Les Petites Affiches de Vaucluse depuis 1839

Ecrit par le 9 novembre 2026

A bas les frigos connectés !



Une chronique de Didier Bailleux

Merci. On peut dire merci aux hackers qui se sont attaqués aux réfrigérateurs et congélateurs connectés de nos supermarchés. Non pas qu'on puisse en vouloir à ces appareils ou aux magasins eux-mêmes, mais ces pirates viennent de nous montrer la limite à ne pas dépasser dans la course folle à l'hyper connexion numérique. A quoi ça sert d'avoir les réfrigérateurs et congélateurs dont les températures sont pilotées à distance, à part nous rendre toujours plus dépend d'autrui et surtout nous rendre encore plus vulnérable ?

Mais qu'est ce qui a pris les responsables des magasins d'accepter l'installation d'appareils frigorifiques connectés ? Les personnels de ces dits magasins ne sont-ils pas les mieux placés pour s'assurer du bon fonctionnement de ces équipements, ils les ont sous les yeux ? Oui le progrès a ses limites. Ce sont des âmes malveillantes dont on peine d'ailleurs à trouver les motivations, qui viennent nous les montrer. Les sociétés qui ont développé ce service vont évidemment chercher à le sécuriser d'avantage. Ce qui ne fera, à mon humble avis, qu'exciter les hackers, qui y verront là un nouveau défi à relever. Mais bon sang revenez aux frigo normaux !

Les Petites Affiches de Vaucluse depuis 1839

Ecrit par le 9 novembre 2026

Mais en attentant on n’est peut-être pas obligé de tout connecter…

Vous l’aurez compris ici le frigo fait figure de symbole, car au fond il en va des frigos comme de nos libertés. Sous couvert de d’avantage de services, de tranquillité on est de plus en plus dépendant de la technique et de ceux qui la gère. Ne confions pas la conservation de nos camemberts à ces vauriens du numérique.

Le 2 novembre dernier, une cyberattaque a permis aux hackers de modifier à distance les paramètres de température des chambres froides de l’Établissement Français du Sang sur trois sites, sans toutefois, d’après l’EFS, entraîner de perte de produits sanguins.

Il y a quelques jours, le Crédit Mutuel Arkéa a été victime d’une cyberattaque. 100 millions d’euros ont été détournés. Le casse du siècle uniquement avec un ordinateur. Le plus cocasse c’est que cette banque s’est distinguée le mois dernier en remportant le prix de la meilleure initiative innovante, pour son Indice de Menace Cyber auprès d’un collège de spécialistes. Comme quoi.

La vraie liberté sera dans le moins connecté possible ça c’est sûr.

On ose imaginer les conséquences si des hackers s’attaquaient aux systèmes d’information de la SNCF, du contrôle aérien, ou des transactions bancaires… On est loin de nos malheureux camemberts… Mais en attentant on n’est peut-être pas obligé de tout connecter… La vraie liberté sera dans le moins connecté possible ça c’est sûr.

Cyberattaque : et si votre avocat était votre premier rempart juridique ?

Les Petites Affiches de Vaucluse depuis 1839

Ecrit par le 9 novembre 2026



En France, 60 % des PME victimes de cyberattaque n'ont pas d'avocat dans leur cellule de crise, ce qui a pour résultat des plaintes mal rédigées, assurances non indemnisées, responsabilités mal gérées. Maitre Djamel Belhaouci* du barreau de Marseille explique pourquoi l'avocat est un acteur incontournable dès la première heure.

Il est 2h du matin, les serveurs d'une PME francilienne viennent d'être chiffrés par un ransomware. Le dirigeant réveille son DSI, contacte son prestataire informatique, alerte son assureur. L'avocat ? Il sera appelé trois semaines plus tard, hélas quand il sera trop tard pour réparer la plupart des erreurs commises.

