

MTR Solutions : Solutions IT sur mesure



Avec la digitalisation rapide de la plupart des secteurs et de plus en plus d'entreprises conscientes de la nécessité de numériser leurs process tout en sécurisant leurs activités, le fait de pouvoir faire appel à des prestataires informatiques à l'écoute de ses besoins est primordial. MTR Solutions, située à Esch-sur-Alzette, est une petite entreprise qui propose des services, conçus sur mesure pour d'autres petites entreprises. La compréhension mutuelle est donc au rendezvous. Mario Mauro, passionné d'informatique depuis toujours, est à la tête d'une équipe aussi discrète qu'efficace, tournée exclusivement vers la satisfaction des clients. Il partage avec nous quelques constats simples mais essentiels.

Quel est votre parcours et quelles sont les origines de l'entreprise ?

Je m'intéresse à beaucoup de choses et j'ai un parcours un peu éclectique. J'ai fait des études de droit, de photo et enfin, d'informatique dont je suis passionné depuis la fin du siècle dernier. À une époque, je ne faisais que ça, quasiment jour et nuit. Depuis quelques années, je suis devenu plus raisonnable. En 2014, j'ai créé MTR Solutions à partir d'une société existante depuis 1997. Dès le départ, je souhaitais aider les petites entreprises dans leurs projets informatiques.

Quelle est exactement l'activité de MTR Solutions ?

Nous proposons toute une gamme de services et surtout de conseils en informatique, que ce soit pour aider les entreprises clientes à s'équiper en hardware et software ou pour construire leur

réseau interne, véritable colonne vertébrale de leur organisation. Nous mettons en place les PC des équipes, les câblages, les serveurs... bref, tout ce qu'il faut pour travailler et cela, dans le souci constant de la sécurité des informations et de l'activité des clients.

Alors justement, qui sont vos clients en termes de profils ?

Ce sont des PME et des TPE dans le secteur des services essentiellement mais nous servons également quelques artisans, des petites sociétés industrielles, des cabinets médicaux, des mono-entrepreneurs. Nos clients sont des entreprises dont la taille ne dépasse pas 80 employés. Nous ne sommes pas spécialisés dans un secteur en particulier et, tout en ne faisant pas de publicité, grâce à notre réseau de clients, nous avons sans cesse de nouvelles demandes. Nos clients ont certains besoins communs et diffèrent sur d'autres aspects, ce qui nous confronte à de nouvelles expériences, nous force à être créatifs et à trouver des solutions qui seront ensuite utiles à l'ensemble de notre clientèle.

Quelle est la particularité de la cible des PME-TPE ?

On ne peut pas généraliser. Chaque entreprise a ses propres besoins et sa propre maturité informatique, compte tenu de sa taille et de son secteur d'activité. Nous tenons donc à avoir une relation très personnalisée avec chaque client et nous nous adaptons à la personnalité du dirigeant et des équipes que nous avons en face de nous. Nous apprenons à les connaître en nouant des relations de long terme. Les clients tiennent beaucoup à cette qualité de relation développée au cours de nos interventions sur site et de dialogues directs. Nous avons testé par le passé la mise en place d'un système de ticketing, mais nous en sommes revenus car nous nous sommes rendu compte que nos clients nous avaient choisi car ils pouvaient justement nous expliquer de vive voix leurs problématiques, en parlant à une personne plutôt qu'en remplissant un formulaire. Dans ce contact direct, la pédagogie a toute sa place pour expliquer les différentes solutions et les clients apprécient cet engagement et nous le rendent en étant très fidèles.

Comment voyez-vous évoluer la sensibilité aux questions de sécurité ?

