamais à l'idée pour un dirigeant ou élu d'ouvrir un établissement qui n'est pas aux normes sans contrôle préalable (consuel, pompiers, etc.). Idem avec le contrôle technique et l'entretien des voitures, ou les équipements de sécurité préventive (airbag, radar avec freinage auto, etc.). Pourtant, c'est comme la cyber… on investit pour 'rien' au départ. Mais ne pas prévoir à la conception les buses d'extinction incendie dans un hôtel, ou les portes coupe-feu, cela couterait extrêmement cher de le rajouter après. »
Des diagnostics gratuits existent rappellent Célia Nowak pour l'ANSSI ainsi que le commandant Nidhal Ben Aloui pour la gendarmerie.

Les Petites Affiches de Vaucluse depuis 1839

Ecrit par le 23 novembre 2024

Les intervenants (de gauche à droite) : Meriem Riadi, directrice des systèmes d'information Veolia Eau France, Jérôme Poggi, responsable de la sécurité des systèmes d'information à la ville de Marseille, Léo Gonzales, PDG de Devensys cybersécurité, Franck Galland, directeur général d'Environmental Emergency & Security Services et président-fondateur d'Aqua Sûreté, commandant Nidhal Ben Aloui, conseiller cyber du commandant de région de gendarmerie Paca, Célia Nowak, déléguée régionale Paca de l'ANSSI, Pierre Gonzalvez, maire de l'Isle-sur-la-Sorgue et président de l'AMV, ainsi que Olivier Campos, directeur Veolia eau Provence-Alpes.

« Nous disposons de guides et d'outils mis à disposition des collectivités dans les domaines de la prévention, de la détection et de la réaction », complète la déléguée régionale de l'ANSSI qui peut s'appuyer sur le CSIRT (Computer security incident response team) de Paca qui traitent les demandes d'assistance des acteurs de taille intermédiaire (PME, ETI, collectivités territoriales et associations).
Même offre complémentaire pour les gendarmes : « nous proposons des supports d'informations lors des situations de crise ainsi que les listes de contacts en cas d'urgence. Nous avons aussi formé des référents dans les brigades de la Région Sud afin d'apporter des réponses adaptées en fonction des profils des personnes qui nous sollicitent. »

> « La question n'est pas de savoir si vous subirez une cyberattaque, mais quand ? »

S'adapter en permanence aux nouveaux défis

S'il est nécessaire de dresser un diagnostic de sa vulnérabilité face aux cyberattaques ainsi que de savoir comment réagir « une poignée d'actions 'défensives' constituent déjà la clef pour limiter drastiquement les risques (sauvegardes, cloisonnement, antivirus), résume Léo Gonzales de Devensys cybersécurité. Les

Les Petites Affiches de Vaucluse depuis 1839

Ecrit par le 23 novembre 2024

attaquants innovent en permanence et il faut s'adapter en face. Il y a forcément une certaine latence dans la réponse, et un coût financier et humain. L'objectif étant de rendre l'attaque plus complexe, plus longue, plus chère. »
De faire en quelques sorte, que le cyberpirate passe son chemin pour, qu'à l'image d'un cambrioleur qui évite une maison avec un chien ou une alarme, il s'oriente vers un 'voisin' moins protégé.
« On doit aussi penser à des systèmes de détection, pour le cas où cela devient trop tard, afin que les 'voleurs' sachent que la 'police' arrive très rapidement, et qu'ils n'aient pas le temps de faire trop de dégâts », poursuit Leo Gonzales.

> « Il ne faut pas rester seul. »
>
> *Commandant Nidhal Ben Aloui, conseiller cyber du commandant de région de gendarmerie Paca,*

Au final, l'ensemble des intervenants s'accordent sur un point : « La question n'est pas de savoir si vous subirez une cyberattaque, mais quand ? »
C'est pour cela qu'à l'image de la Ville de Marseille et de son responsable de la sécurité des systèmes d'information, la collectivité phocéenne est sur le qui-vive. : « Nous pratiquons des exercices en permanence, confie Jérôme Poggi. On teste les sauvegardes, on teste les procédures, on teste la réactivité des équipes, on teste encore et encore pour faire face à toutes les éventualités. »
Cependant, si les solutions peuvent apparaître uniquement techniques, il ne faut pas négliger l'impact humain. « Il ne faut pas rester seul. Il faut savoir s'entourer, insiste le commandant Nidhal Ben Aloui. Surtout si parfois à tort, on pense être bien préparé à une attaque. »
Et le gendarme, comme plusieurs intervenants, d'évoquer les conséquences humaines (dépression, burnout et même suicide) de certaines de ces attaques pour les dirigeants, élus ou chefs de service qui s'en sentent responsables.