> « Une entreprise victime de cyberattaque a 72 heures pour notifier la CNIL d'une éventuelle fuite de données. »
>
> *Maître Djamel Belhaouci*

Ce scénario, Maître Belhaouci, avocat en droit de la cybercriminalité, le rencontre chaque semaine dans son cabinet. « Les entreprises pensent que la cyberattaque est d'abord un problème technique. C'est une erreur fondamentale, dès la première heure, elle est surtout un problème juridique. »

Les Petites Affiches de Vaucluse depuis 1839

Ecrit par le 9 novembre 2026

« Une entreprise victime de cyberattaque a 72 heures pour notifier la CNIL d'une éventuelle fuite de données. Si cette notification est absente, mal rédigée ou tardive, les sanctions peuvent dépasser le préjudice de l'attaque elle-même. Il est de même pour le dépôt de plainte dans le cadre d'une couverture assurantielle. C'est le premier acte juridique à poser et il doit l'être par un avocat. »

Rappel du cadre légal
Notification CNIL obligatoire : 72 heures après la découverte d'une violation de données à caractère personnel (art. 33 RGPD). Information des personnes concernées : sans délai injustifié lorsque la violation est susceptible d'engendrer un risque élevé pour leurs droits et libertés (art. 34 RGPD). Infractions applicables : accès frauduleux à un STAD (art. 323-1 CP), atteinte au secret des affaires (loi du 30 juillet 2018), extorsion (art. 312-1 CP).
Face à la recrudescence des cyberattaques en France le nombre d'incidents déclarés à l'ANSSI a progressé de 30% en 2025 , Maitre Belhaouci appelle les chefs d'entreprise à anticiper : « Intégrez votre avocat dans votre plan de continuité d'activité avant la crise. Le moment le plus coûteux pour appeler un avocat spécialisé, c'est le lendemain de l'attaque. »

Les trois erreurs récurrentes commises en l'absence d'un avocat
1. La plainte rédigée sans conseiller juridique: dans la précipitation, les dirigeants déposent des plaintes incomplètes, sans qualification précise des infractions tel l'accès frauduleux à un système de traitement automatisé de données (STAD), l'extorsion, l'atteinte au secret des affaires. Une plainte mal rédigée affaiblit l'ensemble de la procédure pénale et réduit les chances d'indemnisation.

2. L'assureur cyber contacté sans préparation: les polices d'assurance cyber contiennent des clauses d'exclusion précises. Contacter l'assureur sans avoir préalablement sécurisé les preuves et documenté l'incident avec un conseil juridique expose l'entreprise à un refus de garantie. « J'ai vu des entreprises perdre plusieurs centaines de milliers d'euros d'indemnisation pour des déclarations maladroites faites dans les premières heures », témoigne Maitre Belhaouci.

3. La communication de crise sans garde-fou juridique: informer ses clients, ses partenaires ou la presse d'une violation de données engage la responsabilité civile et pénale de l'entreprise. Chaque mot compte. L'avocat est le seul interlocuteur capable de valider ces communications sous couvert du secret professionnel.

> « Ce n'est pas une question de taille d'entreprise. »

L'avocat dans la cellule de crise : un investissement, pas un coût Maître Belhaouci plaide pour une intégration systématique de l'avocat spécialisé en cybercriminalité dans les plans de réponse aux incidents des entreprises au même titre que le responsable informatique ou le DPO. « Ce n'est pas une question de taille d'entreprise. Une PME de 20 salariés est aussi concernée qu'un groupe du CAC 40. Les cyberattaquants ne font pas de distinction. »

Les Petites Affiches de Vaucluse depuis 1839

Ecrit par le 9 novembre 2026

Concrètement, l'intervention de l'avocat dès la première heure permet : la préservation des preuves dans des conditions juridiquement recevables, la rédaction de la notification CNIL dans les délais légaux (72 heures), le pilotage de la relation avec les forces de l'ordre et le parquet cybercriminalité, la sécurisation des communications internes et externes, et l'anticipation des recours des tiers éventuellement affectés.

L.G.

