INFORMATIQUE & TELECOMS · IMPRESSION · MOBILIER · PAPETERIE · SERVICES GRAPHIQUES

trait d'union

L'AVENIR DU BUREAU ET DU NUMÉRIQUE SE **LIT** ICI

La cybersécurité, enjeu majeur pour tous

Tendances, maturité des TPE-PME françaises, point juridique et assurances... Tour d'horizon de la cybersécurité

eben
ENTREPRISES DU BUREAU ET DU NUMÉRIQUE

N°49 • septembre-octobre 2024

DANS CE NUMÉRO

trait d'union

Le magazine des professionnels du bureau et du numérique

Directeur de la publication : Arnaud Velthuizen

Rédaction : Delphine Cuynet, Valentine Zabarino, Corentin Prelot, Mélissa Baudère

Photos : Adobe Stock

Maquette : Ad'on Communication

69 rue Ampère 75017 Paris

Tel : 01 42 96 38 99

contact@federation-eben.com

L'actualité de votre métier en continu ! à suivre sur **federation-eben.com** et sur les médias sociaux

Edito

Cybermoi/s : mobilisons-nous autour de l'enjeu cyber auprès de nos clients

Arnaud Velthuizen, Président

Une étude menée par Talker Research pour Yubico dévoile que près de 4 personnes sur 10 n'ont jamais reçu de formation à la cybersécurité au sein de leur entreprise et plus d'un tiers (34 %) des sondés ont déclaré ne jamais avoir reçu d'instructions pour sécuriser leurs comptes professionnels, hormis l'utilisation d'un mot de passe, alors que 39 % pensent que l'emploi d'un nom d'utilisateur et d'un mot de passe est le moyen d'authentification le plus sûr.

Il est essentiel que chaque entreprise prenne conscience des risques et adopte une approche proactive. La cybersécurité ne doit pas être perçue comme une contrainte, mais comme un investissement indispensable pour la pérennité de nos activités. Nos adhérents, prestataires informatiques ont un rôle à jouer. Ils ont un devoir de renseignement, de mise en garde et de conseil vis-à-vis du client. Avec leur expertise, leur savoir-faire et leur connaissance approfondie du marché de l'IT, ils doivent sensibiliser leurs clients et leur transmettre des conseils personnalisés en cybersécurité pour renforcer leur protection. Pour ce faire, la Fédération accompagne ses adhérents et met à disposition des outils : lettre d'information Cybersécure, décryptage de la Directive NIS 2 et du règlement DORA, enrichissement du pack juridique avec des conditions particulières pour les prestations de cybersécurité notamment.

Chaque année, en octobre, nous célébrons le Cybermoi/s, campagne de sensibilisation à la cybersécurité. Cette initiative, pilotée par Cybermalveillance.gouv.fr, vise à promouvoir le sujet de la cybersécurité à travers les pays de l'UE pour permettre de mieux comprendre les menaces et les appréhender. Le Cybermoi/s est l'occasion pour chacun de nous de renforcer nos connaissances, de sensibiliser nos clients et de mettre en place des mesures de protection efficaces contre les cybermenaces.

En travaillant ensemble, en partageant nos expériences et nos bonnes pratiques, nous pouvons créer un environnement numérique plus sûr pour tous.

Restons vigilants et unis face à ces enjeux.

Partenaires

TPE et cybersécurité : sont-elles prêtes ?

Ces dernières années, les cyberattaques se sont largement répandues auprès de toutes les entreprises.
Loin d'être épargnées et souvent bien moins armées que les ETI ou les grands groupes, les TPE-PME sont une cible de choix pour les cybercriminels : avec plus de 4 millions d'entreprises, elles constituent 99 %* du tissu économique français.

Une situation qui n'a pas échappé aux principales organisations patronales qui, fort de l'enjeu que représente la cybersécurité, ont décidé de faire front aux côtés du Club EBIOS et de Cybermalveillance.gouv.fr pour lancer une opération conjointe appelée ImpactCyber, afin de convaincre les TPE-PME de se sécuriser en amont.

Première étape de l'opération, la mise en place d'un état des lieux du niveau de maturité cyber des TPE au travers d'une étude** réalisée par OpinionWay pour Cybermalveillance.gouv.fr

Retour en chiffres sur les principales conclusions de cette enquête**.

Des TPE-PME conscientes des risques cyber

De façon assez surprenante, il y a un vrai consensus autour de la cybersécurité : près de 6 entreprises sur 10 considèrent que c'est un sujet qui doit mobiliser tout le monde. Ainsi, plus de la moitié d'entre elles sensibilisent leurs collaborateurs, davantage encore dans les grandes entreprises (79 % des entreprises de 50 salariés et plus et 71 % des entreprises de 10 à 49 salariés).

En toute lucidité, plus de la moitié n'hésite pas à reconnaître être faiblement protégée (42 %), notamment celles de plus de 10 salariés, ou ne pas savoir l'évaluer (19 %).

C'est surtout le manque de temps (60 %), de connaissances / d'expertise (56 %) ou de budget (53 %) voire de ne pas savoir à qui s'adresser (34 %) qu'elles invoquent pour expliquer pourquoi elles n'arrivent pas à atteindre le bon niveau de cybersécurité.

En revanche, plus rassurant, pour s'informer ou se faire aider, les entreprises semblent se tourner prioritairement vers leur prestataire informatique. Cybermalveillance.gouv.fr est cité en deuxième position, particulièrement dans les entreprises de 50 salariés et plus.

Côté équipements, 9 entreprises sur 10 paraissent dotées d'un dispositif de sécurité, tels qu'un antivirus ex-aequo avec les sauvegardes (87 %) ou un pare-feu (66 %).

...mais qui en sous-estiment les enjeux

Derrière cette apparente « prise de conscience », la réalité est toute autre.

Si la plupart se disent insuffisamment préparées (46 %) ou l'ignorent (32 %), 7 entreprises sur 10 ne disposent pas de procédure de réaction.

Pire encore, quand on sonde sur leur niveau d'exposition, seules 38 % des entreprises reconnaissent qu'elles sont fortement exposées à ces risques, en particulier les victimes d'une attaque (57 %) et les entreprises de plus 50 salariés et plus. *A contrario*, la grande majorité d'entre elles pense être faiblement exposée aux risques de cyberattaques (41 %) ou l'ignorent (21 %). Pas étonnant non plus dans ce cas que 7 entreprises sur 10 ne disposent pas de procédure de réaction en cas d'attaque. Cela

n'arriverait-il qu'aux autres ?

En matière d'équipements, ce n'est guère mieux : si près de 7 entreprises sur 10 déclarent connaître des solutions de sécurité, plus d'1 sur 2 ne sait pas si ces solutions sont adaptées ou non à ses besoins (42 %) ou pense qu'elles ne le sont pas (11 %).

...avec une expertise limitée en termes de cybersécurité

Comment réagiraient-elles en cas de cyberattaque ?

