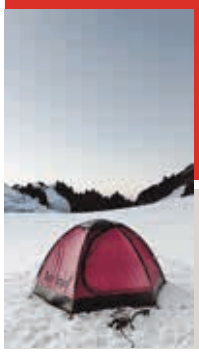
LE FIGARO entrepreneurs

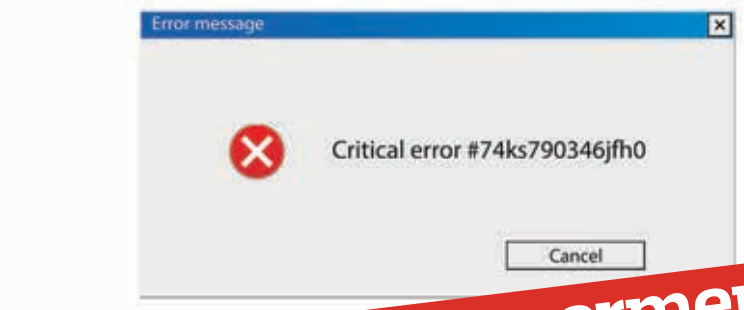


SAMAYA

LA JEUNE ENTREPRISE QUI RÉINVENTE LA TENTE D'ALPINISME PAGE 39

INSTAGRAM

LE COMPTE BALANCE TA START-UP FAIT DES VAGUES SUR LE RÉSEAU SOCIAL PAGE 38



Cyberattaque, supermenace

Aucune entreprise n'est à l'abri des pirates du web mais il existe des moyens efficaces de les contrer. PAGES 36 ET 38

ÉDITORIAL

Du côté obscur

Internet, les réseaux sociaux, le cloud sont de formidables outils pour gérer un business, d'incroyables vecteurs de communication pour toucher les clients. Mais cette force qu'ils donnent à l'entrepreneur a son côté obscur. Sur le web rôdent des gens de sac et de corde, capables de piller ou rançonner une entreprise, de la mettre en grande difficulté.

Il est une autre menace plus insidieuse : les messages acrimonieux qui, sur Google ou Instagram, par exemple, pourrissent votre réputation. S'ils ne mettent pas en péril l'entreprise comme un virus informatique, ces récriminations, le plus souvent anonymes, de salariés ou de clients sont à prendre au sérieux.

Contre les cyberdélinquants, il existe des armes numériques, des procédures éprouvées pour les tenir à bonne distance. Mais contre les mauvaises langues ? C'est plus délicat. S'il y a un fond de vrai dans leurs propos médisants, c'est l'occasion de rectifier le tir. Il faut en profiter pour corriger ce qui ne va pas dans la relation client ou dans la gestion des ressources humaines. Si ces messages sont injustes, c'est rageant, bien sûr. Il convient d'apprendre à y répondre sans colère, de rappeler tout ce que vous faites de bien. **BRUNO JACQUOT**

Le prochain numéro du « Figaro entrepreneurs » paraîtra le 1er février

LA VIE DE BUREAU

Des salles de réunion si exotiques...

Vous connaissiez le syndrome du baby-foot, cliché de la « coolitude corporate », que l'on met en valeur aussi superbement qu'un joli tableau dans un appartement bourgeois. Généralement, ce sont d'ailleurs les baby-foots les plus visibles qui servent le moins. Un phénomène analogue se répand dans les étages : les salles de réunion au nom exotique. L'idée est simple. Il s'agit, dans un grand élan de partage, de lancer un grand brainstorming afin que toutes les équipes puissent choisir des noms « dépaysants » et « inspirants » pour les salles de réunion.

> L'idée est simple. Il s'agit, dans un grand élan de partage, de lancer un grand brainstorming afin que toutes les équipes puissent choisir des noms « dépaysants » et « inspirants » pour les salles de réunion

Une jolie mission, en somme, recommandée pour renforcer la culture d'entreprise et le sentiment d'appartenance. Quels sont les résultats de ces remue-méninges ? Parfois, des noms de penseurs, d'écrivains ou d'explorateurs célèbres. Souvent, des noms de lieux qui font rêver parce que ce sont ceux de destinations, idéales pour les vacances. Bora-Bora, île Maurice, Californie, Acapulco... On est là plus dans le farniente que dans la motivation professionnelle et le dépassement de soi !

Pourquoi choisir de tels noms gorgés de soleil pour des pièces quelconques, sans charme ? Certes, il n'est pas exclu qu'elles soient exposées plein sud. Mais ce n'est pas suffisant ! Non, la vraie raison est que cet exotisme est censé donner envie de se rendre au bureau comme on choisirait une destination de vacances sur Booking.com. À chaque meeting ses sujets impactants... et sa salle de rêve !

Il y a quand même un petit problème dès que l'on pousse la porte... Dans *Mythologies*, Roland Barthes écrit que *« l'automobile est un équivalent assez exact des cathédrales gothiques »*.

Dans le même esprit, découvre-t-on, derrière l'étiquette « salle Seychelles », un décor qui évoque l'anse Lazio, l'une des plus belles plages du monde ? Non, hélas ! La « salle Laponie » ressemble beaucoup à sa voisine « Namibie » ! Quitte à se creuser la tête pour choisir des noms exotiques, pourquoi ne pas aller au bout de la démarche : accorder la décoration des lieux à leur nom. Ce serait toujours ça, à défaut de pouvoir délocaliser la réunion sous des cieux paradisiaques. ■

QUENTIN PÉRINEL
@quentinperinel

SHUTTERSTOCK; HUGO WIRTH/SAMAYA

6 000 euros
Budget nécessaire pour mettre en place dans une PME une protection efficace contre les cyberattaques.

MULTIPLES MENACES

➜ « PHISHING »
L'hameçonnage ou « phishing » consiste à envoyer un courriel visant à dérober des informations ou à introduire un logiciel malveillant dans le système informatique.

➜ RANÇONNAGE
Le cybercriminel demande une rançon après avoir bloqué le système informatique ou en menaçant de divulguer, voire détruire, des données dérobées.

➜ ESPIONNAGE
Des logiciels espions « aspirent » des informations et des données de l'entreprise.

➜ DÉNI DE SERVICE
Pour provoquer un déni de service distribué (DDoS), le cybercriminel rend inaccessible le serveur de l'entreprise en le bombardant de multiples requêtes. Il peut aussi exploiter une faille de sécurité afin de provoquer une panne ou de perturber son fonctionnement. L'objectif est d'extorquer de l'argent à l'entreprise ou de ruiner sa crédibilité.

