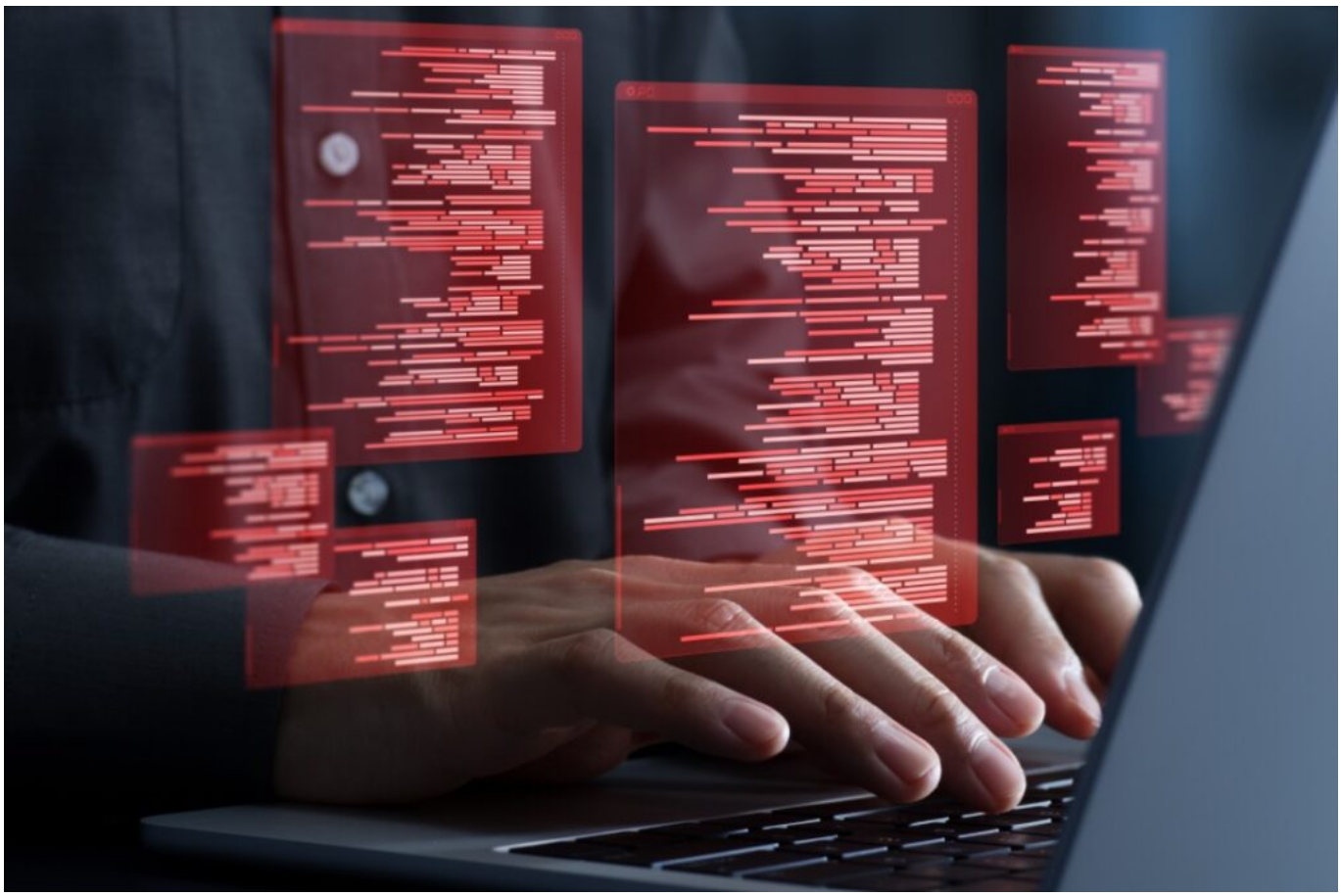
Les Petites Affiches de Vaucluse depuis 1839

Ecrit par le 2 novembre 2026

Bollène : tentative de cyberattaque contre Egide



La société vauclusienne Egide vient de faire l'objet d'une cyberattaque. Le spécialiste mondial des boîtiers et solutions d'interconnexions hermétiques pour composants électroniques sensibles précise que l'incident, détecté au niveau d'un prestataire, « est susceptible d'avoir affecté certains systèmes du site de Bollène. Les équipes techniques d'Egide SA sont intervenues sans délai pour circonscrire l'incident et travaillent en lien étroit avec le prestataire concerné. Dès la détection de cette intrusion, Egide a également mobilisé des experts en cybersécurité externes. »
Cet incident a entraîné une interruption partielle du site de production de Bollène, mise en œuvre par mesure de prévention.