Interrogées, les entreprises reconnaissent que si elles y étaient confrontées, 65 % ne sauraient pas en évaluer les impacts ; seules 35 % d'entre elles pensent qu'elles auraient la capacité de le faire, et particulièrement celles qui sont conscientes d'avoir un faible niveau de protection.

Ce qu'elles redoutent le plus ?

Une destruction ou un vol de données, une perte financière (94 %), une interruption des activités et services (90 %) et une atteinte à l'image de l'entreprise (80 %).

Dans les faits, 15 % des entreprises interrogées déclarent avoir été touchées par un incident de cybersécurité durant les 12 derniers mois. Si près d'1 sur 2 ne saurait les expliquer, pour les autres, ces incidents seraient liés à un hameçonnage (24 %), au téléchargement d'un virus (18 %) ou encore à une faille de sécurité non corrigée pour 14 % d'entre elles.

Et en termes d'impacts avérés, c'est l'interruption d'activité (35 %), le vol de données (25 %), l'atteinte à l'image de l'entreprise (17 %), qui constituent le trio de tête avant la perte financière (15 %) ou la destruction de données (12 %).

Des TPE-PME aux moyens limités et inégaux

Si on a trop souvent tendance à l'oublier, cette catégorie d'entreprises joue un rôle économique crucial et assure un véritable maillage territorial en France ; pour autant, la plupart (95 %) comptent moins de 10 salariés. Et dans ce type de configuration, bien souvent le dirigeant fait aussi office de de DSI. Côté budget, pour 85 % des entreprises, l'enveloppe allouée à l'Informatique est inférieure à 5 000 € par an, particulièrement pour les plus petites (98 % des entreprises de 0 salarié) ; et en matière de cybersécurité, cette enveloppe serait évaluée... à moins de 2 000 € pour 68 % d'entre elles.

Une réalité d'autant plus préoccupante que seules 10 % d'entre elles prévoient de l'augmenter (notamment celles de plus de 50 salariés) et que la majorité n'entrevoit pas davantage de recruter des ressources spécialisées en cyber dans l'année à venir.

Dans un tel contexte, on comprend d'autant plus facilement la facilité ou le pragmatisme dont elles peuvent faire preuve en termes de porosité des usages : ainsi, plus d'1 entreprise sur 2 a recours à des équipements personnels à des fins professionnelles, téléphone portable en tête (95 %) ; 1/3 utilisent leur propre ordinateur et 28 % leur messagerie personnelle.

Et si on note un certain équilibre entre les entreprises ayant fait le choix d'externaliser leur informatique (40 %) ou de l'internaliser (37 %), 27 % indiquent que la gestion de leur cybersécurité est inexistante, notamment pour les petites entreprises.

Face à ces constats, une campagne de communication pour convaincre les TPE-PME de passer à l'acte en se sécurisant a été lancée par Cybermalveillance.gouv.fr et les principales organisations patronales. Ainsi, 3 films ont été réalisés et déclinés à travers des affiches, des prospectus, des kakémonos et des bannières. Enfin, un mémento de cybersécurité à destination des dirigeants de TPE-PME complète l'opération ImpactCyber. À travers des récits de cyberattaque inspirés de faits réels, des témoignages de dirigeants et des conseils et des solutions pragmatiques, il a pour objectif d'accompagner les chefs d'entreprise pour leur permettre de se protéger face aux cybermenaces.

Plus d'informations sur https://www.cybermalveillance.gouv.fr/tous-nos-contenus/actualites/impact-cyber

**Insee, Ésane, 2021*

***Enquête OpinionWay pour Cybermalveillance.gouv.fr, réalisée en ligne entre le 10 juin et le 16 juillet 2024 auprès d'un échantillon de 513 entreprises de moins de 250 salariés en France métropolitaine et régions d'Outre-Mer, représentatif des enreprises françaises de moins de 250 salariés en termes de taille par tranche de salariés et de macro-secteurs d'activité.*

CYBER MOIS

“La cybersécurité ?
Je m'en préoccuperai le
jour où je serai concerné !”

FAUSSE BONNE IDÉE

PARCE QUE LES CYBERATTAQUES N'ARRIVENT PAS QU'AUX AUTRES, DEVENEZ #CYBERENGAGÉS

DU 1ER AU 31 OCTOBRE

EN SAVOIR PLUS SUR
CYBERMOIS.CYBERMALVEILLANCE.GOUV.FR

#CyberEngagés

SHARP
Be Original.

Secure Office,
votre allié contre
les cybermenaces

Protégez les données de vos clients avec le ***Secure Office*** de Sharp !
Grâce à nos solutions à la pointe de la sécurité, renforcez la protection de leur environnement informatique et gardez leurs données à l'abri des cyberattaques.

Formation
& audit cyber

Protection
des données

Sauvegarde
informatique

Une assurance cyber, et si c'était le bon moment ?

Pour vous parler de manière concrète de Cybassur.fr, assurance cyber partenaire de la Fédération EBEN, nous allons opportunément rebondir sur la dernière enquête de conjoncture réalisée par la Fédération.

Face aux défis de l'intelligence artificielle et de la cybersécurité, les résultats de cette enquête dressent un état des lieux d'une menace cyber toujours plus préoccupante pour les petites entreprises puisque 40 % des sondés ont subi au moins une cyberattaque au cours des 12 derniers mois.

Lorsque de tels chiffres viennent des enquêtes des compagnies d'assurance, il est compréhensible de les discuter...Ceux-ci, vous en conviendrez, doivent être fiables. Et pourtant, nombre de petites et moyennes entreprises ne sont toujours pas couvertes par une assurance cyber...

Ce n'est pas faute de vous rappeler à chaque occasion, que cette assurance est devenue essentielle, que son tarif est extrêmement compétitif grâce à des conditions spécifiques pour les adhérents EBEN et que les garanties proposées sont hyper performantes !

Voilà près de 10 ans que nous nous sommes spécialisés dans la couverture du risque cyber. Notre expertise est reconnue à sa juste valeur tant par nos clients que par les compagnies, parce que nous sommes d'abord les partenaires de nos assurés avant d'être des vendeurs de solutions d'assurance. La différence que nous vous proposons de mettre à votre service, c'est le conseil basé sur une expertise solide.

Pour aller à l'essentiel, un devis pour une assurance cyber est un service gratuit et sans engagement qui comprend un scan externe de vos systèmes d'information. Pas de questionnaire et pas de petites lignes indigestes en bas de page !

Notre engagement : vous apporter une proposition d'assurance sous 24h après un premier échange téléphonique.
Bien sûr, avec une tarification spécifique pour les adhérents EBEN !
Pour en parler, contactez-nous par mail ou téléphone :
smonestier@cybassur.fr / 02 54 22 16 20

Jean-Jacques Latour, Directeur Expertise Cybersécurité de Cybermalveillance.gouv.fr répond à nos questions

• Pouvez-vous nous présenter Cybermalveillance.gouv.fr ?