➜ « FOVI »
Avec l'escroquerie au faux ordre de virement ou « fovi », le délinquant amène l'entreprise à effectuer un virement sur un compte bancaire où il pourra récupérer l'argent. Pour parvenir à ses fins, il peut usurper l'identité du dirigeant (c'est l'arnaque au président), d'un salarié ou d'un fournisseur.

UN LABEL DE CONFIANCE

À qui s'adresser pour se protéger ou se faire assister en cas de cyberattaque ? L'État et des sociétés informatiques ont créé le site web cybermalveillance.gouv.fr et le label ExpertCyber. Après audit, l'Afnor l'attribue aux prestataires compétents dans l'installation et la maintenance des systèmes de protection et l'assistance. Quelque 160 prestataires répartis dans 60 départements, ont déjà obtenu cette reconnaissance. Ils devraient être 300 cette année. L'entreprise qui lance un SOS sur cybermalveillance.gouv.fr sera dirigée vers un prestataire qui l'épaulera dans l'urgence et l'aidera ensuite à bien se protéger.

Les hackeurs visent aussi les PME

Mal protégées, les petites entreprises sont des proies faciles pour les cybercriminels.

ANNE BODESCOT
abodescot@lefigaro.fr

La cybercriminalité augmente et les petites entreprises en font les frais. *« Pirater une PME est bien plus facile que de s'attaquer à un grand groupe, en général mieux protégé,* avertit d'emblée Christophe Corne, président du directoire de Systancia, société de protection informatique. *Aujourd'hui, c'est même à la portée du premier hackeur venu, depuis l'autre bout du monde. »* S'attaquer à une petite entreprise est moins lucratif pour les cyberdélinquants que de rançonner un grand groupe ou de voler des secrets industriels. Mais les petits ruisseaux font les grandes rivières et les hackeurs ont industrialisé leur activité pour ratisser de plus en plus large. Avec des rançongiciels qui s'achètent facilement sur les marchés cybercriminels, ils peuvent envoyer en même temps un millier d'hameçons pour ferrer leurs victimes. *« Dans le lot, certaines se feront forcément piéger »,* observe Christophe Corne.

Très souvent, leurs données seront cryptées, leur système informatique paralysé (et l'activité avec lui). Le pirate réclamera une rançon (souvent seulement quelques milliers d'euros), à payer en bitcoins, pour obtenir la clé de déchiffrement. Parfois, le compteur tourne vite : 10 % des données sont détruites toutes les heures… La menace peut être plus subtile. *« Les hackeurs qui ont exfiltré les données se vantent de pouvoir les rendre publiques,* explique Marc Bothorel, référent national cybersécurité de la (Confédération des petites et moyennes entreprises). *L'entreprise peut alors tomber sous le coup du RGPD, le règlement européen qui protège les données personnelles. Elle court le risque de sanctions de la Cnil avec obligation de contacter les personnes dont les données ont été divulguées. C'est très coûteux. »*

Beaucoup de chefs d'entreprise acceptent donc de payer. Au point qu'en France comme à l'étranger, des voix s'élèvent pour demander l'interdiction de verser les rançons… et de les rembourser. C'est encore en effet une prestation prévue par certaines cyberassurances.

Dans un rapport publié en septembre 2021, l'Agence nationale de la sécurité des systèmes d'information (Anssi) constate une hausse de 255 % en 2020 (par rapport à 2019) des demandes de rançons signalées. Ce n'est que la partie visible de l'iceberg. *« La plupart des entreprises ne veulent rien dévoiler de leurs soucis, de peur d'inquiéter clients et fournisseurs »,* rappelle Valentin Gervit, délégué général du Medef Deux-Sèvres.

> La plupart des entreprises ne veulent rien dévoiler de leurs soucis, de peur d'inquiéter clients et fournisseurs
>
> VALENTIN GERVIT, DÉLÉGUÉ GÉNÉRAL DU MEDEF DES DEUX-SÈVRES.

Les bons réflexes

Et les attaques sont de plus en plus sophistiquées, difficiles à déjouer. *« Dans certains cas de fraude au président,* signale Marc Bothorel, *les pirates ont réussi à espionner les mails et parfois les conversations : leurs courriers ressemblent exactement à ceux que le dirigeant a l'habitude d'envoyer et, au téléphone, sa voix, ses intonations, ses expressions sont parfaitement imitées. »*

Cette menace grandissante, de plus en plus médiatisée, a-t-elle incité les entreprises à mieux se protéger ? *« Le budget moyen consacré à la protection informatique dans les petites entreprises n'a pas bougé depuis des années, il stagne autour de 1 000 euros et se limite même parfois à un simple antivirus. C'est très insuffisant »,* répond Christophe Corne. Même les PME qui ont déjà essuyé une première cyberattaque n'investissent pas pour améliorer leur protection et éviter d'être rançonnées une deuxième fois. *« Après la crise, elles changent souvent de prestataire informatique mais sans forcément améliorer la prévention »,* observe Valentin Gervit.

Le coût est-il si dissuasif ? Pour une entreprise de 10 salariés, qui réalise 1 million d'euros de chiffre d'affaires, se protéger exige, selon la CPME, un budget d'environ 6 000 euros la première année, puis autour de 3 000 euros par an en rythme de croisière. Cela permet de réaliser un diagnostic des faiblesses de l'entreprise, d'installer les logiciels adéquats, d'effectuer les sauvegardes (trois dont une sera conservée hors de l'entreprise), de payer une cyberassurance et, surtout, de former les salariés.

La majorité des attaques sont facilitées par une erreur humaine : par exemple, un salarié ouvre un courriel dont il aurait dû se méfier. Les bons réflexes s'oublient vite, les effectifs se renouvelant régulièrement, une piqûre de rappel s'impose chaque année. Cette formation – souvent faite à distance – est en général financée sur le budget de formation, obligatoire dans les entreprises.