**Maître Djamel Belhaouci est avocat au Barreau de Marseille. Il dirige un cabinet dédié au droit de la cybercriminalité et en défense pénale. Il intervient dans les procédures pénales liées aux infractions informatiques, conseille les entreprises victimes de cyberattaques et accompagne ses clients dans leur mise en conformité.*

CPME 84, Cyber attaques, Comment vous protéger ?



Les Petites Affiches de Vaucluse depuis 1839

Ecrit par le 9 novembre 2026

La Confédération des petites et moyennes entreprises de Vaucluse,avec son partenaire le Crédit Agricole Alpes-Provence, propose un petit déjeuner sur le thème : 'Cyber attaques, comment vous protéger ? Mercredi 28 septembre de 8h30 à 10h30.

Les TPE-PME (Très petites et moyennes entreprises) vivent une recrudescence des tentatives de fraude et d'attaque. Des pratiques cyber malveillantes désormais courantes, qui peuvent mettre à mal la réputation du professionnel et mettre en péril la survie des entreprises.

La crise sanitaire a accéléré ce processus. Le recours massif au télétravail, l'usage parfois non sécurisé des technologies de communication, etc… autant de comportements qui ont aiguisé l'appétit des hackers.

Devant l'explosion de ces menaces et l'impact engendré, il est donc indispensable de prendre la juste mesure des risques encourus et d'appréhender les solutions existantes.

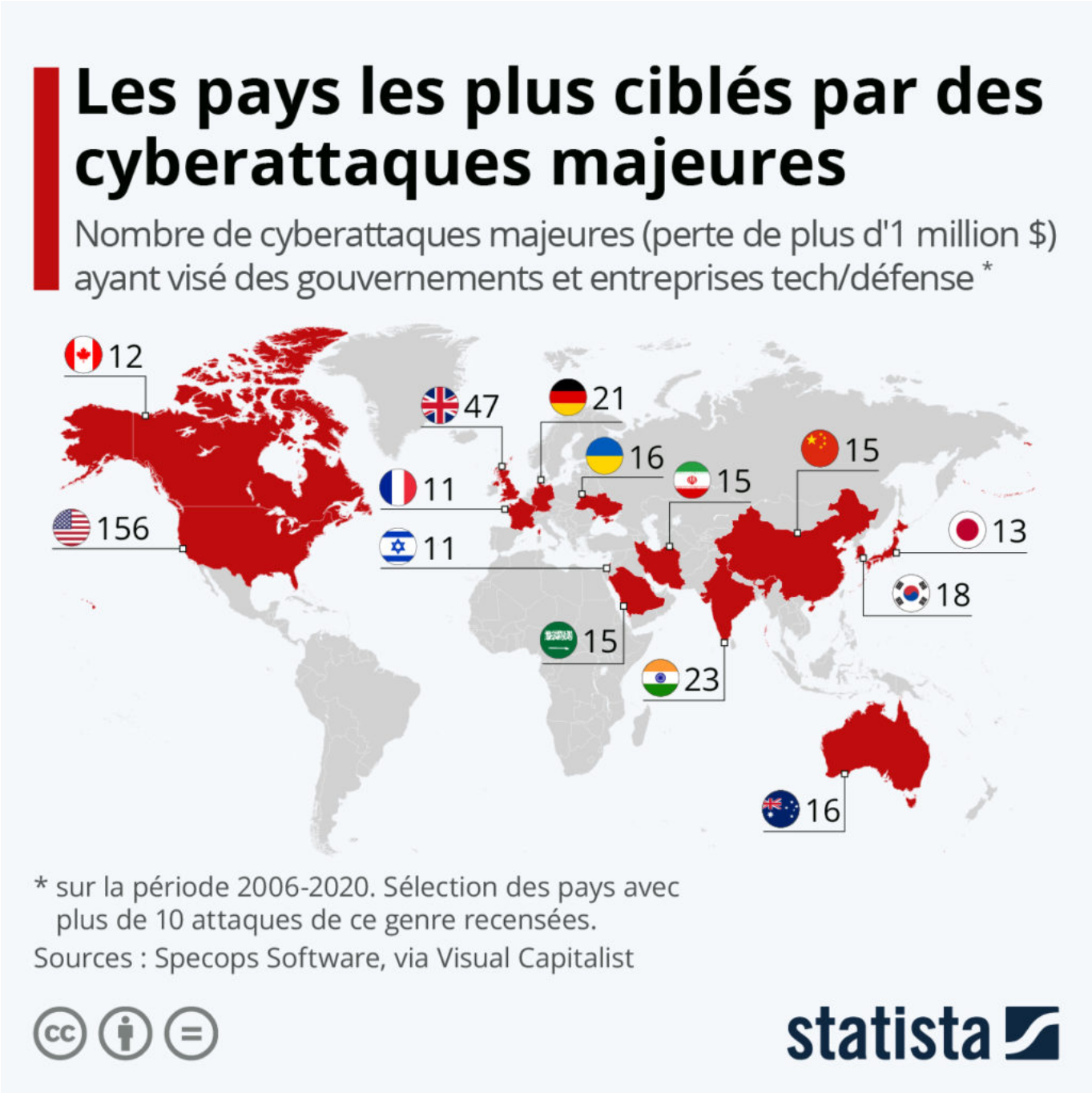
C'est Franck Chemin, responsable du service Cyber sécurité, fraude et continuité d'activité du Crédit agricole qui se chargera de délivrer l'information.

