Les Petites Affiches de Vaucluse depuis 1839

Ecrit par le 23 novembre 2024

Cybersécurité : les collectivités vauclusiennes 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.

Les Petites Affiches de Vaucluse depuis 1839

Ecrit par le 23 novembre 2024

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

Les Petites Affiches de Vaucluse depuis 1839

Ecrit par le 23 novembre 2024

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

Scannez avec prudence, les arnaques aux QR codes fleurissent

Les QR codes font fureur et les escrocs l'ont remarqué. « Méfiez-vous de ces petits carrés noirs et blancs », prévient Benoit Grunemwald, expert en cybersécurité chez Eset France.

Les QR codes ont le vent en poupe. Ces modestes carrés existent peut-être depuis 1994, mais ils sont réellement devenus célèbres depuis la crise du Covid-19. Aujourd'hui, vous pouvez les apercevoir partout, les codes étant utilisés pour l'affichage des menus de restaurants jusqu'aux transactions sans contact en passant par des applications de partage de contacts.
Toutefois, comme toute autre technologie courante, l'utilisation généralisée des QR codes a également attiré l'attention des escrocs, à des fins criminelles. Cette tendance a même suscité une alerte de la part

Les Petites Affiches de Vaucluse depuis 1839

Ecrit par le 23 novembre 2024

du FBI (Federal bureau of investigation) aux États-Unis. Comment les fraudeurs utilisent-ils les codes à des fins illicites ?

Qu'est-ce qu'un QR code et comment fonctionne-t-il ?
Abréviation de 'Quick response', un QR code est un type de code-barres interprétable par une machine instantanément. Un QR code peut contenir jusqu'à 4 296 caractères alphanumériques, ce qui permet un décodage facile par l'appareil photo d'un smartphone.
Les chaînes de texte qui sont codées dans un QR code peuvent contenir une variété de données. L'action déclenchée par la lecture d'un QR code dépend de l'application qui interagit avec ledit code. Les codes peuvent être utilisés pour naviguer vers un site web, télécharger un fichier, ajouter un contact, se connecter à un réseau Wi-Fi et même effectuer des paiements. Les QR codes sont très polyvalents et peuvent être personnalisés pour inclure des logos. Les versions dynamiques des QR codes vous permettent même de modifier le contenu ou l'action à tout moment. Cette polyvalence peut toutefois être une arme à double tranchant.

Comment les QR codes peuvent être exploités ?
Le grand nombre de cas d'utilisation des QR codes (et le potentiel d'utilisation abusive) n'échappe pas aux fraudeurs. Voici comment les cybercriminels peuvent détourner les codes pour voler vos données et votre argent :

1. **Redirection vers un site web malveillant pour voler des informations sensibles :** Les attaques d'hameçonnage ne se propagent pas uniquement par e-mails, des messages instantanés ou des SMS. Tout comme les attaquants peuvent utiliser des publicités malveillantes et d'autres techniques pour vous diriger vers des sites frauduleux, ils peuvent faire de même avec les codes QR.

2. **Téléchargement d'un fichier malveillant sur votre appareil :** De nombreux bars et restaurants utilisent des QR codes pour télécharger un menu au format PDF ou installer une application vous permettant de passer une commande. Les attaquants peuvent facilement falsifier le QR code pour vous inciter à télécharger un fichier PDF malveillant ou une application mobile malveillante.

3. **Déclencher des actions sur votre appareil :** Les QR codes peuvent déclencher des actions directement sur votre appareil, ces actions dépendant de l'application qui les lit. Cependant, il existe certaines actions de base que tout lecteur QR est capable d'interpréter. Il s'agit notamment de la connexion de l'appareil à un réseau Wi-Fi, de l'envoi d'un e-mail ou d'un SMS avec un texte prédéfini, ou de l'enregistrement des informations de contact sur votre appareil. Bien que ces actions ne soient pas malveillantes en soi, elles peuvent être utilisées pour connecter un appareil à un réseau compromis ou envoyer des messages en votre nom.

4. **Détourner un paiement :** La plupart des applications financières permettent aujourd'hui d'effectuer des paiements au moyen de codes QR contenant des données appartenant au destinataire de l'argent. De nombreux magasins vous affichent ces codes pour ainsi faciliter la transaction. Cependant, un attaquant pourrait modifier ce QR avec ses propres données et recevoir des paiements sur son compte. Il pourrait également générer des codes avec des demandes de collecte d'argent pour vous

Les Petites Affiches de Vaucluse depuis 1839

Ecrit par le 23 novembre 2024

tromper.

5. Voler votre identité : De nombreux QR codes sont utilisés comme certificat pour vérifier vos informations, comme votre carte d'identité ou votre carnet de vaccination. Dans ces cas, les QR codes peuvent contenir des informations aussi sensibles que celles contenues dans votre pièce d'identité ou votre dossier médical, qu'un attaquant pourrait facilement obtenir en scannant le QR code.

Nous avons adopté les QR codes dans notre vie quotidienne. Et comme avec toutes les nouvelles pratiques, il nous faut prendre de nouvelles habitudes pour rester vigilants. Chaque nouvelle technologie amène son lot d'avantages mais aussi de menaces.