Un secours rapide

Pour aider les dirigeants à renforcer la protection de l'entreprise, l'État cherche à diffuser les bonnes pratiques. Depuis 2021, le label ExpertCyber a été développé par Cybermalveillance.gouv.fr, avec les principaux syndicats professionnels du numérique. Il atteste de l'expertise des prestataires qui l'ont décroché, après un audit de l'Afnor. La qualité des produits, elle, était déjà estampillée par le visa de sécurité de l'Anssi. Malgré toutes les précautions, une entreprise n'est jamais totalement à l'abri. D'où l'intérêt de s'assurer, notamment pour couvrir les éventuelles pertes d'exploitation qu'elle pourrait subir après une attaque. Aujourd'hui, les assureurs sont certes devenus frileux, car les cyberassurances leur coûtent en indemnisation deux fois plus que le montant des primes collectées, selon l'Association pour le management des risques et des assurances de l'entreprise (Amrae). Ils réduisent les garanties, majorent les franchises et les primes et, souvent, refusent même leur garantie aux grands groupes et aux ETI.

« Mais les petites entreprises, pour lesquelles les sommes en jeu sont moins importantes, trouvent encore à s'assurer surtout si elles ont déjà renforcé leur sécurité », remarque Philippe Cotelle, administrateur de l'Amrae. Outre l'appui financier, elles peuvent espérer de certains assureurs un secours rapide en cas d'attaque. *« Les assureurs disposent d'équipes capables d'intervenir très vite dans l'entreprise pour l'aider à limiter les dégâts et remettre au plus vite en état son système informatique »,* ajoute Philippe Cotelle.

Car réagir vite est essentiel. Les chefs d'entreprise pris de court peuvent adresser une demande d'aide sur Cybermalveillance.gouv.fr qui renvoie sur les prestataires les plus proches. Mais ils ont tout intérêt à apprendre – et à familiariser leurs collaborateurs – avec les bons réflexes en cas d'attaque : ne pas éteindre les ordinateurs mais débrancher les câbles réseaux pour éviter la propagation du virus. ■

Antoine Pigeault, dirigeant d'Oxinet, à Basse-Goulaine (Loire-Atlantique). OXINET

CHARLOTTE DE SAINTIGNON
@ChadeSaintl

OXINET
« Je me suis retrouvé démuni, à poil ! »

En ce mois de novembre 2020, ce lundi matin s'annonçait comme les autres. Antoine Pigeault, dirigeant d'Oxinet à Basse-Goulaine (Loire-Atlantique), se connectait au serveur informatique hébergé chez un prestataire extérieur. Sauf que la machine ne répondait pas. Loin de s'inquiéter, il se dit qu'elle prenait son temps. Au bout d'une heure, il a fini par appeler son prestataire. *« Quand ils m'ont répondu qu'ils étaient sur le coup, mais que c'était compliqué, j'ai compris que c'était plus grave que prévu »,* raconte-t-il.

Oxinet a réalisé 1,4 million d'euros de chiffre d'affaires en 2021 en prestations de ménage et de nettoyage, de travaux de second œuvre et d'entretien d'espaces verts. Depuis sa création en 2011, toutes ses données sont hébergées chez un prestataire nantais. *« Nous n'avions pas de serveur chez nous. Cela résout les problèmes de sauvegardes et permet de se connecter partout dans le monde »,* explique Antoine Pigeault. Dans l'après-midi, il a appris que son prestataire était victime d'un « rançonnage ». Un virus bloquerait les installations tant qu'une rançon ne serait pas versée. Soit l'entreprise payait, en croisant les doigts pour que les hackeurs lui donnent la clef de décryptage, soit elle avait sécurisé une sauvegarde et pouvait continuer à travailler.

Le prestataire d'Oxinet s'est d'abord montré rassurant : le lendemain ou en fin de semaine le problème serait résolu. Antoine Pigeault a dû attendre trois semaines avant de récupérer ses fichiers (clients, prospects, fournisseurs…). *« Les pirates avaient réussi à remonter jusqu'aux sauvegardes et à les crypter. C'était la panique à bord, je n'avais plus rien. Je me suis retrouvé complètement démuni, à poil ! »* Impossible d'accéder au planning de ses 40 salariés ou d'établir devis et factures. *« La première semaine, j'ai travaillé comme j'ai pu. »* Le lundi suivant, il a tenu une réunion de crise avec six salariés pour trouver une parade avec les moyens du bord. Grâce aux messageries ouvertes chez un autre fournisseur, Oxinet a pu contacter clients et fournisseurs. Les téléphones portables et les… bonnes vieilles feuilles de papier sont venus à la rescousse. *« Nous nous sommes réinventés, refaisant la maquette de nos devis sur Excel ou en établissant les plannings sur Outlook. »*

Comme la majorité des salariés travaillent sur site, chez les 250 clients d'Oxinet, ils ont pu continuer à travailler. *« Cela a été totalement transparent pour eux. L'impact a été plus moral que financier. Avec ma femme, nous avons eu des nuits très courtes et nous avons fait de nombreuses heures supplémentaires. »*

Au bout de trois semaines, Oxinet a récupéré toutes ses données. *« L'attaque est restée ultra-confidentielle. J'ai appris que les pirates, basés en Russie, voulaient attaquer à l'origine un hôpital français. Mon prestataire informatique et les vingt clients dont il gère les serveurs sont des victimes collatérales. »* Certaines données ont été récupérées après paiement de la rançon et d'autres par une société informatique qui a pu décrypter les données piratées.

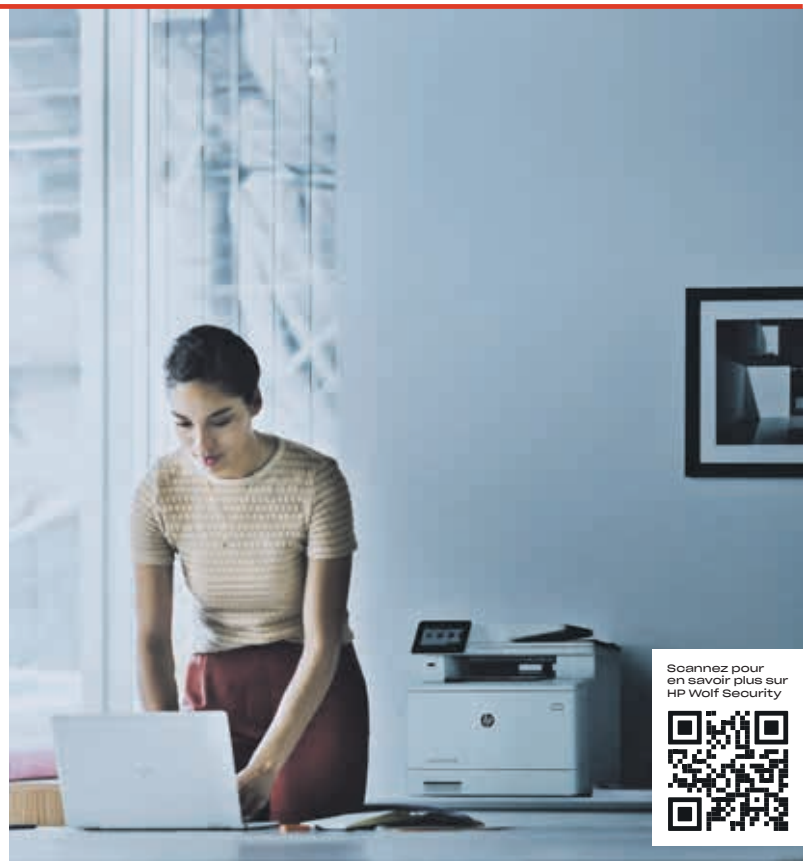
« Quoi qu'il en coûte »