Egide porte plainte
« Les investigations techniques en cours visent notamment à déterminer la nature et le périmètre des

Les Petites Affiches de Vaucluse depuis 1839

Ecrit par le 2 novembre 2026

données éventuellement concernées, poursuit l'entreprise du secteur de la défense. Egide accorde une attention constante à la sécurité des données de ses parties prenantes dans la conduite de cette enquête et les équipes de sécurité d'Egide sont pleinement mobilisées sur ce sujet. Egide a notifié les autorités compétentes, en particulier la CNIL, et a déposé plainte auprès des autorités judiciaires compétentes. »

Créé en 1986 dans les Yvelines, Egide a déménagé son siège social à Bollène en 2010 où la société dispose d'un site de production dans la zone industrielle du Sactar. S'y trouve un bâtiment d'environ 5 700m², équipé d'une salle blanche de 500m² pour le traitement de la céramique crue. Le groupe dirigé depuis un peu plus d'un an par Ignace Dupon est aussi présent aux Etats-Unis avec une usine dans le Maryland.

Le site des impôts piraté vu par Wingz pour L'Echo du Mardi

Les Petites Affiches de Vaucluse depuis 1839

Ecrit par le 2 novembre 2026



Les Petites Affiches de Vaucluse depuis 1839

Ecrit par le 2 novembre 2026



Thucy : protéger les entreprises contre les

Les Petites Affiches de Vaucluse depuis 1839

Ecrit par le 2 novembre 2026

cyberattaques



La cybersécurité est une problématique essentielle à prendre en compte par les entreprises. Thucy est une société basée à Carpentras et spécialisée dans ce domaine technique, avec l'apport de solutions préventives et curatives contre des attaques éventuelles. Trois jeunes associés développent ce concept.

En 2020, Samy Scanna et Sylvain Borreda décident de lancer leur entreprise en cybersécurité. Les deux copains viennent d'obtenir leur Master en cybersécurité, sous forme d'apprentissage à Pertuis auprès de la CCI. « Au lancement de l'entreprise, nous n'avions pas de local professionnel et nous travaillions chez nous à Carpentras. » L'entreprise se développe peu à peu, elle peut alors embaucher un apprenti en 2022.

Les Petites Affiches de Vaucluse depuis 1839

Ecrit par le 2 novembre 2026

Un troisième associé

En 2023, les deux jeunes créateurs rencontrent Thibaud Perrard. Ils décident alors de créer un trio d'associés en créant l'entreprise Thucy, qui vient de la fusion de Volt Security, créée par Samy et Sylvain, et Thucidide, lancée par Thibaud.

Quatrième année à Mon premier bureau

L'entreprise s'est installée en 2022 au Château Durbesson qui abrite Mon premier bureau, loué pour les créateurs d'entreprise de services par le service Développement économique de la CoVe. « Cela été une belle opportunité pour nous sur l'aspect financier car le tarif des loyers est avantageux. Nous sommes dans deux bureaux ici jusque mai 2026 car la durée maximale d'occupation est de 4 ans », explique Samy Scanna qui est basé à Carpentras avec Lana qui est en apprentissage, les deux autres associés étant allés s'installer à Aix-en-Provence. Le projet est de créer rapidement un bureau sur cette ville des Bouches-du-Rhône.



Samy Scanna loue son bureau à Carpentras à la CoVe. ©Olivier Muselet / L'Echo du Mardi

Le concept

« En premier lieu, je veux dire que nous travaillons toujours dans une dimension éthique. Notre métier a deux facettes : l'offensif et le défensif. Pour l'offensif, nous mettons dans la peau d'un hacker. Nous attaquons les entreprises en recherchant les failles de sécurité. Une fois ce diagnostic établi avec une cartographie de tous les vecteurs d'attaque, nous les aidons à corriger ces vulnérabilités informatiques », indique Samy Scanna. Un rapport est alors établi avec des préconisations et un plan d'action proposés.

Les Petites Affiches de Vaucluse depuis 1839

Ecrit par le 2 novembre 2026

Un accompagnement est également assuré pour la mise en place de ces corrections avec les outils nécessaires. Cette prestation concerne plutôt les entreprises d'une certaine taille, comme les ETI ou les grands groupes.