Cybermalveillance.gouv.fr est la plateforme du dispositif national de prévention et d'assistance aux victimes de cybermalveillance. Il s'agit d'un Groupement d'Intérêt Public (GIP), c'est-à-dire un partenariat public – privé, dans lequel nous allons retrouver :
- Des acteurs étatiques comme le Ministère de l'Intérieur, de la Justice, de l'Economie et des Finances, des Armées, etc.
- Les représentants des prestataires tels que la Fédération EBEN, Cinov, Numeum
- Les utilisateurs, les associations de consommateurs, de victimes, des collectivités locales, ...
- Un certain nombre de grands groupes qui viennent nous donner leur appui dans notre mission de service public. Nous pouvons citer par exemple La Poste, la SNCF pour la France mais également des grands groupes internationaux comme Microsoft, Google, Amazon.

• Dans l'étude que vous publiez, on observe que 15 % des entreprises déclarent avoir été victime d'une cyberattaque durant l'année écoulée. De votre côté, quelles sont les principales menaces pour lesquelles elles viennent chercher de l'assistance sur votre plateforme ?

Les principales menaces pour les entreprises :

• **le hameçonnage** : message que vous pouvez recevoir par mail, sms, appel téléphonique, par messagerie instantanée,... L'objectif est de capter votre attention pour vous inciter à divulguer des informations confidentielles

LES MISSIONS DU GIP

1. La prévention

En promouvant les bonnes pratiques à adopter pour éviter les différentes formes de cybermalveillance au travers de différents supports à vocation pédagogique et accessibles à tous les publics y compris les non-spécialistes : articles, infographistes, affiches, vidéos, guides...

2. L'assistance aux victimes

Celle-ci se décline en supports, articles et contenus diffusés sur notre site. Nous avons aussi créé un outil de diagnostic en ligne qui permet aux victimes d'identifier leur problème et de poser un diagnostic. Nous proposons ensuite à la victime des conseils personnalisés qui peuvent être d'ordre administratif (faut-il déposer plainte, comment faire opposition à ma carte bancaire, quelles associations peuvent me venir en aide,...) ou technique avec notamment la possibilité d'être mis en relation avec un réseau de près de 1 500 prestataires de proximité. Ces professionnels implantés sur l'ensemble du territoire ont signé une charte les engageant à respecter l'état de l'art, les bonnes pratiques, les tarifs... Ils remontent également de l'information du terrain puisqu'ils transmettent des rapports d'intervention, ce qui va permettre d'alimenter notre 3e mission :

3. L'observation de la menace

Pour pouvoir donner des conseils et aider les publics à se protéger, il faut bien connaître la menace et comprendre les modes opératoires. Aujourd'hui, sur la plateforme, nous référençons plus de 50 formes de cybermalveillance différentes qui peuvent toucher les publics professionnels et particuliers.

RÉPUBLIQUE FRANÇAISE
Liberté
Égalité
Fraternité

CYBER MALVEILLANCE .GOUV.FR
Assistance et prévention en cybersécurité

Les conséquences d'un piratage de messagerie et d'une arnaque au faux RIB sont nombreuses pour une TPE-PME.
Vol de données, perte financière, contentieux…
L'activité de l'entreprise est menacée. Les clients sont impactés.
Heureusement, il existe des réflexes simples à adopter pour se protéger.

→ 1 Sensibilisez vos collaborateurs aux différentes cybermenaces pour leur permettre de savoir réagir face à un message d'hameçonnage.

→ 2 Activez la double authentification pour limiter les intrusions.

→ 3 Pour sécuriser vos règlements par virement, mettez en place une procédure de confirmation du numéro de RIB.

→ 4 Sécurisez-vous en vous faisant accompagner par un prestataire labellisé en cybersécurité grâce à « Mon ExpertCyber ». →

TPE-PME, FACE AUX CYBERATTAQUES
Pour garder vos clients, protégez-vous dès maintenant.

Campagne réalisée en partenariat avec

(mot de passe, coordonnées bancaires, ...) ou réaliser une action comme ouvrir un fichier contaminé par un programme malveillant qui viserait à prendre le contrôle de votre poste ou du système d'information. Il s'agit d'un vecteur d'attaque, le problème n'est pas de recevoir le message mais d'être vigilant sur la suite à donner.

• **le piratage de compte** : il s'agit de la 2ème menace qui touche les publics professionnels. Les cybercriminels prennent le contrôle sur les comptes de messageries des entreprises, les comptes Microsoft 365, les comptes de réseaux sociaux qui bien souvent, sont les vitrines de l'entreprise.

• **le rançongiciel** : Attaque qui peut commencer par un hameçonnage ou par la recherche d'une vulnérabilité sur le réseau. Le cyberattaquant va profiter d'une faille de sécurité pour entrer dans le réseau, chiffrer les données, détruire les sauvegardes et demander une rançon à l'entreprise pour lui redonner l'accès. Cette menace est en forte hausse, l'année dernière, ce sont plus de 1 400 entreprises qui sont venues sur la plateforme pour des faits de rançongiciels, plus de 400 collectivités (+16 % par rapport aux années antérieures). On constate que les petites structures ne sont pas épargnées, bien au contraire. Il y a toujours des cybercriminels qui essaient de s'attaquer à des grosses structures mais cela demande des compétences très poussées puisque ces structures ont élevé leur niveau de protection. On assiste donc à des attaques très opportunistes, les cybercriminels scannent internet et attaquent lorsqu'ils trouvent des portes ouvertes. Pour les petites structures, les conséquences peuvent être particulièrement dévastatrices. Malheureusement, ce n'est pas parce qu'on paye la rançon qu'on va retrouver l'intégralité de ses fichiers. Certains pirates demandent une deuxième rançon. Aussi, certaines entreprises doivent faire face à une réplique avec une nouvelle demande de rançon. Les entreprises se retrouvent à l'arrêt pendant plusieurs jours voire plusieurs mois, ce qui peut conduire à la cessation d'activité de l'entreprise.

• **fraudes aux virements** : on enregistre une augmentation de cette menace de 63 % entre 2022 et 2023. Suite au piratage du compte d'un créancier ou de l'entreprise, elle va recevoir une facture qu'elle attend, avec un RIB sur lequel effectuer le règlement, or ce RIB appartient à un escroc. Là aussi, on arrive à des situations financières très compliquées.

• Quels rôles jouent les prestataires de services IT dans l'accompagnement des entreprises face à ces menaces ?

Ils jouent un rôle déterminant. Ce que révèle notre étude, c'est que la grande majorité des entreprises de moins de 250 salariés (et à fortiori celles de moins de 50 salariés), n'ont pas de salarié en charge de l'IT. Dans 95 % des cas, ce rôle incombe au dirigeant d'entreprise ou de son assistante administrative qui appelle les prestataires pour pouvoir gérer tous les problèmes liés à l'IT.

Ce que les prestataires doivent bien avoir en tête, c'est qu'ils ont un devoir contractuel de conseil. Par exemple, si le prestataire constate que le client ne fait pas ses sauvegardes correctement, il a le devoir d'informer le client et de lui expliquer comment procéder pour sécuriser le fonctionnement de son entreprise.