Après cet épisode, Antoine Pigeault n'a pas changé de prestataire. *« Il a été jusqu'au bout du "quoi qu'il en coûte" pour protéger ses clients et récupérer leurs données. »* Mais le chef d'entreprise a multiplié les supports de sauvegarde et les zones géographiques d'hébergement. Outre la sauvegarde externe, il en effectue une chaque jour sur un serveur NAS installé dans les murs d'Oxinet. *« Ce périphérique de stockage est situé dans une pièce verrouillée. Il est protégé par de multiples clés et ne s'allume que pour la sauvegarde. Il ne court donc aucun risque avec internet. »* Enfin, le dirigeant procède aussi à une sauvegarde quotidienne sur son propre ordinateur.

Antoine Pigeault avait été échaudé il y a cinq ans. Après une petite attaque venue par un courriel qui avait crypté ses données, l'entreprise avait alors récupéré sa sauvegarde de la veille au bout de quelques heures. Le chef d'entreprise était donc serein. *« Cela nous avait prouvé que nous étions bien protégés et que l'on pouvait dormir sur nos deux oreilles. »* Il reconnaît aujourd'hui avoir été surpris par les « as du piratage ». *« Il ne faut pas se croire invulnérable. Même Google et le Pentagone se font attaquer. La question n'est pas de savoir si l'on sera piraté, mais quand cela arrivera et ce qu'il faut mettre en place pour que cela ait le moins d'impact possible en limitant au maximum le temps d'immobilisation des données. »* Aujourd'hui, il dort plus tranquille. Il sait qu'en cas de pépin, il récupérera ses données facilement et se remettra au travail très vite. ■

Pourquoi les cybercriminels s'intéressent-ils aux PME ?

Moins sensibilisées au cyber-risque, souvent mal protégées, les petites entreprises sont des proies faciles et constituent parfois le maillon le plus faible de leur écosystème en servant de porte d'entrée vers les grands groupes.



Même si la culture change, de trop nombreux dirigeants de PME considèrent encore que le cyber-risque est surtout un problème pour les grandes entreprises qui seraient, du fait de leur richesse, les proies logiques des hackers en matière d'hameçonnage (phishing) ou de demandes de rançons (ransomware). « *Or, ces patrons se trompent*, estime Karim Driss, expert en cybersécurité chez HP. *Contrairement aux grosses entreprises très informées sur les nouvelles méthodes des pirates, les TPE et PME n'ont pas les moyens de posséder de réels services de sécurité informatique (SSI) et se contentent souvent de simples antivirus et pare-feu gratuits. Elles sont donc des proies de choix pour les hackers.* » Les chiffres sont en effet éloquents : en 2020, près de la moitié des sociétés employant moins de dix salariés ont subi une attaque [1]. Depuis le début de la pandémie, la fréquence des cyberattaques a augmenté de 400 % [2] et, au niveau mondial, les terminaux connectés à Internet ont subi 1,5 attaque par minute [3] !

LA PORTE D'ENTRÉE LA PLUS FACILE À OUVRIR

Si leurs effectifs sont essentiellement concentrés sur le développement de leurs projets, les petites entreprises ne doivent donc surtout pas négliger leur protection informatique. « *Ces TPE et PME font souvent partie d'un vaste écosystème en tant que sous-traitants et partenaires de grands groupes*, poursuit Karim Driss, *elles ne se rendent pas compte qu'elles constituent ainsi une porte d'entrée idéale pour les hackers.* » La résistance d'un système se mesure à celle de son maillon le plus faible, et même si les grandes entreprises sont souvent bien équipées, leurs partenaires plus petits peuvent être malgré eux une menace. Les PME sous-traitantes constituent donc des cibles parfaites : soit parce qu'elles possèdent des informations plus faciles à voler chez elles que chez leurs clients (informations « monétisables », demande de rançon à la suite du chiffrement des données), soit parce que le cybercriminel pourra exploiter les adresses e-mails volées afin de lancer une campagne de phishing visant à récupérer des identifiants pour compromettre dans un second temps une plus grosse entreprise au travers de spear phishing (message d'hameçonnage personnalisé et ciblé) ou encore d'attaque de nom de domaine par typosquatting (usurpation de nom de domaine en changeant l'extension .com en .fr ou en inversant une lettre). « *Ces e-mails personnalisés sont très réalistes et, en provenant d'une entreprise dite "amie", ne vont pas être détectés comme malveillants*, indique Karim Driss. *Le destinataire va en toute confiance ouvrir le message et cliquer sur le lien, le fichier ou le document envoyé par la PME partenaire.* » Un simple clic permet à un pirate de lancer l'exécution d'une charge virale (programmes malveillants) visant à compromettre le système d'information.

Mais les TPE et PME sont aussi de plus en plus souvent l'objet d'attaques directes et victimes d'extorsions plus modestes mais qui peuvent suffire à les fragiliser durablement.

Les conséquences sont même souvent catastrophiques : on estime que le ticket moyen payé par les PME est de 50 000 euros. Mais les sommes peuvent atteindre des sommets : un promoteur immobilier parisien s'est ainsi fait extorquer 33 millions d'euros via une attaque basée sur des e-mails contrefaits.

L'ESCALADE TECHNOLOGIQUE PERMANENTE

Face à l'augmentation des risques, le simple recours à un antivirus n'est pas une ligne de défense suffisante. Gratuits ou payants, tous fonctionnent grâce à des bases de données où sont répertoriées les menaces identifiées, et sont renforcés par de l'intelligence artificielle. Malgré toutes ces technologies, aucun antivirus n'est fiable à 100 %. Des millions de nouveaux logiciels malveillants (malwares) naissent chaque mois, on parle de plus de 380 000 nouveaux fichiers malveillants par jour [4].