L'entreprise est référencée en tant que prestataire Cybermalveillance, label donné par l'État. Cela lui permet d'être plus facilement contacté par les entreprises grâce à une plate-forme dédiée. Il s'adresse plus particulièrement aux particuliers, au TPE, et aux PME.

L'autre label de l'entreprise est ExpertCyber, label délivré par l'ANSSI, Agence nationale de la sécurité des systèmes d'information. Il s'adresse plus particulièrement aux entreprises de taille importante que sont les ETI et les grands groupes

Des entreprises qui travaillent dans des secteurs d'activités sensibles comme la défense ont l'obligation d'avoir recours à la cybersécurité.

L'approche défensive

Le second volet de compétences apporté par Thucy est le défensif. Il s'agit alors pour Thucy d'apporter des solutions de protection à des entreprises de toutes tailles, de la PME aux grands groupes. Elle déploie des solutions de sécurité avec la mise en place d'outils comme les pare-feux, la sensibilisation auprès des utilisateurs de l'entreprise ainsi que l'installation de solutions antivirales. « La majeure partie de notre activité concerne du préventif. Il arrive néanmoins que l'entreprise soit attaquée. Nous devons alors appliquer une méthode curative très urgente. » Les cyberattaques sont en effet une catastrophe pour les entreprises car tout est alors bloqué comme le système de paye ou les commandes par exemple. « Ce phénomène est de plus en plus important mais les entreprises y sont en revanche de plus en plus sensibles en se protégeant davantage que par le passé. »

Un second métier

L'autre métier de l'entreprise est l'infogérance qui consiste à gérer le parc informatique d'une entreprise. « Cette activité représente une petite part dans l'entreprise mais nous y ajoutons pour nos clients notre approche cybersécurité qui est véritablement l'ADN de l'entreprise. Nous avons à ce jour cinq clients dans le Vaucluse. » Grâce à leur formation cybersécurité, les trois trentenaires assurent également des formations jusqu'à Bac+5 auprès de la CCI à Avignon.

Un logiciel créé

Thucy vient de lancer un logiciel autonome, Data Shields. Les entreprises peuvent y souscrire sous forme d'abonnement. Cet outil permet de surveiller toute la surface exposée sur internet. Dès qu'il y a une anomalie détectée sur une fuite d'informations, le logiciel envoie alors une alerte. « Nous sommes évidemment passionnés d'informatique. À ce jour, ce nouveau logiciel a été commercialisé auprès d'une dizaine d'entreprises de toutes tailles dont un grand groupe. »

Les perspectives de l'entreprise sont de consolider toutes ses prestations auprès d'un plus grand nombre

Les Petites Affiches de Vaucluse depuis 1839

Ecrit par le 2 novembre 2026

de clients. La recherche et développement, dada de ces trois jeunes créateurs, doit également permettre à terme de sortir de nouveaux produits. L'entreprise va rester à Carpentras et l'ouverture d'un nouveau bureau à Aix-en-Provence va lui apporter un nouveau bassin économique potentiel.

Des chiffres :
– Chiffre d'affaires 2025 : 200 000€ (idem à 2024)

– Pour les collectivités de moins de 25 000 habitants : 1 collectivité sur 10 déclare avoir été victime d'attaques dans les 12 derniers mois
– Un baromètre révèle que 44% de ces collectivités s'estiment faiblement exposées, tandis que 53% pensent bénéficier d'un bon niveau de protection.

Menaces principales pour les entreprises / associations (répartition des demandes d'assistance) :
– Hameçonnage : 21%
– Piratage de compte : 20%
– Rançongiciel : 12%
– Fraudes aux virements : forte hausse en volume (+29%)
– Défigurations de site Internet : baisse en volume (-17%)
– Attaques DDoS : baisse (-4%)

Source : rapport de cybermalveillance.gouv.fr (ANSSI)

Avignon : la French Tech Grande Provence organise une masterclass sur la cybersécurité

Les Petites Affiches de Vaucluse depuis 1839

Ecrit par le 2 novembre 2026



Ce jeudi 23 octobre, la French Tech Grande Provence, qui est un outil de développement économique dédié à l'innovation et au service du territoire à destination des entrepreneurs du Vaucluse et du Pays d'Arles, organise une nouvelle masterclass ce jeudi 23 octobre au Living Lab Le 9 à Avignon.

Ce rendez-vous, dédié à ses adhérents, est organisé en partenariat avec Cyberwings, société française d'experts en hacking éthique et management de l'information stratégique basée à Marseille, qui délivrera les bases de la cybersécurité dans le cadre du Mois européen de la cybersécurité.