Afin de garantir un accompagnement de qualité et un niveau de compétence minimal, nous avons créé le label ExpertCyber avec les principaux syndicats professionnels du secteur dont Eben, la Fédération française de l'Assurance et le soutien de l'Afnor. Aujourd'hui, plus de 200 prestataires sont labellisés ExpertCyber et ont une expertise reconnue dans les domaines suivants :

- sécurisation en amont,
- maintien en conditions de sécurité,
- réponse à incident.

Bien souvent, ce sont des petites entreprises qui ont une vraie compétence et qui ont la capacité d'intervenir en proximité (70 % dans les territoires) et de s'adresser à des PME voire des TPE.

• Quelles sont les recommandations essentielles que vous donneriez aux entreprises pour se prémunir ?

D'abord, les entreprises doivent vraiment prendre conscience du risque. Comme

beaucoup le disent, la question n'est pas de savoir si vous allez être attaqués mais quand ? Si vous n'avez pas encore été attaqué, ce n'est qu'une question de temps. Le chef d'entreprise doit donc être pro-actif et doit couvrir ce risque à minima. Il ne faut pas hésiter à se faire accompagner, la cybersécurité est un métier, il faut faire appel à des spécialistes. Ça ne coûte pas forcément cher, ça peut commencer par 2 heures de prestation pour auditer les systèmes d'information, pointer du doigt les éventuelles grandes failles de sécurité et les principaux axes de progrès pour limiter les risques.

Il faut élever son niveau de sécurité au juste niveau. Il n'est pas question de transformer une PME en Fort Knox américain ! Souvent, on se rend compte que des mesures simples de sécurité permettent d'éliminer toute une quantité de cyberattaques ou tout du moins d'en limiter les impacts. Par exemple, si je fais une sauvegarde sur un disque dur externe, je n'ai pas tout perdu le jour où je suis victime d'une cyberattaque.

• Octobre, c'est le CyberMoi/s en France, quelle est votre actualité vis à vis des entreprises ?

C'est le mois européen de la cybersécurité, initiative européen conçue par l'Agence de l'Union Européenne pour la cybersécurité (ENISA) qui vise à promouvoir le sujet de la cybersécurité à travers les pays de l'Union Européenne. Depuis 2023, le CyberMoi/s est piloté par Cybermalveillance.gouv.fr

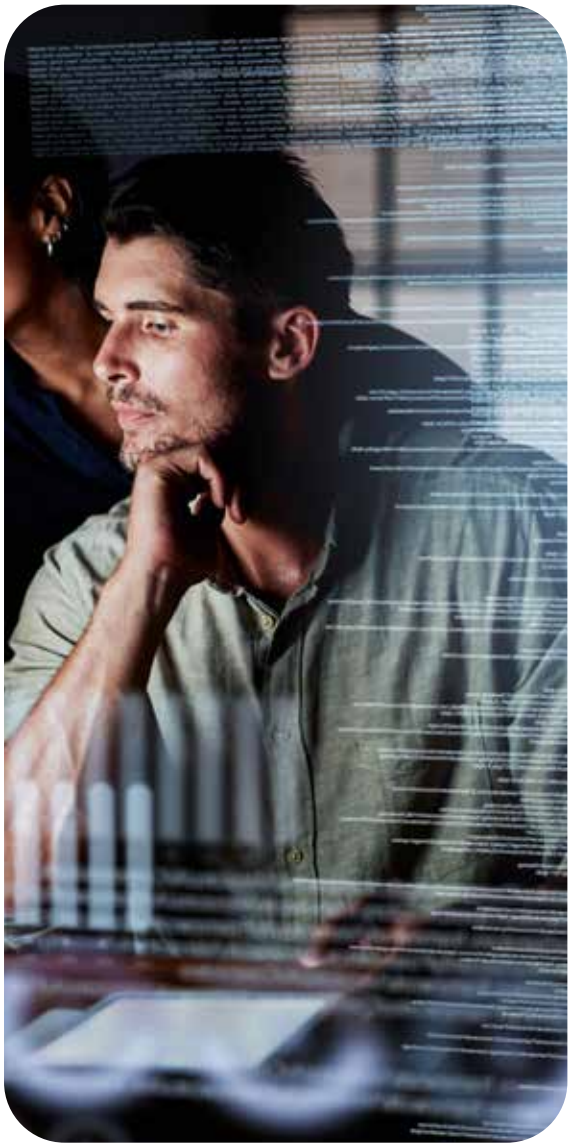
Un évènement de lancement officiel retransmis en direct se tiendra à l'Assemblée nationale. Et tout au long du mois d'octobre 2024, des activités vont être organisées en France et en Europe autour des enjeux de cybersécurité :

👉 L'agenda de Cybermalveillance.gouv.fr

Nous avons mis à disposition de tous les publics un agenda qui recense toutes les manifestations dans le domaine de la cybersécurité, sur l'ensemble du territoire. Vous pouvez consulter l'agenda en ligne ou même y inscrire vos propres événements ici Nous avons aussi réalisé l'étude « Impact Cyber » avec OpinionWay qui vise à faire un état des lieux du niveau de maturité cyber des TPE.

Nous allons diffuser des vidéos de sensibilisation avec un angle original puisqu'on met en évidence les problèmes qu'une cyberattaque peut poser aux clients de l'entreprise (perte de confiance, perte de clients, rupture de chaîne d'approvisionnement, ...)

Enfin, nous réalisons un memento avec des cas concrets, des conseils, des témoignages pour expliquer aux entreprises ce qu'est une cyberattaque, décrypter les principaux types de menaces et donner des recommandations pour les inciter à franchir le pas et se faire accompagner. ●



Propos recueillis par Delphine Cuynet

Sébastien MORIN • HEXATEL

Confiance et transparence au cœur de notre philosophie

• Pouvez-vous nous parler de votre cursus professionnel ?

J'ai été immergé dans le monde des télécoms dès mon plus jeune âge. Influencé par ma mère tout d'abord, qui dirigeait une entreprise dans ce domaine à Orléans ; mais également par mon beau-père à la tête d'une société basée à Rennes et spécialisée dans le même secteur d'activité.

Après des études en école de commerce, j'ai entamé ma carrière dans divers secteurs avant de rejoindre l'entreprise familiale. En 2001, j'ai intégré Hexatel, qui portait alors un autre nom, en débutant au service marketing. J'ai occupé ensuite différents postes afin de développer une connaissance approfondie de l'ensemble des activités et des métiers de l'entreprise. En 2004, j'ai pris la direction de l'entreprise avec pour objectifs premiers de renforcer notre position sur le marché et de consolider les choix stratégiques initiés.