Les infos pratiques
Petit-déjeuner de la CPME 84. Mercredi 28 septembre. De 8h30 à 10h30. Au Crédit agricole Alpes-Provence Avignon-Amandier. 168, avenue Pierre Sémard à Avignon. Inscription ferme et définitive sur ce mail ici. 04 90 14 90 90 le site web ici.
MH

Les pays les plus ciblés par des cyberattaques majeures

Les Petites Affiches de Vaucluse depuis 1839

Ecrit par le 9 novembre 2026



Des données publiées par Specops Software et reprises par le site Visual Capitalist révèlent les pays qui ont été les plus ciblés par des cyberattaques majeures au cours des deux dernières décennies. L'étude porte plus particulièrement sur la période 2006-2020 et recense les attaques informatiques visant des gouvernements ainsi que des entreprises technologiques et de défense qui ont causé des pertes supérieures à 1 million de dollars (environ 820 000 euros).

Les Petites Affiches de Vaucluse depuis 1839

Ecrit par le 9 novembre 2026

Les États-Unis arrivent largement en tête des pays les plus touchés, avec 156 cyberattaques de ce genre documentées. Cela représente une moyenne de 11 attaques majeures par an, soit le même nombre que celui enregistré par la France en quinze ans. Parmi les cibles les plus souvent attaquées, on retrouve ensuite le Royaume-Uni (47), l'Inde (23) et l'Allemagne (21). Avec 11 cyberattaques d'envergure subies depuis 2006, l'Hexagone fait partie du top 15 des pays les plus ciblés, derrière le Canada (12) et à égalité avec Israël (11). Quant à la Russie, non sélectionnée dans ce graphique (moins de 10 attaques majeures), elle en a recensé 8 au total sur la période étudiée, soit deux fois moins que son voisin ukrainien.

L'Agence nationale de sécurité des systèmes d'information (ANSSI) a récemment alerté sur la hausse du niveau de menace cyber en France, en lien notamment avec le contexte de crise sanitaire. L'an dernier, les attaques informatiques contre des entreprises ou institutions françaises ont été multipliées par 4.

De Tristan Gaudiaut pour Statista

Avignon, le système d'information n'a jamais eu autant besoin de Probe iT !

Les Petites Affiches de Vaucluse depuis 1839

Ecrit par le 9 novembre 2026



Sabrina Feddal, ingénieure systèmes et réseaux a créé, en 2016, la société Probe it, spécialisée dans la cyber sécurité. Son équipe et elle interviennent auprès des petites et grandes entreprises pour la mise en sécurité de leur système d'information. Une expertise qui s'inscrit dans l'évaluation du risque jusqu'à la mise en place de remparts adéquats et opérants, en passant par la formation du personnel.