« *Les attaques exploitant les vulnérabilités "zero day" ne sont pas détectables par l'antivirus car elles n'ont jamais été identifiées comme malveillantes auparavant.* » Les cybercriminels exploitent donc une faille du système informatique de l'entreprise avant que l'antivirus ou les responsables de la sécurité de l'entreprise puissent la neutraliser ou qu'un correctif soit disponible. De plus, ces malwares imparables, capables de passer sous les radars des solutions classiques de protection, peuvent ensuite s'attaquer à tout le matériel informatique : les ordinateurs bien sûr, mais aussi les objets connectés comme les imprimantes. Et, en cette époque de télétravail généralisé, infiltrer le réseau domestique d'un salarié peut permettre à un hacker de pénétrer celui de l'entreprise…

[1] Rapport du Sénat sur la cybersécurité, juin 2021.
[2] Rapport de l'Agence nationale de la sécurité des systèmes d'information, 2020.
[3] Étude du cabinet KuppingerCole, 2020.
[4] Nombre de fichiers relevés par la société Kaspersky en 2021.

TROIS QUESTIONS À KARIM DRISS, CHIEF TECHNOLOGY OFFICER CHEZ HP

« Une protection qui n'est basée que sur la détection est insuffisante »

Karim Driss nous détaille l'offre HP Wolf Security qui consiste à protéger sans détecter.

DANS UN CONTEXTE D'INFLATION PERMANENTE DES LOGICIELS MALVEILLANTS, LES ANTIVIRUS SEMBLENT DÉPASSÉS. COMMENT HP GARANTIT LA PROTECTION PARFAITE DES ORDINATEURS ?

Karim Driss : Aucun antivirus n'assure une protection à 100 %. Des millions de virus ne sont pas identifiés et de nouveaux apparaissent tous les jours ! Une protection qui n'est basée que sur la détection est insuffisante. Notre méthode, innovante, est basée sur la philosophie du « zero trust » (ne jamais faire confiance avant de vérifier) et consiste à isoler le fichier ou le lien malveillant avant qu'il ne puisse nuire. C'est ce que nous appelons la « protection sans détection ».

CONCRÈTEMENT, COMMENT CELA FONCTIONNE-T-IL ?

Nous utilisons un procédé d'isolation matérielle grâce aux processeurs modernes permettant la micro-virtualisation : lorsque l'utilisateur lance une application ou son navigateur, ouvre un fichier Word, un PDF ou même une image, le fichier sera ouvert non pas dans le système d'exploitation mais dans une petite machine virtuelle de sécurité, étanche par rapport au reste de la machine. Toutes ces tâches vont donc s'effectuer dans une bulle sécurisée, comme dans un coffre-fort virtuel, évitant la propagation dans le système d'information en cas de pièce jointe malveillante. Nous agissons donc en amont des dispositifs classiques de sécurité. Cette technologie d'isolation, que nous avons baptisée HP Sure Click Enterprise et qui fait partie de l'offre HP Wolf Security, permet ainsi d'éviter toute infection et interruption du travail des utilisateurs. De plus, HP Sure Click Enterprise est compatible sur l'ensemble des constructeurs PC.

SI UNE ENTREPRISE SE FAIT ATTAQUER, COMMENT POUVEZ-VOUS L'AIDER À RESTAURER SES ORDINATEURS ?

En cas d'attaque, nous sommes capables de permettre aux appareils d'être résilients, c'est-à-dire de revenir à leur état nominal, avec notre solution HP Sure Start, qui fait également partie de l'offre HP Wolf Security. Cette fonction de réparation automatique permet, en cas de compromission du BIOS (programme permettant la configuration du système), de restaurer son intégrité en toute autonomie. Certaines attaques ciblent en effet spécifiquement le BIOS et affectent ainsi les appareils avant que le système d'exploitation ne démarre, restant donc invisibles pour les antivirus. HP Sure Start permet de se protéger de ce type d'attaque avant même que la mise en route de votre ordinateur. Nous avons obtenu pour cela une certification CSPN (certification de sécurité premier niveau) par l'Agence nationale de sécurité des systèmes d'information. Et cette résilience ne concerne pas que le BIOS, mais aussi le système d'exploitation en lui-même. Grâce à HP Sure Recover, l'utilisateur peut lui-même restaurer l'image de sa machine en un seul clic, sans l'aide d'un technicien, et se remettre immédiatement à travailler. Et cela même dans un environnement sans réseau grâce à une carte mémoire embarquée sur la machine, autrement dit une sauvegarde du système d'exploitation et de ses applications pouvant être mise à jour dans la carte mère qui permet de restaurer entièrement le système. Ce qui est très pratique pour des PME ayant plusieurs sites au niveau national par exemple. Cela représente un gain de temps et donc d'argent. Et évite tout stress pour les équipes informatiques !

Publi-communiqué réalisé par 14HAUSSMANN

Jeu de massacre sur Instagram

Sur le réseau social, le compte Balance ta start-up pointe les entreprises dont les RH sont jugées déficientes. Leur seul moyen de redorer leur image est de réussir à rectifier le tir.

THOMAS LESTAVEL
@lestavelt

Trois années chez Nestlé auront suffi à convaincre Lucie Basch de la nécessité de lutter contre le gaspillage alimentaire. Elle a quitté la multinationale à 25 ans pour créer la start-up Too Good To Go. Son application sur mobile permet de repérer près de chez soi et d'acheter à prix cassés des repas invendus. Téléchargée plus de 10 millions de fois, elle est désormais utilisée dans une quinzaine de pays. L'histoire est belle. Mais l'image de la société a été écornée, il y a quelques mois, sur Instagram après une campagne de dénonciation menée sur le compte Instagram Balance ta start-up, suivi par près de 194 000 personnes.