En effet, dès 2000, nous avions saisi l'opportunité d'intégrer des services opérateurs à notre offre. Nous nous sommes positionnés très tôt sur ce marché, ce qui nous a permis de nous démarquer rapidement. En l'espace de trois ans, nous sommes devenus un acteur majeur du secteur, à la fois en tant qu'installateur et dans la commercialisation de services opérateurs.

En 2009, j'ai accepté la proposition de mon beau-père de reprendre l'entreprise rennaise, tout en continuant à collaborer avec ma mère à Orléans. J'ai mené les deux sociétés en parallèle jusqu'à leur fusion en 2015 sous la marque Hexatel. Depuis cette date, nous avons consolidé notre présence nationale grâce à plusieurs acquisitions stratégiques, et nous comptons désormais une trentaine d'agences technico-commerciales à travers le territoire.

• Vous êtes président d'Hexatel, pouvez-vous nous présenter la société ?

Hexatel est l'un des principaux opérateur-intégrateur télécoms et réseaux indépendant en France.

Notre entreprise est présente sur l'ensemble du territoire Français et compte 300 collaborateurs. En 2023, nous avons réalisé un chiffre d'affaires avoisinant les 43 millions d'euros annuels.

Hexatel est une entreprise 100% indépendante puisque qu'elle n'a recours à aucun capital externe, Ce qui est de plus en plus rare dans notre secteur d'activité. Cette indépendance garantit une maîtrise totale de notre développement puisque chaque décision technologique est le fruit de nos propres choix stratégiques.

L'entreprise est née il y a bientôt 80 ans pour répondre aux besoins télécoms de son époque. Depuis, elle a traversé toutes les grandes révolutions technologiques dans le domaine de la téléphonie et a su élargir son champ de compétences et de services.

Nous intervenons désormais sur trois secteurs majeurs : les communications d'entreprises, les services Internet et réseaux et la sécurité des personnes (dans le domaine de la santé principalement). Nous intégrons des solutions complètes pour connecter et optimiser les échanges professionnels. Nous offrons à nos clients des infrastructures intégrées allant de la téléphonie aux réseaux en passant par les équipements matériels, en garantissant une approche clé en main.

Et Hexatel continue à se réinventer puisque nous proposons depuis peu à nos clients des prestations de services managés informatique (hébergement, sauvegarde, infogérance, Office365...).

• Quels enseignements tirez-vous des crises successives que l'on a connues ?

La crise des subprimes a permis de confirmer une stratégie déjà initiée chez Hexatel quelques années auparavant : celle de la récurrence des revenus. Actuellement 65 % de notre chiffre d'affaires provient de la facturation de services récurrents. Cela nous permet d'être moins dépendant de la volatilité des commandes et peut être moins vulnérable lors de crises importantes.

Avec le Covid, nous avons dû pour la première fois mettre en sommeil l'entreprise du jour au lendemain. On ne se doutait pas que le redémarrage serait aussi lent ensuite ! Avec un peu de recul, on ne mettrait certainement pas

autant l'entreprise à l'arrêt. Nous avons eu de nombreuses demandes pour router les appels téléphoniques vers des mobiles. Nous n'avons pu apporter à cet instant que des solutions de dépannage et non un projet de communication unifiée bien réfléchi. Ce type de demande est venu dans un second temps.

• Selon vous, quels sont les enjeux de votre marché ?

Selon moi, l'enjeu principal de notre marché est la convergence des métiers. Il y a 20 ans, j'ai choisi de lancer les services opérateurs en plus de la vente d'installations téléphoniques. J'étais pour cela parti du constat que nos clients, en cas de souci, se retrouvaient avec trois interlocuteurs différents : Orange pour l'abonnement téléphonique, un opérateur alternatif pour les communications téléphoniques (à la fin du monopole d'Orange) et nous pour le matériel. Les deux premiers se renvoyant souvent la balle, les clients se tournaient vers leur prestataire le plus proche : nous. Dorénavant, nous intervenons à tous les niveaux pour donner un interlocuteur unique et apporter une réelle valeur ajoutée à nos clients.

La convergence des métiers dans notre domaine est toujours un sujet à l'heure actuelle selon moi. Même si les offres que nous proposons sont de plus en plus dématérialisés, nous devons avoir la capacité d'accompagner nos clients sur les problématiques télécoms, informatique et réseaux d'un bout à l'autre de la chaîne (conseil, installation, équipements, maintien en service...).

• Avez-vous des projets de développement ?

Nous poursuivons des projets d'expansion géographique et de consolidation. Lors d'acquisitions, nous souhaitons avant tout préserver notre philosophie et nos valeurs. Il nous tient à cœur que les employés des entreprises acquises puissent s'aligner naturellement avec notre culture d'entreprise et notre philosophie.

• Vous investissez-vous dans des projets extra-professionnels ?

Matériellement, je n'ai pas trop le temps et peut-être pas la volonté aussi de m'investir dans l'associatif aujourd'hui. Toutefois, je suis très présent sur les concours hippiques depuis 4-5 ans pour accompagner ma femme et mes filles.

• Pouvez-vous nous partager une anecdote professionnelle ?

Un des souvenirs qui me tient particulièrement à cœur est l'évènement que nous avons organisé pour fêter les 70 ans d'Hexatel. C'était en 2016 et nous avions privatisé pour l'occasion le Château de Chambord. Le temps d'un week-end, nous avons pu rassembler l'ensemble de nos équipes et leur famille dans ce lieu unique. C'est également à cette occasion que mon beau-père et ma mère ont effectué le passage de témoin en me transmettant la direction de l'entreprise à 100 %.

• Quel serait le pire souvenir de votre carrière ? Et le meilleur ?

Je pense que l'année 2020 dans son ensemble est mon pire souvenir. Il y a eu tout d'abord, le décès de mon beau-père en février (ancien dirigeant de l'entreprise). La crise du COVID et le confinement imposé nous a ensuite contraint à rapidement mettre en sommeil l'entreprise. Cette décision est intervenue quelques semaines après l'inauguration de l'extension du siège rennais. Elle nous a contraint à limiter nos activités et nos contacts.

Pour le meilleur souvenir, je citerai notre séminaire annuel. Comme je l'évoquais la crise COVID à tenu les collaborateurs isolés pendant de longs mois. Au quotidien, nous n'avons pas non plus l'occasion de nous voir physiquement car les équipes sont éclatées sur une trentaine d'agences en France. Chaque année, le séminaire nous permet de tous nous réunir et de partager de bons moments ensemble. C'est un rendez-vous très important et attendu par tous.

• Comment on gère une société avec autant d'agences réparties en France ?

Nous nous appuyons sur l'un des piliers de notre culture d'entreprise : la confiance. C'est une valeur à laquelle tout le monde adhère : collaborateurs, clients, moi-même en tant que dirigeant d'entreprise multisites.

D'un point de vue pratique, nous avons massivement investi dans notre système d'information afin d'entretenir une bonne dynamique de travail, peu importe la localisation du collaborateur. En tant que dirigeant, je mets également un point d'honneur à informer régulièrement les équipes sur les résultats et les grandes orientations stratégiques que nous prenons. Cela répond à un autre de nos piliers : la transparence. Ces deux éléments sont très importants car ils participent au bien-être de tous, pérennisent les équipes et limitent le turnover.

