GROUPE BLOCHON MARTIN (60)

INTERNALISER LA DSI POUR MAÎTRISER LA CYBERSÉCURITÉ

Outre une politique de sauvegardes composites des données, le groupe Blochon Martin (60) s'appuie sur des solutions d'antivirus, d'antispam et de filtrage de contenus Web. Quant à la sensibilisation des salariés aux cybermenaces, elle s'effectue au fil de l'eau.

Internaliser le service informatique a des chances de faciliter la cybersécurité autant que la cyberprévention. En témoigne Aurélien Laurent, directeur des systèmes d'information du groupe Blochon Martin, basé à Caen (14), qui réalise un chiffre d'affaires de 38 millions d'euros en 2019, emploie 400 salariés dans six agences en France et possède un parc de 335 moteurs (bennes, plateaux-grues, tautliners…). « *Ce choix s'est opéré en 2003* », explique Aurélien Laurent, qui compte, dans son équipe, deux développeurs et un responsable de l'informatique embarquée.

PHOTOS : BLOCHON MARTIN

Aurélien Laurent (groupe Blochon Martin) : « Les ateliers cyber sont intégrés aux processus de formation de l'entreprise. »

Depuis 2003, le groupe Blochon Martin a décidé d'avoir son propre service informatique. Un atout pour la cyberprotection et la cyberprévention.

Même philosophie pour la cybersécurité où domine une bonne dose de pragmatisme : les antivirus régulièrement à jour ainsi que l'antispam MailInBlack protège la messagerie électronique des e-mails provenant de personnes non identifiées. Quant à la solution de sécurité Web et de filtrage de contenus d'Olfeo, elle contraint les utilisateurs à ne surfer que sur des sites catégorisés et à usage professionnel. Ainsi, les utilisateurs évitent-ils de se retrouver par accident sur des sites exotiques potentiellement porteurs d'attaques par rançongiciel. « *Si un utilisateur nous avertit que, suite à un e-mail externe, il ne peut se rendre sur le site de la banque, nous lui montrons qu'il s'agit en fait d'un site pirate qui lui ressemble beaucoup !* » décrypte Aurélien Laurent. À ces protections, s'ajoute une combinaison de sauvegardes complètes tous les jours, de sauvegardes instantanées (sous forme de cliché) toutes les heures et de sauvegardes inaltérables de tous les serveurs : les données seront ainsi stockées pendant trente jours sans pouvoir les modifier. « *En cas d'attaque cryptographique, nous limitons considérablement les dégâts* », ajoute Aurélien Laurent.

En matière de cyberprévention, tous les courriers électroniques provenant de l'extérieur comportent le message suivant sur fond jaune : « MAIL EXTERNE : Soyez prudent lorsque vous ouvrez des liens ou des pièces jointes. En cas de doute, appelez le service informatique. » Régulièrement, le DSI envoie des notes d'information aux collaborateurs pour les avertir de nouvelles menaces. « *Cet été, une vague importante d'hameçonnage imitait les mails provenant de banques* », se souvient Aurélien Laurent qui n'a pas hésité à téléphoner aux services concernés pour rappeler les bonnes pratiques. Pas besoin de mobiliser tous les salariés le même jour pour les former à la cyberprévention car les ateliers cyber sont intégrés aux processus de formation de l'entreprise. Par exemple : « *Dès l'embauche, lorsque l'on forme les salariés aux outils métiers de l'entreprise, nous réservons toujours un moment pour leur apprendre les bonnes pratiques de cyberprévention* », reprend le DSI.

Quant à l'informatique embarquée, elle est en train de migrer vers des Smartphones. Lettre de voiture électronique, photos de bons de livraison, tickets de pesée… le groupe Blochon Martin a décidé d'instaurer une gestion professionnelle des Smartphones dotés des seules applications autorisées. Par exemple, Tiny MDM retire, pour renforcer la sécurité routière, les fonctionnalités tactiles pendant que le conducteur roule. Et, à l'instar d'Olfeo, le conducteur n'accède qu'aux applications et aux sites autorisés. Résultat, le dernier incident de cybersécurité a eu lieu il y a six ans.

ERICK HAEHNSEN/AGENCE TCA