Pour vous inscrire, cliquez ici.
Jeudi 23 octobre. 18h. Living Lab – Le 9. 120 Rue Jean Dausset. Avignon.

Cybercriminalité : avec POWERiti, une start-up innovante d'Avignon, votre sécurité est garantie

Les Petites Affiches de Vaucluse depuis 1839

Ecrit par le 2 novembre 2026



Les cyberattaques sont en croissance constante et exponentielle en France : +37% en 2020. En 2021, l'ANSSI (Autorité Nationale de la Sécurité des Systèmes d'Informatique) avait recensé 1082 intrusions et en 2024, le chiffre a explosé à 385 000, dont 330 000 visaient des PME, 37 000 des organismes publics et 17 000 des ETI (Entreprises de taille intermédiaire).

Pêle-mêle : l'Hôpital Simone Veil à Cannes, Engie, la SNCF, La Société Générale, Chronopost, France Travail, Bouygues Telecom, Auchan, les villes de Marseille et Nîmes ont vu leurs serveurs attaqués, leurs données sensibles violées, leurs fichiers clients pillés. Des millions de données, listings de clientèle, dossiers confidentiels utilisés frauduleusement après ces innombrables attaques-éclair. Personne, quelle que soit la taille, n'est à l'abri.

C'est là qu'intervient l'Avignonnais Jantien Rault, qui a créé son entreprise POWERiti en février 2021 à Agroparc, « pour offrir une proposition globale de solutions de sécurisation des données, grâce à une équipe d'experts digitaux soigneusement sélectionnés, une connectivité fiable évolutive, une veille H-24, 7 jours sur 7 et une sauvegarde permanente. »

Grâce à ce système de « coffre-fort numérique », les patrons peuvent dormir sur leurs deux oreilles et retrouver leur sérénité. Les mails, bulletins de salaire de leurs employés, listes de fournisseurs et de clients sont protégés, impénétrables et ne peuvent pas être revendus à d'éventuels concurrents.

Une entreprise en croissance

Et comme la demande grimpe à la vitesse grand V, « en un an, le chiffre d'affaires a grimpé de +50%, le nombre de mes salariés est passé de 9 à 12 et l'investissement se poursuit. Pour 2025, la courbe de la croissance continue de grimper avec un chiffre d'affaires probable estimé à 1,4M€, et pour 2026, la tendance est à la stabilisation des acquis et à la recherche de nouveaux clients », explique le jeune PDG.

Les Petites Affiches de Vaucluse depuis 1839

Ecrit par le 2 novembre 2026

Aujourd'hui, l'entreprise compte environ 150 clients, dont un quart dans le Sud-Est de la France. « Je suis fier d'avoir acquis un service qui officie pour le Ministère de la Défense, même si je dois rester discret. Il a validé la qualité et le périmètre de notre accompagnement comme 100% fiable pour des données militaires, donc absolument confidentielles. Nous avons aussi la confiance d'industriels avec des secrets de fabrication, que ce soit dans l'agroalimentaire, la métallurgie, la construction. Certains travaillent à flux tendu jour et nuit avec des équipes qui font les 3 x 8h, Donc la cybersécurité doit être constante, ne jamais interrompre le processus industriel », précise Jantien Rault.

À l'avenir, il compte développer son propre outil pour apporter une vision plus ludique du parc informatique à ses clients, même ceux qui ne sont pas fondamentalement des 'geeks'. « Le sens que nous donnons à ce que nous faisons est important. Comme la confiance qui nous lie à nos clients. Nous devons être transparents, leur assurer une fiablité, un plus. » Et comme il a le sens de la réciprocité, Jantien Rault compte créer une sorte de fondation qui soutiendra des actions caritatives, qui sera au service d'une communauté, de l'intérêt général.

Contact : 04 12 04 01 90

(Vidéo) Comment les Vauclusiens gèrent leur mot de passe ?

Les Petites Affiches de Vaucluse depuis 1839

Ecrit par le 2 novembre 2026



Mardi 6 mai, c'est la journée mondiale des mots de passe. L'occasion de rappeler les bonnes pratiques en matière de cybersécurité à une époque où la fraude en ligne n'a jamais été aussi répandue. En amont de cette journée, l'Echo du mardi, en partenariat avec Orange, est allé à la rencontre des avignonnais lors d'un micro-trottoir dans les rues de la cité des papes.