Les Petites Affiches de Vaucluse depuis 1839

Ecrit par le 9 novembre 2026

Travail & persévérance
«Je suis issue d'un milieu modeste et l'obtention d'un diplôme d'ingénieur Systèmes et réseaux consacrait tout le travail et la persévérance que j'avais investis, notamment lors des classes préparatoires, sourit Sabrina Feddal, la dirigeante de Probe iT. Ma carrière s'est poursuivie, en tant que salariée, durant une quinzaine d'années en tant qu'ingénieur réseaux pour venir progressivement à la sécurité et à la protection des données. Les attaques informatiques, vers les années 2 000-2010 n'étaient alors pas aussi répandues qu'aujourd'hui. Ce domaine se voulait, à l'époque, nécessaire même si aujourd'hui, il a pris beaucoup d'ampleur.»

Sécurité rime avec organisation
«J'ai abordé ce nouveau volet de la profession par le biais de la technique appelée Sécurité opérationnelle. Je réalisais l'ingénierie, c'est-à-dire l'architecture de protection. Petit à petit j'ai évolué sur l'aspect plus organisationnel car la sécurité n'est pas que l'affaire des techniciens et ingénieurs, elle touche également l'humain. Beaucoup d'attaques peuvent aboutir lorsque l'on clique sur un mail ou que l'on s'est fait piéger au téléphone. On en vient à toucher la composante des Ressources humaines puisqu'il faut former l'ensemble des collaborateurs aux bonnes pratiques et même, d'un point de vue technique, via des volets de sécurité d'accès physique. La sécurité est très transverse et nécessite de l'organisation. Peu à peu j'ai occupé des postes de conseil auprès du directeur informatique, puis de la direction générale pour les accompagner dans une démarche qualité, d'amélioration continue, notamment, sur le plan d'actions dévolues à la protection et à la prévention des attaques, faire en sorte qu'elles ne se produisent pas et si cela advenait, pouvoir y réagir dans les meilleurs délais pour rétablir une situation normale.»

La cyberattaque
«Et puis la cyberattaque s'est généralisée. A l'origine ça pouvait être l'adolescent qui essayait, par défi, d'aller hacker telle ou telle société. Ça pouvait être la concurrence, les Etats… La cyberattaque pouvait cibler les établissements de santé. Là, nous sommes plus sur des attaquants crapuleux, de la délinquance en ligne… Au fil des années, celle-ci a d'ailleurs bien compris l'intérêt d'Internet en démultipliant sa portée sur des millions de cibles, comme, par exemple, en menant une campagne de phishing (hameçonnage, récupération de données), ce qui est, proportionnellement, beaucoup plus rentable. Aujourd'hui, Internet se structure, se réglemente mais, préalablement, la délinquance s'est mondialisée au-delà des frontières françaises, ce qui induit plus de difficultés et donc le ralentissement des investigations.»

Concrètement
«Le réseau de cyber criminels appelé Emotet (Cheval de Troie bancaire) qui orchestrait, depuis plusieurs années, des attaques pour récupérer des données bancaires a été mis au jour et démantelé par Interpol, aux termes de plus de deux ans de travail acharné, en ayant noué des coopérations internationales et mobilisé plus de huit pays. Si les serveurs ont été saisis, on n'a pas entendu parler de criminels véritablement identifiés car, techniquement, Internet pose des difficultés à la traçabilité et s'appuie sur le relatif anonymat que permettent les outils informatiques. En clair ? On n'arrive pas à tracer les personnes et les groupes. Vous avez l'impression que le flux malveillant vient de tel pays, alors qu'en réalité, il provient d'un autre.»

Les Petites Affiches de Vaucluse depuis 1839

Ecrit par le 9 novembre 2026

Les places de marché

«Un autre exemple ? Vous croyez saisir vos codes carte bleue sur un site identifié alors que vous renseignez le serveur de l'attaquant, lui permettant de se servir de votre carte bleue. Ces données sont ensuite mises en vente sur les places de marché organisées du Darknet sur Alphabet et autres… Ces places vont, en quelque sorte, professionnaliser les délinquants et leur permettre la revente de données, de bloquer l'activité d'entreprises pour les rançonner comme ça a été le cas avec les hôpitaux, ou l'Afnor (Association française de normalisation) ou encore Bouygues construction. Là, non seulement l'outil est bloqué mais en plus un chantage s'exerce à la publication de données confidentielles.»