Des témoignages anonymes de salariés et d'anciens de Too Good To Go évoquent *« un turnover de malade »*, une rémunération *« au lance-pierre »* et des horaires de travail indécents. *« J'arrive le matin avec la boule au ventre »*, raconte l'un d'eux. *« Les témoignages nous ont touchés et nous ne pouvons pas rester sans agir »*, a commenté la direction au lendemain de la publication sur Instagram. La société indique au *Figaro* avoir mis en place *« pas mal d'actions en interne »*, mais n'en dit pas plus : *« Nous ne souhaitons pas communiquer sur le sujet pour le moment. »*

Il n'est pas simple de rebondir après un tel *bad buzz* sur les réseaux sociaux. Meero, Lydia ou Doctolib sont aussi passés par là. Depuis un an, de grands noms de la French Tech ont été épinglés par Balance ta start-up, dont la fondatrice ne dévoile pas son identité par volonté de *« se protéger »*, dit-elle. S'il lui est beaucoup reproché de communiquer des critiques anonymes, donc difficilement vérifiables, son compte Instagram est scruté de près par les entreprises de la tech. Si elles sont épinglées, les conséquences peuvent être désastreuses. Elles doivent travailler dur pour corriger les dysfonctionnements pointés sur Instagram et redorer leur image auprès de leurs salariés, des clients et des investisseurs.

Captures d'écran du compte Instagram Balance ta start-up riche de 194 000 abonnés.
INSTAGRAM BALANCE TA START-UP

L'agence d'intérim numérique Iziwork en sait quelque chose. Il y a un an, Balance ta start-up rapportait des témoignages accablants sur la société, accusée de bafouer le droit du travail. *« Nous devions réagir »*, explique la direction qui a demandé un diagnostic au cabinet de conseil PwC. Des consultants ont mené une trentaine d'entretiens avec les salariés.

Verdict : Iziwork n'a pas su gérer sa croissance rapide. En deux ans, le chiffre d'affaires a été décuplé et ses effectifs sont passés de 30 à 250 employés. *« En phase d'hypercroissance, les managers sont obsédés par les performances car il faut lever des fonds. Cela exacerbe les comportements déviants »*, analyse Thierry Romand, avocat associé du cabinet CMS Francis Lefebvre.

Dans la foulée de l'audit, Iziwork a mis en place plusieurs actions pour *« corriger les dysfonctionnements observés »*. Les salariés remplissent un questionnaire mensuel sur leurs attentes et leurs besoins. Les entretiens d'évaluation annuels prennent désormais la forme de *« feedback à 360 degrés »* où le manager se prononce sur le salarié et vice-versa. La direction dit aussi avoir mené une *« réorganisation interne »*. Un lien web a été créé pour signaler anonymement *« tout comportement perçu comme trop pressurisant »*.

Lutter contre les dérives

Le *bad buzz* provoqué par une story de Balance ta start-up sur Instagram peut entraver la trajectoire de jeunes pousses qui s'efforcent d'attirer et de fidéliser les meilleurs éléments. D'autant qu'elles s'arrachent des professions prisées comme les développeurs, les designers ou les analystes de données. Les entreprises mises en cause se targuent de mener des actions correctrices. *« Seule une volonté sincère du dirigeant de changer les choses permet de lutter efficacement contre les dérives. À défaut, les chartes éthiques, les audits et les lignes de signalement n'ont aucun intérêt. Ce sont des gesticulations, rien de plus »*, estime Thierry Romand. Il importe pour ces jeunes pousses en hypercroissance de constituer une direction des ressources humaines *« dotée d'un vrai pouvoir coercitif »*, ajoute Thierry Romand. La DRH doit *« pouvoir licencier un manager mis en cause pour harcèlement s'il ne change pas immédiatement de comportement »*, précise l'avocat. Autre acteur essentiel : le représentant du personnel. Toute entreprise d'au moins 11 salariés doit organiser les élections de son comité social et économique (CSE) qui porte à la connaissance de la direction les éventuels écarts. ■

EN CAS DE CYBER-ATTAQUE…

1 – Ne pas éteindre les ordinateurs mais les déconnecter du réseau informatique de l'entreprise et mettre en quarantaine les postes ou équipements touchés. Couper tous les accès à internet.

2 – Faire appel à un professionnel pour vous aider, par exemple l'un de ceux qui sont labellisés ExpertCyber.

3 – Identifier les origines possibles de l'intrusion afin d'y remédier et qu'elle ne se reproduise pas.

4 – Repérer toute activité inhabituelle telle que la création de comptes administrateurs ou l'ajout d'un fichier dans le système.

5 – Réinstaller le système à partir de sauvegardes antérieures à l'incident et réputées saines.

6 – Changer au plus vite tous les mots de passe d'accès aux équipements potentiellement touchés.

7 – Effectuer une mise à jour des systèmes de protection.

8 – Porter plainte auprès de la gendarmerie ou de la police nationale ou, par écrit, auprès du procureur de la République du tribunal judiciaire.

9 – Si des données personnelles ont été dérobées, la Commission nationale de l'informatique et des libertés (Cnil) doit en être avisée.

Sur internet, les faux avis de consommateurs peuvent faire des dégâts

HENRI DE LESTAPIS

L'affaire s'est déroulée en 2020, dans une agence immobilière. Sur sa page Google, la dirigeante reçoit l'avis incendiaire d'un locataire. C'est de bonne guerre. Elle répond. Mais le lendemain, sept avis rédigés par des inconnus mitraillent sa page. Après une petite enquête, la chef d'entreprise réalise qu'ils ont été rédigés par des amis du mécontent. *« Ils habitaient tous au Moyen-Orient. Il n'était pas difficile de montrer qu'ils n'avaient rien à voir avec nous »*, se souvient-elle. Elle constitue donc un dossier et l'envoie à Google, en réclamant la suppression des avis. Elle reçoit une réponse laconique, qualifiant les preuves avancées comme insuffisantes. Pour rééquilibrer sa moyenne, elle a donc joué à son tour les faussaires en demandant à ses salariés d'inciter leurs amis à déposer de faux avis positifs. *« J'ai fait une demande pour ne plus avoir d'avis Google du tout*, confie-t-elle, *mais c'est impossible d'y échapper. »* La plateforme américaine confirme : la notation est obligatoire.