5 conseils pour bien choisir son mot de passe

Si auparavant le grand public n'était pas forcément mobilisé à ces questions de sécurité numérique, il semblerait qu'il soit davantage sensibilisé aujourd'hui. Une très large majorité des gens est ainsi déjà au fait des principales précautions à avoir et évite les codes du type : 000, 1234, les dates de naissance, etc. Aucun ne fait également l'erreur de divulguer son mot de passe même si beaucoup avoue avoir du mal à se souvenir de tous.

L.G.

Les Petites Affiches de Vaucluse depuis 1839

Ecrit par le 2 novembre 2026

Cavaillon : B2P se diversifie dans la cybersécurité



Crée en 2006, la société B2P a été une des premières à avoir développée et exploitée une bourse de fret en ligne pour les professionnels du transport. Après avoir élargi son offre à des services complémentaires, la société cavaillonnaise crée aujourd'hui un pôle de cybersécurité. Il s'agit d'apporter une réponse technique à la montée en puissance des cybermenaces dans le secteur du transport et de la logistique.

Le domaine du transport et de la logistique n'est pas lui aussi épargné par les cyberattaques. La digitalisation toujours plus importante de ce secteur lui fait courir des risques croissants. Jusqu'alors la

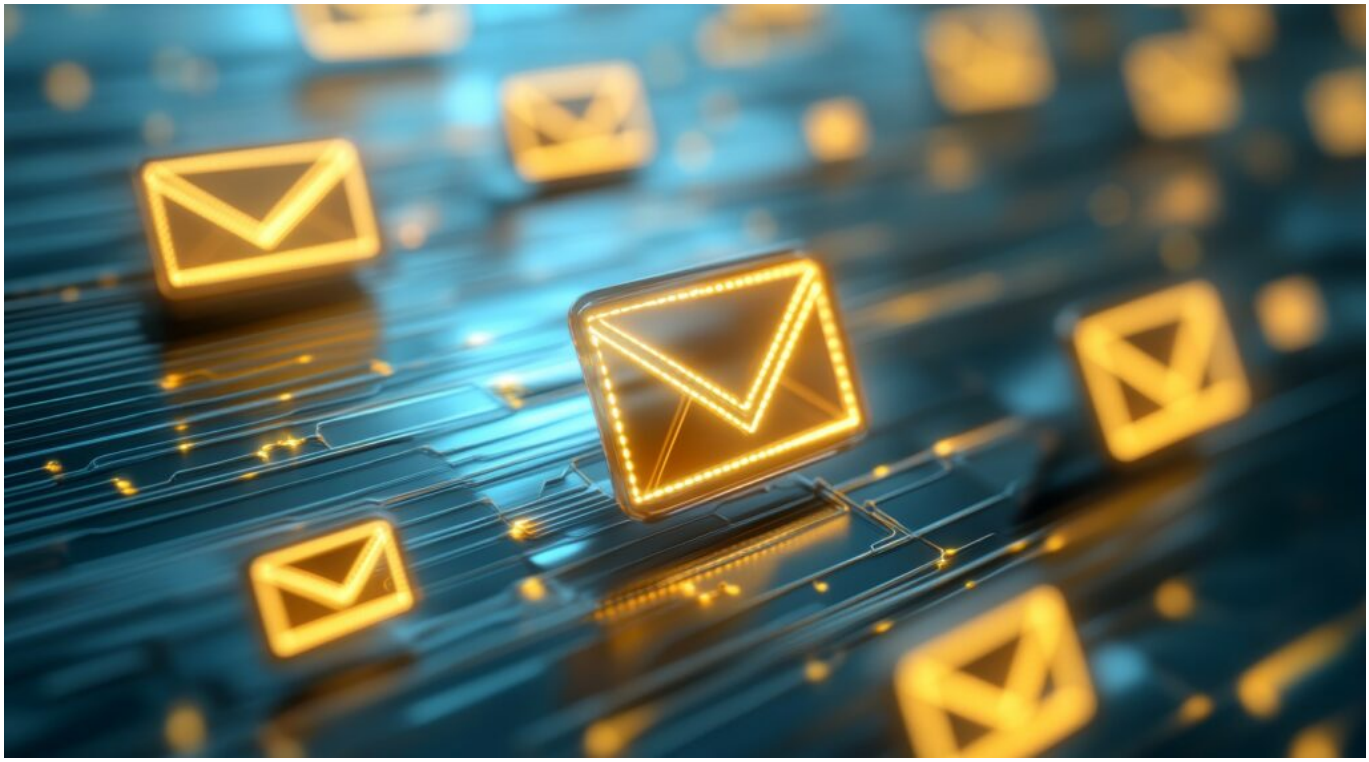
Les Petites Affiches de Vaucluse depuis 1839

Ecrit par le 2 novembre 2026

cybersécurité était intégrée de manière transversale à tous les projets, B2P a décidé de passer la vitesse supérieure en créant un service entièrement dédié au sein de l'entreprise. Cette orientation, qualifiée de majeure par ses dirigeants, est une étape nécessaire pour l'obtention de la certification ISO 27001, norme internationale garantissant les meilleures niveaux de sécurité en matière de traitement de l'information.