Aujourd'hui, les personnes qui créent des entreprises ont toutes un minimum de connaissances en informatique, acquises dans leur vie privée ou dans des expériences professionnelles précédentes, mais nous avons constaté qu'elles ont besoin d'accompagnement sur les questions de sécurité, pour bien protéger tout ce qui a de la valeur pour l'activité. Je vais vous donner un exemple auquel on ne pense pas toujours. Les informations concernant les déplacements des employés. Ces informations ne semblent pas critiques et pourtant, elles ne sont pas anodines pour des pirates qui préparent une attaque. Donc, attention à ce que vos employés publient sur les réseaux sociaux ! Aujourd'hui, les questions de sécurité préoccupent tout le monde, surtout depuis les deux dernières années. Les hackers lancent des attaques de plus en plus sophistiquées et les médias relatent de plus en plus d'informations sur des failles de sécurité. Cela crée un climat de peur. D'un

côté, cette peur est salvatrice car elle réhausse le niveau de vigilance, mais il ne faut pas que cela tourne à la panique. Nous « Aujourd'hui, les personnes qui créent des entreprises ont toutes un minimum de connaissances en informatique, mais nous avons constaté qu'elles ont besoin d'accompagnement sur les questions de sécurité. » sommes là pour redimensionner la peur et offrir des solutions pour éviter les dégâts. Certains clients vont jusqu'à nous faire suivre les mails qu'ils estiment douteux pour que nous les analysions. Et ils ont raison ; il vaut toujours mieux être trop prudents que pas assez. Ces petites interventions font partie intégrante de nos prestations d'assistance. En effet, certaines sociétés nous confient la totalité de la gestion de leur système informatique. D'autres nous confient des missions ponctuelles.

Le télétravail et les nouvelles façons de travailler ont-ils créé de nouveaux besoins ?

Très nettement. La situation pandémique a été une période d'intense activité pour nous, au cours de laquelle nous avons installé 20 à 30 fois plus de solutions de travail distant que par le passé, avec fourniture de PC portables et système sécurisé par des accès en VPN (Virtual Private Network, ndlr). Avant la crise Covid, la moitié de nos clients n'en n'avait jamais entendu parler. Maintenant que ces nouvelles habitudes de travail se pérennisent, nous nous assurons que la sécurité est bien optimale et au besoin, nous en rajoutons une couche.

Le niveau de sécurité est-il plus fort grâce au cloud computing ?

Quand on parle de cloud, il faut se mettre d'accord sur ce qu'on entend par là. Avoir des serveurs distants dédiés, à accès contrôlé est parfait pour la sécurité des données, à condition que seules les personnes de la société qui loue ces serveurs aient accès aux données. Cela n'est pas du cloud computing. Dans le cloud proposé par de grands opérateurs – comme Google ou Microsoft pour ne citer que deux exemples – qu'on pourrait appeler cloud partagé, on ne sait pas où sont les données. Elles sont parfois hébergées un peu partout dans le monde, en particulier les backups, et leur sécurité ne peut pas être garantie à 100% car des intrusions via internet ou la récupération des backups sont toujours possibles. L'idéal est donc de disposer d'un serveur privé au sein de l'entreprise ou d'un datacenter, avec cryptage des données et accès restreint au moyen d'un VPN sécurisé.

Si vous deviez donner trois conseils essentiels à des PME pour leur cybersécurité, quels seraient-ils ?

Il y en aurait quatre ! Tout d'abord, la mise en place d'une stratégie de sécurité formalisée et respectée par tous. Ne jamais faire d'exception aux règles mises en place pour ne pas créer de trou dans le bouclier. S'il doit y avoir des exceptions, il faut les prévoir pour pouvoir les mettre en place de façon sécurisée. Ensuite, il faut former le personnel à la sécurité, car il ne suffit pas de se doter d'une stratégie pour qu'elle soit appliquée. Il faut donc prévoir du temps et du budget pour la formation des équipes. Par la suite, il faut prévoir des rappels réguliers des règles et contrôler que

celles-ci sont appliquées. Il faut également que les chefs d'entreprise prennent conscience que le budget de sécurité informatique est aussi incontournable que l'assurance qu'ils souscrivent pour les bâtiments, le matériel ou leurs véhicules. Ce budget est en général relativement minime par rapport aux pertes importantes que peuvent causer les cyberattaques. Et un dernier conseil, car les entreprises n'y pensent pas toujours : il faut sécuriser les téléphones portables connectés au réseau de l'entreprise. C'est une chose trop souvent oubliée, or, les téléphones constituent des portes d'entrée vulnérables.

Rencontrez-vous des soucis de recrutement de personnel ?