Pour se plaindre, il faut cliquer sur l'onglet « signaler un abus ». Mais ce recours en ligne, impersonnel et flou, la chef d'entreprise n'y croira plus du tout. *« Il est rare qu'une personne s'acharne longtemps sur une entreprise. L'être humain passe naturellement à autre chose*, relativise Anne-Sophie Le Bras, directrice France du programme Google atelier numérique. *Mais il est vrai que depuis que nous avons créé un service d'aide aux TPE et PME, le sujet de la gestion des avis est souvent soulevé. »* Les grands noms du référencement ont mis en place des algorithmes de plus en plus sophistiqués qui décèlent les avis injurieux et les faux avis flagrants. Ils y dédient aussi des équipes. *« Traiter les faux avis relève toujours de situations délicates et demande du temps*, souligne Anne-Sophie Le Bras. *Nous répondons dans un délai de cinq à huit jours. »* PagesJaunes prend le sujet au sérieux. Des algorithmes traquent les comptes aux comportements inhabituels, tel le dépôt soudain de multiples notes très positives ou négatives. Ainsi, la note d'un restaurant passant de 2 à 5 en 24 heures serait suspectée. *« Nous ne pouvons communiquer sur tous les paramètres que nous analysons. Il ne faut pas donner de billes aux gens qui cherchent à contourner nos systèmes*, confie Anthéa Quenel, directrice médias de PagesJaunes. *Si nous avons un doute sur un comportement ou si on nous le demande, nous enquêtons en contactant l'émetteur de l'avis. Si nous n'avons pas de réponse, ou que l'avis est injustifié, nous le supprimons. »*

15 millions
d'avis en ligne ont été enregistrés sur la plateforme PagesJaunes en 2021

Solution à l'amiable

En 2016, la plateforme enregistrait 1 million d'avis en ligne. En 2021, elle en compte 15 millions. Et 18 % des avis sont supprimés pour injures, transmissions de données personnelles, contenus illicites ou parce qu'ils sont inintelligibles. PagesJaunes ne peut échapper à quelques procédures judiciaires engagées par des dirigeants d'entreprises. *« Elles sont souvent le fruit d'une réaction à chaud et entamées durant le laps de temps qui nous est nécessaire pour réagir*, justifie Anthéa Quenel. *Elles conduisent habituellement vers une solution à l'amiable. »*

Depuis une dizaine d'années, les avocats spécialisés en e-réputation notent une croissance des litiges. Ils concernent surtout les TPE et les PME. *« Les grosses structures résistent mieux aux avis négatifs »*, constate Romain Darrière, avocat. Il confirme que les cas d'avis injurieux ou grossièrement dénigrant sont rapidement traqués par les plateformes. Les faux avis les plus difficiles à contrer sont ceux de la diffamation douce. Il faut alors entamer une enquête pour prouver le mensonge, en réclamant par exemple au poseur d'avis, souvent anonyme, une preuve de son acte commercial. L'étape suivante est la requête auprès d'un juge, afin d'autoriser la levée de l'anonymat du poseur d'avis, via son adresse IP. *« Cela peut-être rapide. Quelques jours »*, précise Romain Darrière. L'affabulateur peut ensuite être condamné. *« Outre la suppression de l'avis, cela crée un passif sur lequel l'entreprise peut communiquer pour que la peur change de camp ! »*

Quant aux plateformes, Romain Darrière assure qu'elles se montrent plus réactives face aux démarches judiciaires. *« PagesJaunes est une plateforme coopérative »*, constate-t-il. *« Google serait plutôt meilleur élève que Facebook et Twitter, qui pratiquent l'évitement permanent*, constate l'avocat Olivier Iteanu. *Nous avons parfois l'impression qu'ils se moquent de la justice française. »* Quand bien même cela leur apporte un surplus d'activité, les hommes du droit regrettent que les plateformes n'aient pas peaufiné leurs systèmes d'avis lorsqu'elles les ont créés. ■

Le mécontentement peut être retourné à l'avantage de l'entreprise

Le constat de PagesJaunes est formel : les entreprises qui sont l'objet d'avis en ligne reçoivent trois fois plus de visites que les autres. Et 83 % des internautes s'appuient sur ces avis pour faire leurs choix. Seul problème : les clients mécontents sont plus diserts que les consommateurs satisfaits. Les garages auto et les restaurants figurent parmi les plus exposés aux avis. Gérer ces commentaires est devenu une discipline à part entière. Tout d'abord, quand on répond à un avis, on ne s'adresse pas au seul client mécontent mais à toute la toile. Aussi ne faut-il jamais répondre à chaud à un commentaire négatif et veiller à toujours remercier les avis positifs. Il convient de faire preuve de courtoisie en toutes circonstances, de personnaliser les réponses et d'apporter des solutions. *« Les réponses peuvent être l'occasion de faire passer de subtils messages marketing sur des produits ou des services*, rappelle Édouard Richemond, auteur du livre *Les avis client* (Éditions du Puits Fleuri). *Cela peut être utilisé comme un véritable outil promotionnel. Il faut en profiter pour travailler sur des mots-clés qui font remonter l'entreprise dans les moteurs de recherche. »* Il rappelle que quelques mauvais avis peuvent être profitables à la crédibilité de l'ensemble, pourvu que de bonnes réponses leur soient apportées. Enfin, Édouard Richemond incite les entrepreneurs à solliciter les commentaires positifs auprès de leurs clients les plus fidèles. *« Je conçois qu'ils puissent être gênés de faire la démarche*, dit-il. *En réalité, il n'y a qu'une infime partie de clients que cela dérange. »*

H. L.

L'EXPERTISE

La loi exige plus de dirigeantes

COLLECTION PERSONNELLE

JILALI MAAZOUZ
AVOCAT ASSOCIÉ,
MCDERMOTT WILL
& EMERY

Le 24 décembre 2021 a été promulguée la loi n° 2021-1774 destinée à accélérer la participation des femmes à la vie économique (articles L.23-12-1 du Code de commerce et L.1142-11 à L.1142-13 du code du travail). Cette recherche d'égalité et de parité au sein des entreprises s'inscrit dans la continuité de la loi Copé-Zimmermann du 27 janvier 2011. Ce texte avait instauré les premiers quotas de femmes au sein des conseils d'administration et de surveillance des grandes entreprises.

■ Pourquoi légiférer à nouveau, dix ans plus tard ? Trois raisons peuvent justifier cette nouvelle initiative. D'une part, la nécessité de « booster » la loi Copé-Zimmermann, après le succès qu'elle a rencontré : 45,6 % des administrateurs sont aujourd'hui des femmes, contre 12,5 % en 2010, selon le cabinet Ethics & Boards. D'autre part, la volonté d'étendre le champ d'application de la lutte pour l'égalité au-delà des seuls conseils d'administration et de surveillance. Enfin, l'urgence à renforcer plus globalement les dispositifs d'égalité professionnelle et salariale, urgence qui ressort du rapport de consultation présenté le 26 janvier 2021 et intitulé « Comment assurer l'égalité femmes-hommes dans l'économie ? ».