De nouvelles initiatives

«Pourtant, des cadres réglementaires visent à plus de protection, plus de respect de la vie privée notamment avec le RGPD (Règlement général sur la protection des données) qui va consacrer la protection de la vie privée des citoyens européens. La France s'inscrit, depuis quelques années, dans la loi de programmation militaire, un enjeu national, qui identifie un certain nombre d'opérateurs vital ayant l'obligation de sécuriser leur système d'information pour éviter la catastrophe en cas de panne majeure qui pourrait impacter la vie des citoyens. Ces cadres s'organisent, imposent la sécurité aux différentes parties prenantes de la société, en tout cas pour les grands acteurs, les grands groupes. Par ruissellement, cela impactera les sous-traitants, tout comme le tissu des TPME (Très petites et moyennes entreprises) qui, indirectement, vont devoir également se conformer à ces nouvelles règles. Evidemment, le risque zéro n'existe pas, cependant le socle minimal de sécurité permet d'éviter d'être la proie facile d'attaquants comme on a pu voir les attaques se multiplier auprès des établissements de santé qui ne bénéficient peut-être pas d'assez de sécurité sur place, ce qui est peut-être aussi le cas des TPME.»

Les clients

«Nos clients ? Le milieu de l'enseignement, de la banque, de l'assurance, des mutuelles… Si nous étions, à l'origine, axés sur les grands comptes, depuis plus de cinq ans nous travaillons aux côtés des petites et moyennes entreprises dont nous comprenons les problématiques dans le sens où elles sont débordées par d'autres sujets, et particulièrement pendant cette crise sanitaire. D'ailleurs, à ce sujet, le télétravail a été le point d'entrée de pas mal d'attaques du fait qu'il n'était pas suffisamment sécurisé. Il faudra travailler à ce qu'il ne soit pas le maillon faible, le trou de sécurité et donc la porte d'entrée dans le système d'information de l'entreprise.»

Un marché ultra concurrentiel

«Nous cultivons l'expertise au quotidien, s'il y a beaucoup de concurrents il y a aussi une pénurie des ressources, alors nous misons sur la qualité de nos prestations, en termes d'expertises nous sommes certifiés en sécurité CISSP (Certified information systems security professional) ; des certifications sectorielles dans le domaine de la protection des données monétiques : cartes bancaires PCIDSS (Normes de sécurité de l'industrie des cartes de paiement), des certifications sur les bonnes pratiques, les normes, l'organisationnel Iso 27 001 (Mise en œuvre et gestion d'un système de management de la sécurité de l'information), sur l'analyse de risque qui est très demandé, Iso 27 005 (Gestion des risques en sécurité de l'information), techniquement nous travaillons avec des personnes certifiées qui permettent de faire des tests d'intrusion, ce qu'on appelle des certifications OSCP (Offensive security certified professional) avec des professionnels surentraînés en laboratoires virtuels qui passent un examen réel sur 24 à 48h

Les Petites Affiches de Vaucluse depuis 1839

Ecrit par le 9 novembre 2026

pour faire 'tomber' une centaine de machines. Nous nous démarquons également par l'expertise d'expérience car, comme je vous le disais, nous faisons face à une pénurie de talents et lorsque ceux-ci arrivent sur le marché, ils ne possèdent pas notre expérience.»