• Que vous apporte la Fédération EBEN ?

EBEN nous permet d'échanger facilement entre confrères et de nous ouvrir à d'autres métiers, également présents au sein de la Fédération. EBEN met à disposition de tous ses adhérents de nombreux services : les différents packs, l'aide au changement de convention collective et des informations partagées. Nous avons déjà pu en bénéficier à plusieurs reprises.

A l'avenir, nous aimerions nous aussi apporter notre contribution à la Fédération EBEN en faisant notamment grandir la communauté des télécoms parmi les adhérents.

• Avez-vous une devise ?

Elle n'est pas très originale mais je l'utilise à la fois dans la professionnel et le personnel : « *Un problème, une solution* ». ●

Propos recueillis par Valentine ZABARINO

Au fil du droit

Cybersécurité : inflation juridique, opportunité professionnelle et source de risque

La cybersécurité est tout à la fois un cadre complexe, une source presque infinie de business et une nouvelle source de risque.

Un cadre complexe et presque complet

Dans le domaine de l'informatique et du numérique, la cybersécurité est assurément le domaine du droit qui a connu le plus de textes sur les 10 dernières années. Tout a commencé en 1978 avec la loi informatique et libertés et 2 articles consacrés à la sécurité des données personnelles. Puis dix ans plus tard, en 1988, le législateur intègre dans le Code Pénal un ensemble de dispositions consacrées à la fraude informatique. La machine législative a commencé à s'emballer avec la loi pour la sécurité intérieure, la loi pour la sécurité au quotidien, LOPSI 1 et 2, LPM, ...

Avec le développement des cyberattaques, les acteurs publics ont renforcé considérablement l'arsenal juridique avec un texte de nature générique et des textes de nature sectorielle. Le texte de portée générale est l'incontournable RGPD et son lot d'obligations de sécurité en amont (mesures de sécurité, audit, contrat prestataire, analyse d'impact) et en aval (notification Cnil, PCA, PRA, forensic, ...). Les textes sectoriels visent des pans entiers de notre économie et autant de vos clients :

- DORA pour le secteur banque, finance, assurance ;
- NIS 2 pour les secteurs d'activités considérés comme critiques et hautement critiques ;
- eIDas 2 pour les prestataires de services de confiance ;
- le PGSSI-S pour le secteur santé ;
- ou encore l'IA Act particulièrement pour les professionnels proposant des IA ;
- sans oublier le Cybersecurity Act notamment

pour les services Cloud, Cyber Resilience Act, le Data Act, etc.

Il y en a donc pour tout le monde ou presque. Même les acteurs publics ou privés qui ne sont pas directement impactés par ces règlementations le sont indirectement. En effet, ces nouvelles règles feront assurément office de référentiel de bonnes pratiques.

Le point commun de toutes ces règlementations est la redéfinition de rôle et responsabilité entre le client et ses prestataires IT. La plupart de ces textes imposent de considérer les prestataires IT tiers comme une source particulière de risque. Sur le plan contractuel, certains textes comme le RPGD, DORA ou l'IA Act imposent même des clauses contractuelles. Le prestataire se voit donc de moins en moins libre d'imposer ses propres conditions générales.

Une source presque infinie de business

La cybersécurité est une source de business importante pour les membres de la Fédération. Les besoins des clients sont très larges.

La première source de business porte sur des prestations de conseil. Les clients ont en effet besoin de comprendre les obligations qui sont les leurs et d'auditer leurs pratiques soit par rapport aux textes sectoriels mentionnés plus haut soit par rapport à d'autres référentiels (Règles d'hygiène de l'ANSSI, normes,...). Les prestations de conseil peuvent aussi consister à accompagner le client dans ses certifications, notamment la suite ISO 27000.

La seconde source de revenus presque « naturelle » est la mise à disposition, le déploiement et toutes les prestations associées (formation, support, maintenance, ...). La liste des prestations potentielles est longue : elles peuvent porter sur du hard, du soft, du service et très souvent la combinaison des trois.

Certaines prestations sont plus pointues et nécessitent des moyens plus importants aussi bien côté client que prestataire : Data Center, PCA, PRA, SoC, ... Ce sont autant de prestations qui s'imposent aux clients dont les exigences de sécurité sont plus importantes que les autres.

Au rang des prestations spécialisées, on notera les prestations d'audit de sécurité comme le test d'intrusion (pentest) particulièrement imposés par le règlement DORA mais aussi l'ensemble des prestations de type forensic dans le cadre d'une attaque informatique. Ces prestations sont très rémunératrices, généralement prises en charge par l'assureur du client (pour autant que le client soit assuré), mais nécessitent des moyens, notamment humains, assez importants et pouvant être mobilisés sur l'heure.

Une nouvelle source de risque

Enfin, la cybersécurité est une nouvelle source de risque juridique, ce qui est le corollaire de tout nouveau business. On peut distinguer les risques anciens remis au goût du jour et les risques vraiment nouveaux. Dans la catégorie « risques anciens » remis au goût du jour, on mentionnera l'éternelle obligation de conseil. Ce risque est d'autant plus important que même les conseils les plus avisés n'empêcheront pas les pirates de pirater. En tant que professionnel, il est donc très important de bien préciser quelles sont les limites de vos conseils et recommandations à destination des clients. Les prestations liées à la sécurisation d'un SI, elles aussi, poseront de nouvelles questions. Si l'on prend l'exemple des tests intrusifs, il y a fort à parier que si, après des tests considérés comme positifs, une entreprise se faisait pirater, le client mettra en cause la responsabilité de son prestataire. Il en sera de même pour un SoC défaillant ou encore un défaut de patch management. Ici, en dehors du professionnalisme de chacun, la maîtrise du risque passera par des contrats bien rédigés et une assurance professionnelle adaptée (nous ne pouvons de ce point de vue que vous suggérer de contacter Cybassur, partenaire de la Fédération).

Pack juridique 2024

Comme vous le savez sans doute, le Cabinet travaille depuis plusieurs années dans le cadre d'un pack juridique. Ce pack comporte des contrats, des documents d'exécution ou encore des éléments pour une mise en conformité au RGPD. Avant la fin de l'année 2024, ce pack sera complété des plusieurs contrats et documents portant exclusivement sur les prestataires de sécurité informatique.

Eric BARBRY

BNP PARIBAS
LEASING SOLUTIONS

Méthodes de travail et de consommation bouleversées par la transformation numérique : risques de cyberattaque amplifiés

La France est le pays européen qui a été le plus victime de cyberattaques, avec 727 incidents en 2023, suivie par l'Allemagne (463) et l'Italie (456) selon un rapport AV Test.