Réglementations sur la protection des données & cybersécurité

Cybersécurité : les collectivités vauclusiennes

Les Petites Affiches de Vaucluse depuis 1839

Ecrit par le 23 novembre 2024

ne sont pas à l'abri

La section départementale de Vaucluse du Syndicat des directeurs généraux des collectivités territoriales (SNDGCT) vient d'organiser une rencontre sur le thème de la cybersécurité. L'occasion pour Kevin Heydon, délégué à la sécurité numérique de l'Anssi en Paca et en Corse, ainsi que Karine Icard, présidente du SNDGCT 84*, de sensibiliser sur les risques de cyberattaque sur le secteur public.

Paralysie des services, pertes de données essentielles : le secteur public est aujourd'hui de plus en plus la cible des cyberattaquants. En 2020, en France, 30% des collectivités territoriales ont été victimes d'une attaque de type rançongiciel (envoi d'un logiciel malveillant de chiffrage des données de quelqu'un dans le but de lui extorquer de l'argent). Un chiffre en hausse de 50 % par rapport à 2019 selon une étude du Clusif. Pour autant, il y encore peu de temps la cybersécurité ne semblait pas encore être une préoccupation centrale des collectivités territoriales. Ainsi, selon un sondage Ifop pour l'Observatoire des politiques publiques réalisé en janvier 2020, seuls 33 % des fonctionnaires territoriaux interrogés déclaraient que leur organisation avait mis en place un programme de cybersécurité.

Depuis, la mobilisation des associations d'élus et structure d'agents territoriaux comme le SNDGCT

Les Petites Affiches de Vaucluse depuis 1839

Ecrit par le 23 novembre 2024

notamment a permis une certaine prise de conscience des collectivités territoriales. Ces dernières tâchent donc maintenant de se prémunir au mieux face à ce phénomène expansionniste avec des pratiques numériques réinterrogées, des actions de sensibilisation, un risque numérique intégré au plan de continuité d'activité, etc.

Dans cette logique, l'Association des maires de France (AMF) a ainsi édité en novembre 2020 un guide intitulé 'Cybersécurité : toutes les communes et les intercommunalités sont concernées' regroupant une trentaine de recommandations et de bonnes pratiques en matière de sécurité numérique. De son côté, le sénat s'est également penché sur cette problématique, en octobre dernier, lors d'une table-ronde sur 'Les collectivités territoriales face au défi de la cybersécurité'.

> **« La question n'est plus de savoir 'si' les collectivités seront la cible d'une cybermalveillance, mais plutôt 'quand'. »**

« L'objectif des cyberattaquants est de capter de la donnée, de la bloquer et ce, à des fins lucratives. Aujourd'hui, la question n'est plus de savoir 'si' les collectivités seront la cible d'une cybermalveillance, mais plutôt 'quand' », expliquent Karine Icard, présidente du SNDGCT 84 et directrice générale des services de la Communauté d'agglomération Luberon Monts de Vaucluse, ainsi que Kevin Heydon, délégué à la sécurité numérique de l'Anssi en Paca et en Corse, lors de la rencontre de sensibilisation 'Cybersécurité : les collectivités territoriales du Vaucluse en parlent…' qui vient de se tenir dans les locaux du syndicat des eaux Durance Ventoux à Cheval-Blanc.

Un nouveau fléau

« Ce nouveau fléau peut entraîner une paralysie des services publics, entacher lourdement l'image même de ces derniers et engendrer des dépenses élevées », poursuivent les organisateurs de ce rendez-vous auquel a participé une trentaine de dirigeants provenant de communes, d'intercommunalités ou de syndicats du territoire de Vaucluse.

