De la gestion des infrastructures informatiques à la gestion des situations de crise

Le Groupe MDSI accompagne les entreprises depuis 15 dans la gestion, l'exploitation et l'évolution de leur système d'information, tout en garantissant la sécurité des données. Pour de nombreuses structures, la gestion d'un système d'information représente une contrainte, une mission chronophage et couteuse qui éloigne les gestionnaires de leur cœur de métier. Le Groupe MDSI propose des services sur mesure, adaptées aux besoins spécifiques de chaque entreprise et intervient en cas de cyber attaque. Marc Henri Ravaux, Directeur Général du groupe MDSI et son équipe nous expliquent ces enjeux primordiaux.

Une expertise globale en gestion des Systèmes d'Information (SI)

Spécialisé dans l'accompagnement des entreprises, MDSI assure le maintien en condition opérationnelle et l'amélioration continue des environnements des SI. Le groupe **MDSI** intervient sur l'ensemble des infrastructures serveurs et applicatives, en assurant les mises à jour, la surveillance et la supervision des systèmes. Son objectif est de garantir que les services fournis aux clients restent pleinement fonctionnels et performants. **MDSI** développe également des solutions innovantes pour le maintien en condition de sécurité *(MCS)*, avec un fort accent sur la prévention et la mise à disposition des meilleures pratiques en matière de sécurité. Le maintien en condition opérationnelle *(MCO)* est également au cœur de ses activités, permettant aux entreprises d'optimiser la gestion et la pérennité de leurs infrastructures informatiques. Le groupe est présent à La Réunion, à Mayotte, aux Antilles et en Guyane.

Eric FLEURIE

La proactivité de **MDSI**, alliée à une analyse rigoureuse des dangers et de l'actualité, fait toute la différence pour un chef d'entreprise soucieux de sécuriser son entreprise et ses données informatiques. Grâce à sa fiabilité et à ses ressources, notamment avec un pôle sécurité et un pôle projet dédiés, **MDSI** se positionne comme un partenaire incontournable dans le domaine informatique. Sa passion pour l'innovation et son engagement dans la recherche et le développement permettent d'anticiper les évolutions futures du secteur, offrant ainsi aux entreprises des solutions adaptées et avant-gardistes pour naviguer dans un paysage technologique en constante mutation.

MDSI interviendra au **congrès des DAF**, organisé par le cabinet d'expertise comptable et d'audit **HDM, le 3 octobre 2024**, sur le thème de ***«La cybersécurité : réglementations, détection et prévention des menaces»***. Dans ce cadre, **MDSI** mettra en avant l'importance du maintien en condition de sécurité *(MCS)* en insistant sur la défense proactive contre les menaces internes et externes. De nos jours, aucune entreprise n'est à l'abri des cybermenaces, nous le constatons avec les attaques récentes, comme celles qui ont ciblé des entreprises à La Réunion, illustrent la gravité de la situation. Ces cyberattaques peuvent non seulement compromettre la confidentialité des données, mais aussi perturber gravement les activités des entreprises.

Les entreprises victimes subissent des pertes de chiffre d'affaires considérables, souvent accompagnées d'interruptions d'exploitation. Ces interruptions peuvent engendrer des coûts indirects, tels que la perte de confiance des clients et des partenaires, aggravant encore la situation.

Face à ce contexte préoccupant, MDSI s'engage à fournir des solutions adaptées et innovantes pour contrer ces menaces. En développant des stratégies de cybersécurité robustes et personnalisées, MDSI vise à protéger non seulement les données sensibles des entreprises, mais aussi à assurer leur pérennité dans un paysage cybernétique en constante évolution. Cela inclut des formations pour sensibiliser les utilisateurs, des outils de détection des menaces et des protocoles de réponse aux incidents, permettant ainsi aux entreprises de renforcer leur résilience face aux cyberattaques.

Un danger d'autant plus risqué pour les petites entreprises

Les petites entreprises, souvent dépourvues de services informatiques spécialisés, sont particulièrement exposées aux risques cybernétiques. Ne disposant pas toujours de ressources suffisantes ou d'un partenaire compétent pour se concentrer sur la cybersécurité, elles recherchent avant tout à réduire leurs coûts. Cette approche peut toutefois les fragiliser face aux cyberattaques. Sans accompagnement spécialisé, la sécurisation des systèmes informatiques devient un défi, mettant en péril la pérennité des petites structures.

Le danger auquel font face les entreprises à La Réunion est similaire à celui rencontré ailleurs, et aujourd'hui, une véritable prise de conscience émerge concernant la cybersécurité, bien que la démarche ne soit pas encore totalement aboutie. Une société qui reconnaît ces dangers peut significativement diminuer sa vulnérabilité. La protection des sauvegardes se révèle cruciale : préserver les données informatiques est essentiel, car une faille dans ce domaine peut avoir des conséquences catastrophiques, allant jusqu'à mettre en péril la pérennité de l'entreprise. Il est donc impératif d'adopter des mesures proactives pour assurer la sécurité des informations et des opérations.

Erwan PERRIN

Vigilance et protections sont les meilleurs outils

Dans un monde où une très grande partie des attaques informatiques proviennent des e-mails, la sensibilisation aux dangers est plus cruciale que jamais. L'intelligence artificielle amplifie ces risques en rendant les menaces plus sophistiquées et difficiles à détecter. Face à cette réalité, il est impératif d'adopter une approche plus rigoureuse en matière de sécurité. Chaque collaborateur doit être conscient des techniques de ***« phishing »*** et des signaux d'alerte, car une simple erreur peut avoir des conséquences désastreuses. En renforçant notre vigilance, nous pouvons mieux protéger nos données et notre infrastructure contre ces attaques de plus en plus fréquentes.

L'État met en place un ensemble de mesures pour renforcer la protection des entreprises contre les cyberattaques, en réponse à l'augmentation des menaces numériques. Parmi ces mesures, le Règlement Général sur la Protection des Données ***(RGPD)*** joue un rôle central en fixant des normes rigoureuses pour la gestion et la protection des données personnelles en Europe. Parallèlement, la **directive NIS2** vise à renforcer la cybersécurité des activités critiques, imposant des exigences accrues de sécurité aux collectivités, moyenne et grandes entreprises, ainsi qu'aux fournisseurs de services numériques. Cette directive précise que toutes les entreprises non conformes pourront être sanctionnées, ce qui souligne l'importance d'une démarche proactive de conformité.

A l'approche de 2025, avec les nouvelles réglementations européennes **DORA et NIS2**, les entreprises devront intégrer une stratégie cyber. Ces réglementations encouragent non seulement une vigilance accrue en matière de cybersécurité, mais aussi la mise en place de plans de réponse aux incidents. L'État propose également des aides financières pour soutenir les entreprises dans la réalisation d'audits de sécurité, afin d'évaluer et d'améliorer leurs systèmes de protection. En consolidant ces initiatives, l'État s'efforce de créer un environnement numérique plus sécurisé, garantissant ainsi la continuité des activités et la confiance des consommateurs dans l'économie numérique.

Informations et inscription : **congresdesdaf.re**