■ La loi commence par adopter une définition élargie de la notion d'instance dirigeante pour y intégrer notamment les comités exécutifs ou de direction. Elle impose ensuite aux entreprises de plus de 1 000 salariés de publier chaque année, à compter du 1er mars 2022, les écarts de représentation entre les cadres dirigeants des deux sexes au sein des instances dirigeantes et les objectifs de progression pour réduire ces écarts, s'ils dépassent un certain seuil.

■ Elle instaure enfin des quotas progressifs requérant la présence au sein des instances dirigeantes d'au moins 30 % de femmes à compter du 1er mars 2026, puis d'au moins 40 % à compter du 1er mars 2029.

■ Pour garantir l'efficacité de ce dispositif, la loi prévoit une sanction financière pouvant atteindre 1 % de la masse salariale et une obligation de suivi dans le cadre de la négociation obligatoire. Difficile de dire aujourd'hui à quel rythme ces mesures, qui complètent l'index de l'égalité professionnelle femmes-hommes permettront de remodeler le casting des instances dirigeantes du futur.

Samaya déplace les montagnes

Pour concevoir et fabriquer ses tentes d'alpinisme innovantes, la jeune entreprise a su réunir des partenaires complémentaires.

Une trentaine d'alpinistes et de grimpeurs testent les produits de Samaya lors de leurs expéditions. SAMAYA

SOPHIE DE COURTIVRON

START-UP Tout est parti d'un défi. *« Faites-moi une tente 3 places de 1 kg et 3 litres, volume emballé »*, a lancé à quelques-uns de ses étudiants, un jour de 2017, Antoine Barthélemy, professeur dans le cadre du bachelor Performance sports, textile & footwear à l'IUT d'Annecy-le-Vieux (Université Savoie Mont-Blanc). Ghislain Pipers s'y est attelé et, le jour de la soutenance, le jury découvrait ébahi deux prototypes de tente fonctionnelle. *« Cela fait vingt ans qu'il n'y a pas eu d'innovation sur le marché de la tente*, analyse le jeune homme de 26 ans, ancien champion d'escalade. *Les grandes marques ont délaissé cette niche car elle ne rapporte pas et la recherche coûte cher. »* Il a fait le pari inverse : miser sur la haute technicité de ses tentes pour ensuite décliner le savoir-faire acquis sur d'autres produits.

Tout en intégrant l'Ensait, école d'ingénieurs textile à Roubaix (Nord), le jeune homme a poursuivi ses recherches et créé la société Samaya, à l'automne 2018, avec un ami, Arthur Jallas, qui avait testé avec lui les tentes en altitude. Début 2019, après bien des nuits blanches, ils présentaient la tente Samaya 2.5 lors d'un salon professionnel à Munich : *« La plus légère, la plus compacte, la plus technique et la plus innovante jamais sortie sur le marché ! »*, s'enthousiasme Antoine Barthélemy.

> « Cela fait vingt ans qu'il n'y a pas eu d'innovation sur le marché de la tente »
> GHISLAIN PIPERS, SAMAYA

Les deux entrepreneurs ont sous-traité la fabrication de 500 exemplaires en Chine. Ils se sont écoulés en quelques mois en 2020. Le dieu des grimpeurs veille sur Ghislain Pipers et Arthur Jallas. En l'occurrence, Google. C'est en cherchant une tente sur le web que Benoît David, polytechnicien et banquier d'affaires qui a fui le bitume parisien, a découvert Samaya. Il a rencontré le duo et, convaincu par le projet, il a décidé de consacrer quelques heures par semaine à l'entreprise en tant que directeur financier. Il a organisé une première levée de fonds auprès de cinq investisseurs, dont son épouse, Victoire, et lui-même. Puis une deuxième de 1,5 million d'euros en 2021 auprès d'une dizaine de personnes : Jean-Marc Pambet, ancien président de Salomon, une dizaine de managers de l'entreprise, des business angels et des financiers.

Ghislain Pipers a mobilisé une cordée de partenaires. Côté R&D, le CEA de Grenoble, le Gemtex, laboratoire textile de l'Ensait, et l'Université Savoie Mont-Blanc pour travailler sur l'imper-respirabilité (afin de prévenir la condensation à l'intérieur de la tente), la résistance mécanique et les propriétés thermiques. Côté matériaux, le nylon vient de Corée et la fibre Dyneema des États-Unis. Pour répondre aux contraintes de poids, Samaya a pris le parti de la tente mono-paroi en concevant sa propre membrane, la Nanovent. L'objectif est de rapatrier la fabrication dans l'entreprise, à Annecy. Cela commencera par les petites séries sur-mesure, à forte valeur ajoutée, notamment pour l'armée. Mais cela prendra des années. *« Il faut d'abord que nous fassions tout le développement en interne. Nous avons pour cela acquis les mêmes machines que l'usine chinoise, recruté des prototypistes, et nous sommes dotés d'un laboratoire et d'un atelier »*, explique Ghislain Pipers.

Ghislain Pipers, Victoire David-Poinsier et Arthur Jallas dirigent Samaya.
HUGO WIRTH/SAMAYA

Victoire David-Poinsier, polytechnicienne comme son mari, a rejoint l'équipe à temps plein à la fin de 2020 pour diriger Samaya avec Ghislain Pipers et Arthur Jallas. L'entreprise, qui emploie 17 salariés, a réalisé 1,5 million d'euros de chiffre d'affaires en 2021 contre 500 000 en 2020. L'objectif est, pendant trois à quatre ans, d'asseoir Samaya en tant que leader technique mondial de la tente d'expédition 4 saisons, puis d'aller vers la tente 3 saisons, marché six fois plus important, de l'ordre de 400 millions d'euros au niveau mondial. Des sacs à dos ultralégers sortiront en mars 2022, modulables selon l'activité pratiquée. *« C'est un concept, comme nos tentes en 2020 »*, souligne Arthur Jallas. Une trentaine d'amis – alpinistes et grimpeurs parmi les meilleurs du monde – testent les produits de Samaya lors de leurs expéditions. *« Au boulot, tout le monde est passionné*, confie Louis Darnault, responsable administratif et financier. *Nous faisons parfois de l'escalade ensemble, ce sont des moments extrêmement forts. »* Samaya est bien partie pour déplacer des montagnes. ■

LE COMPTE VRAIMENT PRO

Qonto, c'est le compte tout-en-un au service des pros.

- ✓ Ouverture d'un compte pro en 10 min
- ✓ Service client ultra-réactif 7j/7
- ✓ Gestion des notes de frais en temps réel

qonto