MAATEL

29/04/2025

N°5

MAATEL actu

INNOVATION ET PERFORMANCE ELECTRONIQUE

Le bulletin d'information de MAATEL

La cybersécurité au service de nos clients

Votre moment Interview avec...

Dominique RAMBAUD
Responsable Informatique chez MAATEL

À l'ère du numérique, la sécurité informatique est un enjeu crucial pour toutes les entreprises. Aujourd'hui, nos projets sont numériques, nos données sont connectées, et nos clients sont exigeants et cela à juste titre.

Alors comment une PME innovante comme MAATEL peut-elle garantir un haut niveau de sécurité face à des cybermenaces de plus en plus complexes ?

Pour le savoir, nous avons échangé avec Dominique RAMBAUD, Responsable Informatique, qui pilote la cybersécurité de MAATEL avec rigueur... et passion, depuis 18 ans.

Voir plus

Pourquoi la cybersécurité est-elle un enjeu central pour MAATEL ?

La cybersécurité est au cœur de notre activité, car notre métier repose avant tout sur la confiance. Chez MAATEL, nous concevons des dispositifs électroniques sur mesure, souvent pour des secteurs sensibles comme le médical ou l'industrie.

Protéger les données de nos clients, garantir la continuité de nos services et prévenir toute faille de sécurité sont des exigences indispensables. Une attaque, même minime, peut compromettre la confidentialité des informations et impacter notre fonctionnement.

La cybersécurité n'est donc pas un simple sujet d'actualité pour nous : c'est une démarche intégrée à notre quotidien, structurée, partagée et portée à tous les niveaux de l'entreprise.

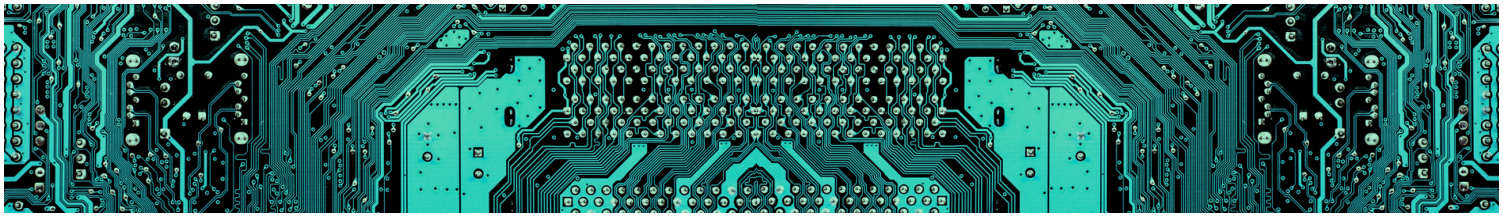
Quelle est votre approche globale en matière de sécurité informatique ?

Nous avons mis en place une stratégie de cybersécurité proactive, structurée et durable, reposant sur trois piliers essentiels : la technologie, l'organisation et l'humain.
Cette démarche s'appuie sur des solutions techniques avancées, une organisation rigoureuse et une implication forte des collaborateurs, afin de garantir une sécurité globale, cohérente et partagée.

Notre approche est alignée avec les référentiels de l'État, notamment ceux de l'ANSSI (Agence nationale de la sécurité des systèmes d'information) et du CERT-FR (Centre gouvernemental de veille, d'alerte et de réponse aux attaques informatiques).

Elle est également pensée pour anticiper les évolutions réglementaires, comme l'arrivée prochaine de la directive européenne NIS2 (Network & Information Security).

Toutes les décisions sont prises en concertation avec les différents métiers, avec le soutien actif de la direction, afin de garantir une vision cohérente et de long terme.



Quelles mesures concrètes avez-vous mises en place ?

Voici les principales :

Formation continue :

Tous les collaborateurs reçoivent des formations régulières sur les bonnes pratiques en cybersécurité.

Campagnes de phishing :

Nous testons régulièrement la vigilance de nos équipes avec des scénarios réalistes, suivis de débriefings pédagogiques.

Protection des serveurs critiques :

Pare-feu, segmentation réseau, accès restreints et supervision en temps réel.

Politique stricte de mots de passe :

Mots de passe complexes, changement régulier, et authentification à deux facteurs.

Mises à jour centralisées :

Cela nous permet de corriger rapidement les failles dès qu'elles sont connues.

Sauvegardes multisupports :

Données sauvegardées sur site et hors site, en ligne et hors ligne.

Solution EDR (Endpoint Detection and Response) :

Pour surveiller le comportement des postes et détecter les anomalies.

Partenariat avec notre cyberassureur :

Il nous accompagne pour auditer notre dispositif et l'améliorer en continu.

Et pour les collaborateurs en télétravail ?

On a bien évidemment mis en place des accès via VPN sécurisé, avec des contrôles stricts. Depuis la crise sanitaire, le télétravail s'est largement développé et a modifié les usages numériques au sein des entreprises. Evidemment, le télétravail change les usages, donc il faut accompagner, expliquer, prévenir. On préfère une personne qui nous appelle trois fois pour être sûre qu'un lien est fiable, plutôt que de prendre le risque d'un clic douteux.

Vous collaborez également avec un cyberassureur. En quoi cela vous aide-t-il ?

C'est une vraie plus-value. Il ne s'agit pas seulement de se "couvrir" en cas de problème. Notre cyberassureur agit comme un partenaire de confiance : il nous aide à évaluer notre niveau de maturité, à identifier les points faibles, à rester alignés avec les meilleures pratiques du marché.

Grâce à lui, on réalise des audits réguliers et on bénéficie d'un accompagnement pour mieux répondre aux exigences futures, comme celles de la directive européenne NIS2* qui va bientôt s'appliquer à davantage d'acteurs industriels.

Comment garantissez-vous l'efficacité et l'actualisation de ce dispositif ?

La cybersécurité est un processus vivant. Nous effectuons des audits réguliers, internes ou accompagnés de notre cyberassureur, et nous nous tenons informés des nouvelles menaces. Notre objectif est clair : **"anticiper plutôt que subir"**. Cette rigueur nous permet de garantir un haut niveau de sécurité à nos clients.

Et pour conclure, un dernier message à faire passer ?

Je dirais simplement que la cybersécurité est l'affaire de tous. Ce n'est pas seulement une question de logiciels ou de protocoles : c'est avant tout une culture partagée, une vigilance collective.

Chez MAATEL, chacun a un rôle à jouer que ce soit en repérant un mail suspect, en appliquant une mise à jour ou en respectant les consignes internes.
Notre objectif, c'est la confiance dans un environnement sécurisé, à la hauteur des projets que nous construisons avec nos clients.

Et c'est grâce à cet engagement commun que nous pouvons avancer sereinement, ensemble.

commercial@maatel.fr
+ 33 (0) 4 76 07 39 50
259 rue du Rocher de Lorzier 38430 MOIRANS