Des échéances réglementaires se profilent à très court terme :

• En octobre 2024, la directive **NIS 2**, une réglementation européenne qui vise à renforcer la cybersécurité des entités essentielles pour les services publics et privés ;

• En janvier 2025, le règlement européen **DORA** qui vise à renforcer la gestion des risques liés aux TIC et à la sécurité des réseaux et des systèmes d'information dans le secteur financier.

La cybersécurité est donc très logiquement devenue une préoccupation majeure de toutes les entreprises et se place ainsi au cœur du plan d'action stratégique de BNP Paribas Leasing Solutions sur le marché de l'IT.

Pleinement conscients de ces défis, nous nous engageons résolument à offrir des solutions de financement et de paiement adaptées aux besoins de nos partenaires et de leurs clients. Et pour encore mieux cerner les enjeux liés à la cybersécurité et les besoins de l'ensemble des acteurs de l'écosystème - éditeurs, distributeurs, revendeurs, prestataires de services et clients finaux - sur le financement de ce type de projets, nous avons fait le choix de rejoindre la Fédération Française de Cybersécurité.

Pour partager avec vous les objectifs de la Fédération mais aussi quelques conseils, nous sommes allés à la rencontre de **David Ofer, Président du Conseil d'Administration de la Fédération Française de Cybersécurité (FFCyber).**

• ***Monsieur Ofer, depuis quand la FFCyber existe-t-elle et quelles sont ses missions ?***

La Fédération était en projet depuis 2019 en raison de la crise sanitaire de 2020, elle a été officiellement créée sous mon impulsion en octobre 2020 pour répondre aux multiples besoins du tissu économique français sur ce sujet.

Son principal objectif est de communiquer le plus possible afin d'accompagner les entreprises pour qu'elles bénéficient d'un environnement législatif et réglementaire qui leur permettent de concourir efficacement à la cybersécurité de la nation.

Nous organisons des rencontres régulièrement, nous participons à des tables rondes, à des congrès. Nous menons des études, des actions médiatiques, des actions d'accompagnement et de communication aux cotés des institutions publiques.

• ***Qui peut adhérer ?***

Tout le monde peut adhérer : la fédération est ouverte aux écoles, aux centres de formation, aux sociétés de conseil, aux fonctionnaires, aux universitaires, ...

La diversité de ses adhérents contribue à sa richesse !

• ***D'après vous, quels sont les points majeurs d'un bon plan de cybersécurité ?***

Un bon plan part de le gouvernance des données au sens large, c'est le point de départ. Il faut être en mesure de décliner cette gouvernance vers les équipes, les applications, le réseau et le stockage.

Aussi, aujourd'hui, l'un des points importants est de former et sensibiliser les employés au sujet, ils doivent être le 1er rempart car 80 % des attaques sont du phishing.

La politique liée aux mots de passe doit être communiquée et respectée : mots de passe forts avec une identification multifactorielle en cas de besoin.

Cela va sans dire, mais disons-le quand même, il est indispensable de faire des sauvegardes des données régulières, gérer le plus rapidement possible les mises à jour et patchs des systèmes et des logiciels.

Les pare-feux sont aussi nécessaires couplés à des Endpoint Detection and Response qui eux sont en mesure de bloquer une attaque que l'antivirus aurait laissé passer.

Et bien sûr, il faut concevoir et faire vivre un plan de réponse aux incidents en cas d'attaque !

• ***Un dernier conseil ?***

Pour réussir son plan, je conseille de se faire accompagner par un spécialiste de la cybersécurité car les prestataires IT traditionnels ne sont pas forcément des experts du sujet.

• ***Un mot de conclusion ?***

On oublie souvent que le numérique est utilisé par l'homme pour lui faciliter la vie et non pas la lui compliquer !

Alors toute chose égale par ailleurs, nous tentons d'y contribuer.

Les contacts :

👉 Fédération Française de la Cybersécurité : contact@ffcybersecurite.org

👉 BNP Paribas Leasing Solutions :
Mme Valérie TIEFENBRUNNER
valerie.tiefenbrunner@bnpparibas.com

RG system

Témoignage client

TELMO et la transition vers les services IT complets avec RG System

Fondée en 1963, TELMO a évolué de téléphoniste à spécialiste des réseaux d'entreprise, de l'informatique (poste de travail et serveur), et opérateur (DATA et voix). L'entreprise intervient dans les secteurs des réseaux, télécommunication, informatique, sécurité, opérateur et câblage courant faible. Aujourd'hui, TELMO compte 40 employés répartis sur trois sites à Marly (57), Verdun (55), et Troyes (10). Sa mission est de connecter, innover, et protéger ses clients.

• ***Comment avez-vous découvert RG System ?***

Nous cherchions à nous diversifier et avions entendu parler de la solution N-able et avons commencé à réfléchir à ce sujet. Au salon IT Partner, nous avons rencontré RG System et eu un échange sur ce thème. Par la suite, nous avons découvert que le couplage de notre ERP (Artis) avec RG System était très puissant. Après des présentations de la solution en visio ainsi qu'une période d'essai, nous avons été convaincus de la pertinence de RG System.

• ***Quelles ont été vos premières impressions sur RG System et ses solutions ?***

RG System nous a semblé complet, incrémental, et intégrable. C'était une solution capable de nous faire progresser dans la supervision de nos équipements, notamment les serveurs, et d'apporter de la visibilité et de la réactivité pour l'accompagnement de nos clients avec un contrat d'infogérance.

Évolution vers une offre de services IT

• ***Pourquoi avez-vous décidé d'évoluer vers une offre de services IT ?***

Nous avons réalisé que nos clients avaient besoin d'une offre plus complète. Avant de proposer une supervision informatique complète, nous avons d'abord supervisé les serveurs de téléphonie chez nos clients pour monter en compétence sur le produit RG System.

• ***Quels ont été les facteurs déclenchants ?***

L'évolution du marché, la demande croissante des clients, et la compétitivité nous ont poussés à diversifier nos revenus et à augmenter notre compétitivité.

Identification des besoins

• ***Quels étaient vos besoins spécifiques avant de choisir RG System ?***

Nous avions besoin de remontées d'indicateurs, d'une solution intuitive et évolutive, capable d'orienter rapidement les diagnostics et de simplifier les questions à poser aux clients.

Expérience après un an d'utilisation

• ***Quels sont vos retours après un an d'expérience avec RG System ? Avez-vous constaté des bénéfices ?***

L'usage de RG System nous a permis d'améliorer notre rapidité et notre diagnostic grâce à des indicateurs précis. Assist a uniformisé notre solution de connexion à distance, et l'agent RG a simplifié le diagnostic, apportant gain de temps et pertinence.

Nous avons gagné en autonomie, simplicité, et avons observé une satisfaction générale parmi nos techniciens, chacun trouvant de la valeur dans la solution RG System.

Conseils pour d'autres entreprises

• ***Quels conseils donneriez-vous à d'autres entreprises souhaitant faire la transition vers un service IT ?***

Il est crucial d'adopter une montée progressive en testant le produit sur des environnements existants avant de proposer de nouvelles offres. Cela permet de rajouter de la valeur aux contrats existants et d'évaluer l'efficacité et la rentabilité de la solution.