Benoit Grunemwald, expert en cybersécurité chez Eset France

Cybersécurité et postes de travail : vers une stricte limitation aux usages professionnels ?

Les Petites Affiches de Vaucluse depuis 1839

Ecrit par le 23 novembre 2024

À quelques exceptions près, en particulier dans les secteurs les plus sensibles, l'habitude est souvent prise d'utiliser son poste de travail professionnel pour certains (si ce n'est tous) usages personnels. D'autant plus lorsqu'il s'agit d'un poste portable. Or, ce sont ces postes qui constituent le vecteur le plus 'efficace' des malveillances à l'encontre du SI (Système d'information) des organisations. Dès lors, peut-on imaginer un monde aux usages numériques professionnels et personnels strictement étanches ?

Postes de travail : une porte ouverte vers l'ensemble du SI

Par principe, les attaques malveillantes à l'encontre des entreprises ou administrations ont généralement deux objectifs, bien souvent couplés : l'argent et l'information. Et dans tous les cas, elles sont menées via des méthodes industrielles, assurant efficacité et reproductibilité aux assaillants.

Parmi ces méthodes, le piratage de réseaux Wifi non protégés est efficace, mais il nécessite un accès physique. Les attaques de serveurs mal protégés peuvent créer des dégâts, mais ils restent souvent circonscrits à leurs environnements applicatifs. Il est aussi possible de s'attaquer au VPN-SSL de l'organisation lorsque celui-ci est vulnérable. Mais rien n'est comparable à la réussite du ciblage utilisateurs, par mail (phishing) ou surf (implantation de logiciels malveillants sur les postes via des sites web corrompus).

Même bien protégé, le poste utilisateur reste de loin le plus vulnérable car, par définition, il est connecté

Les Petites Affiches de Vaucluse depuis 1839

Ecrit par le 23 novembre 2024

à 'l'Active directory' de l'entreprise (l'outil d'annuaire le plus représenté sur le marché). Et cette solution, malgré l'effort des développeurs, reste sujette à de nombreuses vulnérabilités permettant l'accès distant et l'élévation de privilèges depuis un compte utilisateur. C'est la porte ouverte au fameux « admin access » et à l'ensemble des données de l'entreprise.

Une cybersécurité proactive et transparente pour l'usager

Pour se prémunir au maximum de ces risques, rien de plus simple a priori : en plus des logiciels de cybersécurité dédiés, il suffirait de maintenir ses postes de travail à jour, pour éviter l'exploitation de failles connues. Certes, mais c'est encore sans compter sur les failles Zero Day, sur lesquelles les cyberattaquants sont de plus en plus productifs.

Pour contrer ces risques, la mise en œuvre de solutions capables de bloquer des actions non habituelles des applications ou du système demeure une pratique efficace, car proactive. Par essence en effet, les logiciels malveillants ont des comportements très spécifiques, cherchant tout type d'ouverture pour s'introduire et modifier les systèmes.

Dans tous les cas en revanche, ces outils doivent être le plus transparent possible pour l'usager, afin qu'il puisse accomplir sereinement ses tâches quotidiennes et ne pas perdre en productivité du fait de blocages permanents. Ce qui ne doit en rien l'empêcher de rester vigilant pour autant.

Sébastien Viou.

Au-delà des chartes d'utilisation, vers un usage strictement professionnel des postes de travail ?

En dehors de quelques secteurs manipulant des données sensibles où les postes de travail sont très verrouillés et limitent au strict minimum les usages, nombreux sont les utilisateurs à se servir de leur poste de travail pour leurs usages personnels. Allant souvent même jusqu'à autoriser leurs enfants à s'en servir, ou jouer en réseau avec. Une situation sans doute encore exacerbée avec l'accélération du

Les Petites Affiches de Vaucluse depuis 1839

Ecrit par le 23 novembre 2024

télétravail, quand ce n'est pas l'entreprise qui demande au collaborateur d'utiliser sa machine personnelle pour ne pas avoir à payer une machine professionnelle.
Si un certain nombre d'organisations ont mis en place des chartes d'usages et des outillages informatiques mis à disposition de leurs collaborateurs, dans les faits, peu d'entre elles appliquent des sanctions en cas de comportements imprudents, même s'il en résulte des situations particulièrement graves pour l'ensemble du système d'information (perte, vol de données ou ransomwares, etc.).
Avec le développement de l'informatique domestique (smartphones, tablettes, PC, accès internet), associé à des risques numériques toujours plus importants pour les organisations, peut-être est-il temps pour ces dernières de limiter strictement aux usages professionnels les outils numériques de l'entreprise mis à disposition de leurs collaborateurs.
Dans ce cas, on parlerait d'outils numériques de service (uniquement à usage professionnel) et non plus d'outils numériques de fonction (à usage « global » du salarié). Cela ne résoudra pas tous les problèmes en matière de cybersécurité, mais pourrait a minima contribuer à cyber-responsabiliser les collaborateurs et ainsi à l'amélioration des usages.

Tribune de Sébastien Viou, directeur cybersécurité produit et 'cyber-évangéliste' chez Stormshield, spécialiste et éditeur français de logiciels spécialisés en sécurité informatique