Localisation des collectivités territoriales françaises ayant été victime d'une attaque au rançongiciel en 2020.

Au travers des témoignages des directeurs généraux des services, Emmanuel Bohn de la Communauté de communes du Pays d'Apt et Vincent Rey de la ville de Morières-lès-Avignon, dont les collectivités ont été victime « de perte totale de leurs données nécessitant une reconstruction longue de leur système d'information », les participants ont pu ensuite travailler autour de la notion du risque numérique en s'interrogeant sur les moyens pour s'en prémunir, les bonnes pratiques à déployer, les leviers à activer ou bien encore les bons réflexes à avoir en cas de cyberattaque ?

La piste d'une protection collective ?

Bien souvent, le manque de budget et de personnes qualifiées justifie en partie les difficultés des

Les Petites Affiches de Vaucluse depuis 1839

Ecrit par le 23 novembre 2024

collectivités territoriales en matière de cyberprotection de leurs outils et données numériques.
« Faute de temps mais également de compétences et de ressources humaines qualifiées, les petites communes se contentent parfois d'installer ponctuellement un anti-virus, alors que la cybersécurité doit être mise à jour en permanence, constatent les travaux du sénat. Or, la pénurie de compétences est telle que l'Anssi a lancé un 'observatoire des métiers de la cybersécurité' afin d'aider les acteurs concernés dans leur politique de recrutement et de formation. Dans ce contexte, la mutualisation au plus près des collectivités concernées s'avère être un choix judicieux pour mettre en commun les efforts, affronter les pénuries de professionnels qualifiés et ainsi mettre en place une protection collective. »
Pour cela, les responsables et DGS des collectivités de Vaucluse peuvent ainsi compter sur le l'accompagnement de l'Anssi et du SNDGCT 84 des acteurs territoriaux dans la sécurisation de leur développement numérique.

Le SNDGCT 84 et l'Anssi lors de la rencontre de sensibilisation sur le thème 'Cybersécurité : les collectivités territoriales du Vaucluse en parlent…' qui s'est tenue dans les locaux du syndicat des eaux Durance Ventoux à Cheval-Blanc.

**Le SNDGCT a été créé en 1948. L'organisation professionnelle compte aujourd'hui près de 4 000 adhérents au niveau national. Elle se compose d'Unions régionales, elles-mêmes divisées en Sections départementales. Karine Icard est présidente de la section départementale de Vaucluse depuis septembre 2020. Autour d'elle, un bureau avec 3 membres, Gilles Meunier, directeur général adjoint de la Communauté de communes de Pays des Sorgues Monts de Vaucluse, Johanna Quijoux, directrice générale des services de Piolenc et Emmanuelle Licitri, directrice générale adjointe mutualisée Ville de Cavaillon et Luberon Monts de Vaucluse Agglomération.*

Les Petites Affiches de Vaucluse depuis 1839

Ecrit par le 23 novembre 2024

Rile, Cybersécurité, risques et bonnes pratiques en entreprise

Le Rile, pépinière d'entreprise et la Communauté d'agglomération des Sorgues-du-Comtat proposent des rencontres professionnelles sur le thème : 'La cyber sécurité, les risques et les bonnes pratiques en entreprise.

Au programme

Bastien Pinheiro, pour Pinheiro création spécialiste de l'aménagement paysager, travaille des systèmes d'irrigation et du traitement des eaux ; créé des toitures et murs végétaux pour réguler les eaux

Ecrit par le 23 novembre 2024

pluviales, propose de filtrer l'eau et l'air tout en améliorer le bilan carbone.

Yannis Martin, président de Nistin conseil, spécialiste de la gouvernance, du management de la transition et de la sécurité numérique. L'opportunité 'cyber' : vecteur de développement économique durable. La transformation numérique s'accompagne des risques de cybersécurité réels ; la réduction significative du risque est possible par l'application des 12 bonnes pratiques ANSSI. L'anticipation des incidents en amont permet une meilleure protection.
Puis échange entre les participants et verre de l'amitié.

Les infos pratiques
Jeudi 7 avril à 18h30, au siège de la Communauté d'agglomération à Monteux. 340, boulevard d'Avignon. Inscription ici.
MH