« La cybersécurité est notre affaire à tous. En créant ce pôle dédié, nous affirmons notre ambition d'être à la pointe de la sécurité numérique et d'offrir des solutions fiables et pérennes à nos clients », précise Christophe Leininger, Directeur des systèmes d'information de B2P. Ce service a été confié à Antoine Boyer, un jeune ingénieur spécialisé en cybersécurité.

Utilisez une messagerie sécurisée pour contacter les Finances publiques



La Direction générale des finances publiques (DGFIP) vous invite à utiliser sa messagerie

Les Petites Affiches de Vaucluse depuis 1839

Ecrit par le 2 novembre 2026

sécurisée lorsque vous souhaitez rentrer en contact avec elle.

« La messagerie sécurisée est le service en ligne le plus simple qui vous permet de contacter directement le service compétent de l'administration fiscale, explique le DGFIP. Accessible 24 heures sur 24,7 jours sur 7, sur le site impots.gouv.fr la messagerie sécurisée vous permet de réaliser, depuis votre espace professionnel, en toute confidentialité, les démarches suivantes :

– dépôt d'une demande (poser une question générale ou transmettre une information utile à la gestion de votre dossier, déposer une réclamation, signaler une difficulté…),

– réception d'un accusé de réception après le dépôt d'une demande,

– suivi de l'avancement de vos demandes,

– consultation de l'historique de vos demandes,

– alerte pour tout nouveau message disponible directement à l'adresse électronique que vous avez renseignée lors de l'habilitation à ce service. »

Des réponses sécurisées et archivées
« Les réponses qui vous sont apportées par l'administration sont 'historisées' et sécurisées, poursuit la Direction générale des finances publiques. Elles lui sont opposables. Ce système garantit votre sécurité juridique. A noter : pour simplifier au quotidien vos contacts avec l'administration fiscale, une arborescence intuitive vous guide dans la rédaction de vos demandes. Pour utiliser ce service, consultez dès-à-présent la fiche FOCUS SL2 « Demander une adhésion aux services en ligne (mode expert) »sur le site impots.gouv.fr. »

Les Petites Affiches de Vaucluse depuis 1839

Ecrit par le 2 novembre 2026

RÉPUBLIQUE FRANÇAISE
Liberté
Égalité
Fraternité

FINANCES PUBLIQUES

Votre espace professionnel

Services en ligne des **professionnels**

FOCUS

sur

Les téléprocédures Demander une adhésion aux services en ligne (mode expert)

Dernière mise à jour
11/10/2024

Ecrit par le 2 novembre 2026

Les usagers souhaitant bénéficier des services de l'administration fiscale sur internet doivent posséder au préalable un espace professionnel. Pour plus de renseignements sur la création d'espace, vous pouvez consulter la fiche FOCUS ci-dessus (cliquer sur le visuel). Il n'est pas nécessaire de créer un espace professionnel par entreprise : un même espace regroupe l'ensemble des habilitations détenues par un usager pour une ou plusieurs entreprises gérées. Il est cependant conseillé de limiter le nombre de dossiers gérés dans un même espace à un maximum de 100 : au-delà, des ralentissements importants, voire des blocages, pourraient être rencontrés en périodes d'affluence.

L.G.

Piratages des collectivités : à qui le tour ?

Les Petites Affiches de Vaucluse depuis 1839

Ecrit par le 2 novembre 2026



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 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

Les Petites Affiches de Vaucluse depuis 1839

Ecrit par le 2 novembre 2026

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 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

Les Petites Affiches de Vaucluse depuis 1839

Ecrit par le 2 novembre 2026

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… »

> « Cette connectivité expose ces systèmes à des cyberattaques potentielles. »

Les Petites Affiches de Vaucluse depuis 1839

Ecrit par le 2 novembre 2026

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 2 novembre 2026



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 2 novembre 2026

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