Le coût de la sécurité

«C'est aussi toute la problématique du coût d'un service plus que nécessaire. Nous avons identifié, chez Probe iT le fait que les PME n'ont pas de budget exponentiel au regard de leur chiffre d'affaires et aux solutions mesurées et adéquates pour assurer leur sécurité. C'est la raison pour laquelle nous proposons aussi de l'accompagnement, du conseil, pour que les réalisations techniques ne soient pas que l'apanage de cabinets parisiens ou nationaux. C'est justement sur ce créneau que nous portons notre valeur. Nous sommes un cabinet à taille humaine avec une offre de services et des solutions abordables. Nous avons développé des plateformes de sensibilisation, des offres de mise en conformité au RGPD, pareil pour l'évaluation du niveau de sécurité qui est la 1re chose à faire pour savoir si l'on est suffisamment sécurisé et ce que l'on peut faire de plus. Autant de packages à proposer à des prix raisonnables.»

Demain ?

«Nous continuons sur notre lancée, espérant conforter notre position dans le tissu économique local, plus largement national et international. Nous proposons à nos clients deux plateformes : Sensibilisation et RGPD qui vont continuer à évoluer, complétées d'un mixte services-solutions pour pouvoir répondre à la demande du marché. Nous maintenons une veille d'actualité sur la cyber sécurité et l'intelligence artificielle, plus de 1 200 personnes nous suivent depuis la création du compte parmi lesquels des influenceurs sur Twitter et veillecyber.com

Au tout début ?

«Ce qui m'a fait basculer dans l'entrepreneuriat ? Le besoin d'indépendance et de liberté par rapport au cadre salarié de l'époque, avec la vocation de revaloriser le métier d'ingénieur par rapport à la séniorité, au parcours. Dans nos métiers nous manquons de bras et de cerveaux. Alors j'enseigne dans une école d'ingénieurs pour former les jeunes générations. Cela m'a donné envie de monter une structure qui reflète mes valeurs : de l'âme, de la transmission, plus de place pour les femmes – qui ne représentent que 10 à 11% des ingénieurs- en cyber sécurité. Chez Probe iT ? Nous existons depuis 2016 et sommes 5 femmes. Ce n'est pas de la discrimination (rires) mais ça s'est fait comme çà. Mon chiffre d'affaires ? Ça reste confidentiel. Notre portefeuille clients ? Nous sommes positionnés sur de grands comptes dans le secteur bancaire, de l'assurance, des mutuelles, de la sphère médicale comme cette fondation qui compte plus de 15 établissements médicaux, cliniques de soins et de psychiatrie avec des données extrêmement sensibles sur la sécurité et au sens du RGPD. C'est la raison pour laquelle, dans mon équipe, nous accueillons des juristes pour une approche globale, cohérente car, de plus en plus, la cyber sécurité est réglementée.»

La proposition

«Nous proposons d'organiser l'amélioration continue de la sécurité, de sensibiliser les collaborateurs des entreprises ; de piloter la mise en conformité normative et réglementaire de celle-ci. L'entreprise a besoin d'établir et de maintenir la confiance numérique ; d'évaluer son niveau de sécurité ; de protéger son activité et ses données sensibles. Nous sommes experts en audit sécurité et RGPD ; nous portons

Les Petites Affiches de Vaucluse depuis 1839

Ecrit par le 9 novembre 2026

assistance en cas de piratage et nous assurons une assistance technique.»

Créativa
«Nous sommes ravis d'être hébergés chez Créativa, d'être chez les FCE (Femmes cheffes d'entreprise), nous faisons également partie de la French Tech, du Clusir Paca (Club de la sécurité Paca en Avignon), nous allons adhérer à la Cpme 84 (Confédération des petites et moyennes entreprises) de Vaucluse. Nous avons été accueillis à bras ouverts par les réseaux de Vaucluse. Si j'avais un conseil à donner je dirais : 'Installez-vous à Agroparc car ce sont un lieu et des associations qui dynamisent les entreprises. L'endroit est bienveillant et tout y est facilité'.»
Probe iT, hébergée chez Créativa à Agroparc. 200, rue Michel de Montaigne 84140 Avignon. 04 90 23 67 59. contact@probe-it.fr et probe-it.fr



Sabrina Feddal, ingénieure systèmes et réseaux a créé, en 2016, la société Probe it, spécialisée dans la cyber sécurité.