Oui, comme beaucoup de confrères qui cherchent les mêmes profils que nous. Or, c'est important pour la qualité du service client de stabiliser les équipes. Nous sommes en contact avec les lycées techniques du Luxembourg qui nous envoient des stagiaires. Cela nous permet de garder le pouls de ce qui se passe dans les écoles. Nous avons pris quelques stagiaires universitaires également, du Luxembourg ou de l'étranger. Nous avons constaté que la qualité de formation varie beaucoup d'un établissement scolaire à l'autre. La personnalité du stagiaire joue aussi, bien entendu. La passion est très importante car elle stimule la curiosité des jeunes, indispensable pour aller chercher continuellement des informations sur les mises à jour des logiciels ou les technologies émergentes. Se contenter des cours n'est pas suffisant. Ensuite, il y a la question de la rémunération pour attirer des talents et c'est évidemment un peu plus compliqué pour une petite structure comme la nôtre. Une nouvelle recrue met en moyenne un an à être totalement opérationnelle car ce ne sont pas seulement des connaissances techniques qu'il faut avoir mais aussi apprendre les procédures internes et acquérir la connaissance des clients. Si on fait cet effort de formation, on n'a pas envie que la personne nous quitte. C'est aussi pour cela que nous essayons de maintenir une ambiance de travail où chacun doit se sentir heureux de venir tous les matins.

Quels sont les facteurs clé de succès pour une entreprise de conseil en informatique ?

D'abord, l'écoute des clients et être tourné vers leur satisfaction. Ça, c'est notre credo journalier. Ensuite, il faut maintenir ses connaissances. Prendre du temps pour aller toujours au-devant des nouveautés et se demander comment on pourrait les utiliser au bénéfice de nos clients. C'est un process d'amélioration permanente. C'est pourquoi il est important d'avoir des employés passionnés qui s'abonnent à des newsletters, s'informent sur des sites spécialisés, etc. Nos partenaires, nos fournisseurs, les éditeurs de logiciels et les fabricants de matériel, nous aident également en proposant des informations et des formations.

Quels sont vos principaux défis ?

L'un des défis du moment est l'augmentation de nos coûts à cause des prix de l'énergie et des coûts du carburant qui affectent les frais de déplacement de nos collaborateurs chez les clients.