Pour conclure

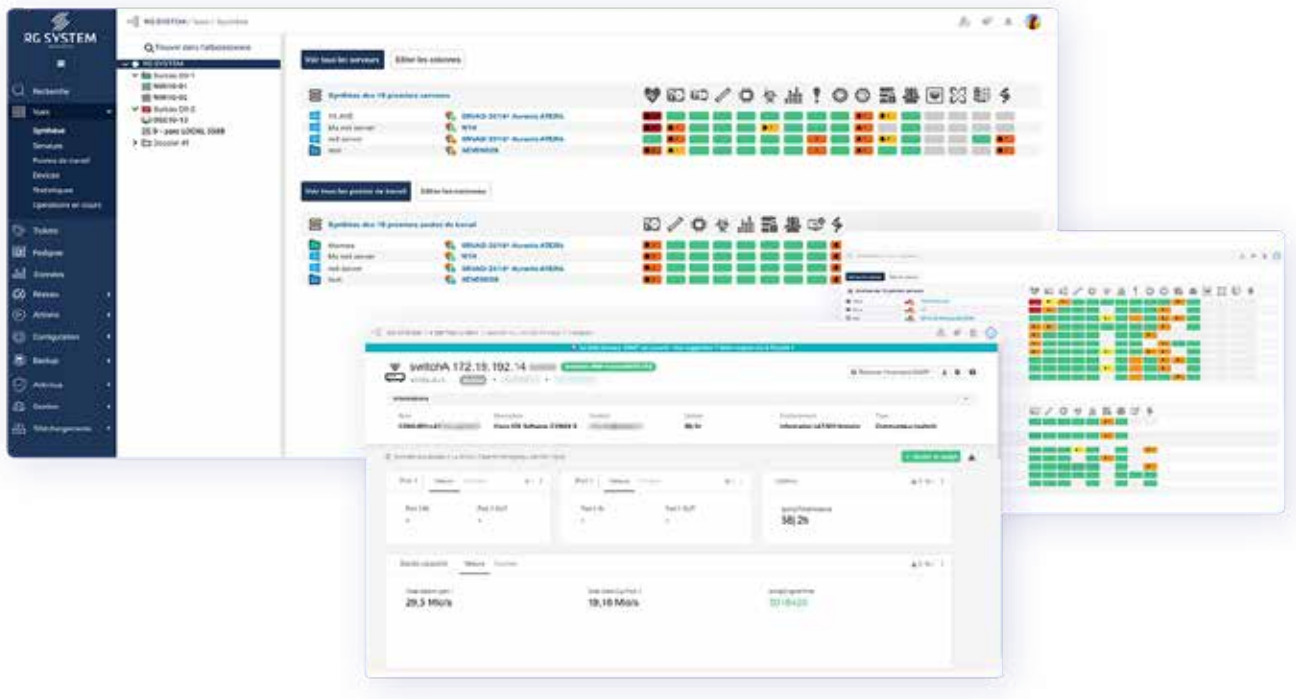
• ***Comment décririez-vous votre expérience globale avec RG System ?***

Globalement, nous sommes très satisfaits. RG System a uniformisé et simplifié notre approche client, nous faisant gagner du temps et augmentant notre efficacité. La perspective d'avenir inclut l'approfondissement du produit, la gestion des alertes, et l'intégration avec notre ERP pour la création automatique de tickets.

• ***La plus-value pour les clients ?***

Travailler avec des entreprises locales comme RG System renforce la sécurité et la protection des données, tout en soutenant l'économie locale et européenne, plutôt que d'enrichir systématiquement les GAFAM.

Le témoignage de Timothée ADAM de TELMO illustre comment la transition vers des services IT complets avec RG System peut non seulement répondre aux besoins évolutifs des clients, mais aussi renforcer la compétitivité et l'efficacité des intégrateurs.



Telmo
Intégrateur de solutions IT

OCIRP

Engagés
*pour l'**autonomie** !*

L'OCIRP, assureur paritaire à vocation sociale, innove depuis près de 60 ans en collaborant avec ses institutions de prévoyance membres pour protéger le salarié et sa famille en les aidant à faire face aux conséquences d'un décès ou de la perte d'autonomie.
Plus de six millions d'assurés couverts par les garanties OCIRP bénéficient de cette protection face à ces risques lourds. Négociées au sein des entreprises ou des branches professionnelles, elles garantissent le versement d'une rente ou d'une aide financière ponctuelle, ainsi qu'un accompagnement social personnalisé.

Agenda

WEBINAIRES

JEUDI
17
OCT

Présentation du programme IA Booster France 2030

Animé par Bpifrance.

JEUDI
07
NOV

Intelligence Artificielle : cas d'usages et opportunités pour gagner en performance

Animé par Cross Data.

RENDEZ-VOUS

MARDI
02
OCT

Lancement du Cybermoi/s 2024

Le **Mois européen de la cybersécurité**, créé en 2012, vise à **promouvoir le sujet de la cybersécurité** à travers les pays de l'UE pour permettre de **mieux comprendre les menaces et les appréhender**.

En France, il est décliné en « **Cybermoi/s** ».

Tout au long du mois d'octobre 2024, **des activités sont organisées en France et en Europe autour des enjeux de cybersécurité**.

EBEN vous représente

Prochains rendez-vous :

08 octobre	**Commission IT/Télécoms**
10 octobre	**Comité directeur Ufipa**
22 octobre	**CPPNI**
24 octobre	**CPNEFP**
24 octobre	**Commission sociale**

Lexmark

Les NOUVELLES A3 séries 9. Conçues pour durer.

POLYVALENCE

Prise en charge d'un **grand nombre de formats supports** (A6 à SRA3) en haut volume, un ensemble d'options modulaires de gestion du papier, des capacités de finition et des couleurs professionnelles y compris l'étalonnage Pantone®.

SIMPLICITÉ d'utilisation et de maintenance

Une **interface intuitive** grâce à des instructions et messages simples. L'entretien est simplifié grâce à des cartouches pouvant être remplacées d'une seule main, des repères visuels et une **facilité d'intervention**.

DURABILITÉ*

Les séries 9 sont **fabriquées pour durer 7 ans** ou plus. Le **PCR** : Post-Consumer Recycled* contenu représente 56% du poids pour les multifonctions et 73% pour les imprimantes. Le nombre réduit de composants diminue la probabilité de défaillance technique et minimise le temps de service nécessaire aux réparations et à l'entretien.

**Teneur en PCR mesurée conformément à la norme IEEE Std 1680.2a™ - 2017 Standard for Environmental Assessment of Imaging Equipment - Amendment 1 - norme utilisée par EPEAT. L'ensemble de la gamme a reçu la certification ENERGY STAR®. PCR signifie Post-Consumer Recycled, c'est-à-dire les matériaux recyclés post-consommation. Pour plus d'information, rendez-vous sur lexmark.com/sustainability.*