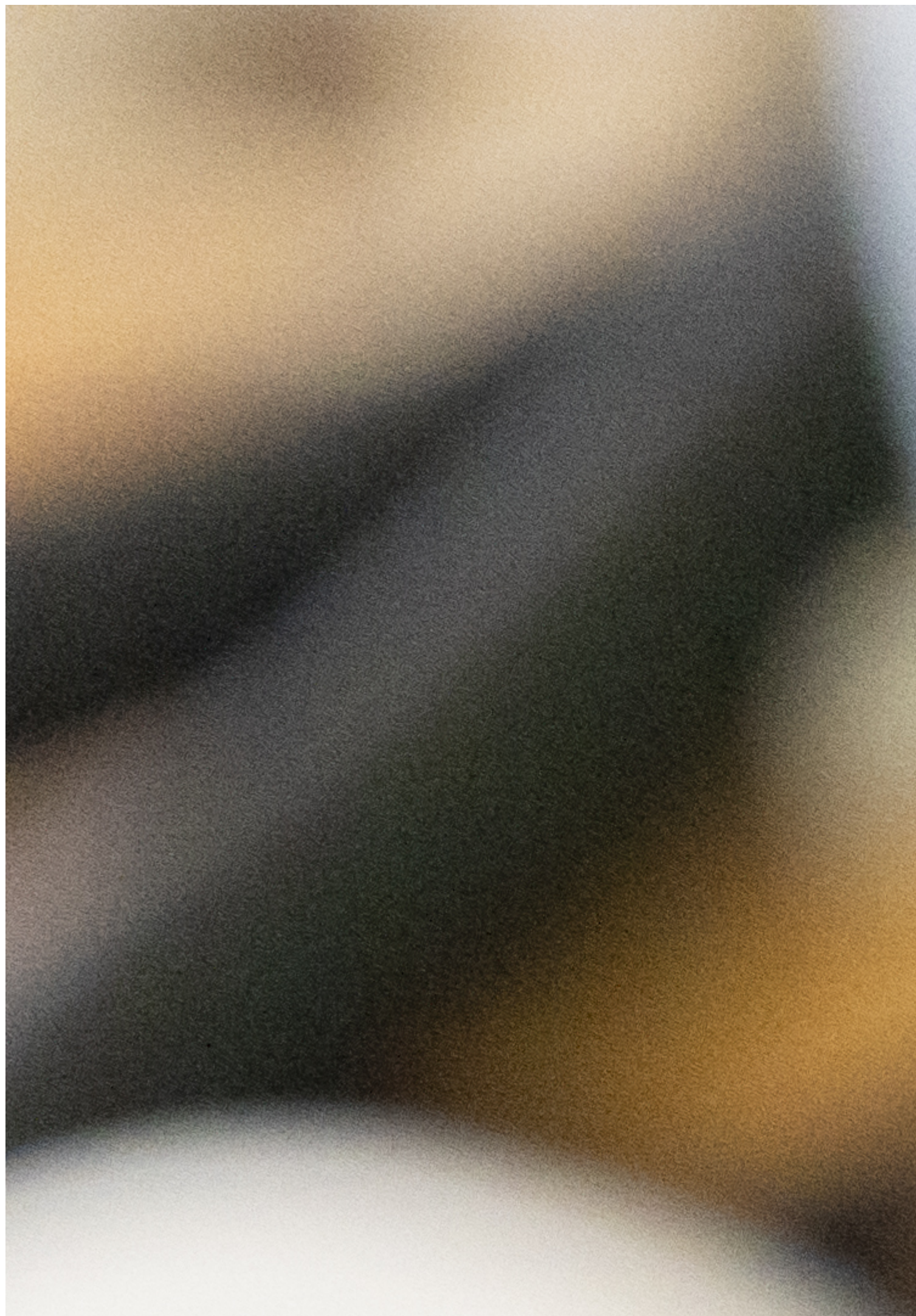
Nous sommes obligés de les répercuter sur les factures mais en général, les clients sont compréhensifs et, surtout, nous essayons de limiter ces hausses au strict minimum. Cette situation conjoncturelle mise à part, le grand défi actuel est la déferlante de l'intelligence artificielle. D'une part, elle est pleine de promesses mais d'autre part, elle facilite le travail des pirates informatiques. Je vous donne un exemple. Il n'y a encore pas si longtemps, les spams étaient faciles à détecter car ils contenaient des fautes, étaient mal écrits, etc. Maintenant, grâce à l'IA, les messages frauduleux sont de plus en plus réalistes et perfectionnés. Ils deviennent difficiles à détecter. Heureusement, les systèmes antispam se mettent à jour et nous, les professionnels, avons des outils pour détecter ces messages, mais nos clients pas toujours. C'est pour cela que, comme je vous le disais tout à l'heure, il vaut mieux qu'ils n'hésitent pas à nous faire suivre les messages douteux. C'est un bon réflexe.

Comment est la concurrence dans votre domaine ?

Je dirais qu'il y a du travail pour tout le monde. Comme nous ne fournissons pas tous exactement les mêmes services, nous sommes souvent amenés à collaborer avec un concurrent chez un client. Nous devons travailler en bonne intelligence et maintenir des rapports cordiaux et professionnels dans l'intérêt des clients. De notre côté, pour nous démarquer, nous mettons en avant notre approche directe et notre écoute.

Quels sont vos souhaits pour l'avenir de l'entreprise ?

Pour l'avenir et même le présent, je souhaite gérer la croissance de l'entreprise en maintenant la satisfaction de tous nos collaborateurs. Nous venons en effet de racheter une société qui était active dans le même domaine que le nôtre. Nous allons donc avoir plus de clients à servir. C'est une belle opportunité mais aussi un défi. Il m'importe beaucoup de maintenir une bonne atmosphère de collaboration entre les employés car l'entreprise, c'est eux ! On a également embauché pour faire face au surcroît d'activité et personnellement, je reste à l'écoute de tous





Les objets connectés et les applications utilisant l'intelligence artificielle représentent à la fois des opportunités de développements mais aussi des points de vigilance supplémentaires pour la sécurité des données (crédit Emmanuel Claude / Focalize).

Les salariés des entreprises peuvent être le premier rempart contre les attaques et intrusions, à conditions d'être soigneusement informés et formés aux bons réflexes de la sécurité informatique (crédit Emmanuel Claude / Focalize).