Cybersécurité : secteur privé ou public, tous concernés

L'Activité Eau Région Méditerranée de Veolia a lancé, depuis deux ans, une série de Matinales sur les thématiques du climat, de la transition énergétique et de la relance verte. Et parce que les services d'eau sont des cibles de cyberattaques, le dernier rendez-vous, organisé en partenariat avec l'Association des maires du Var, a réuni des acteurs de la cybersécurité pour une table ronde passionnante au RCT Campus de Toulon.

De gauche à droite : Denis Carreaux, directeur des rédactions du Groupe Nice-Matin ; Christophe Kleinklaus, directeur du territoire Veolia Var Provence Méditerranée ; Nidhal Bel Aloui, chef d'escadron de réserve Groupement de Gendarmerie du Var ; Jérôme POGGI, responsable de la sécurité des systèmes d'information de la Ville de Marseille ; Jean Larroumets, fondateur et président-directeur général d'Egerie Software ; Olivier Cavallo, délégué régional Veolia ; Jean-Pierre Véran, maire de Cotignac et président de l'Association des maires du Var ; Matthieu Bertin, responsable de la sécurité des systèmes d'information Veolia Eau. (Photos C. B.)

« *Ce sont des moments qu'on n'oublie jamais* », avoue Jérôme Poggi, responsable de la sécurité des systèmes d'information de la Ville de Marseille. Le 14 mars 2020, 7 h 31, l'attaque du système et 10 h 37, l'envoi du message "Compromission confirmé". « *C'était le week-end des élections municipales juste avant l'annonce du confinement pour le Covid. Autant dire un moment à part...* » Sa direction estime un retour à la normale en 3 semaines. « *Au bout de 3 mois, on a commencé à redémarrer le système d'information (SI), on était à 80 % au bout de 6 mois et 90 % après un an.* » Jérôme Poggi raconte les semaines où les services ont dû retourner au papier, les situations humaines compliquées dans un contexte difficile, l'impact psychologique sur les agents... « *Il faut un incident pour que les gens se réveillent. Aujourd'hui, tout va bien, on observe notre SI pour identifier des indicateurs de compromission. On a davantage de personnel et une surveillance H24. On sensibilise aussi nos agents car ils sont la porte d'entrée de l'attaque* (via les mails de phishing) *mais ils sont surtout la première barrière.* »

« *Il vaut mieux avoir "un peu de cyber" dans chacun des agents qu'embaucher un expert,* abonde Jean Larroumets, p.-d.g. fondateur d'Egerie Software. *C'est l'agent de l'état civil qui est responsable de la sécurité du système de l'état civil. Chaque métier est concerné directement par la cyberdéfense.* »

Partager les pratiques

Son entreprise toulonnaise, créée en 2016, propose de simuler une attaque et de modéliser les risques. « *Un euro dépensé en amont équivaut à 300 euros après un incident. Il vaut mieux donc anticiper que subir. La cybercriminalité est ce qu'il y a de plus rentable : elle représente 6 000 milliards de dollars actuellement. Alors oui, les systèmes innovent et il faut s'adapter, les hackers partagent leurs pratiques sur le dark web. Mais l'avantage, c'est que les systèmes des collectivités se ressemblent, vous pouvez donc, vous aussi, partager vos bonnes pratiques de protection.* »

Les collectivités peuvent aussi profiter de la cyber expérience de la Gendarmerie. « *Depuis deux ans, notre service engage des actions en amont des attaques et plus seulement après,* explique Philippe Faucon, référent cyber menaces de la Gendarmerie du Var. *Mais il y a une résistance au changement... Alors que notre service est gratuit et permet de commencer à se protéger rapidement, nous n'avons obtenu un rendez-vous qu'avec douze collectivités sur les 140 communes varoises.* »

> **"La question n'est pas de savoir *si* vous subirez une cyberattaque mais *quand*..."**
> **Mathieu Bertin, responsable de la sécurité des systèmes d'information Veolia Eau**

4 piliers essentiels

La cyberdéfense est composée de quatre piliers, résume Matthieu Bertin, responsable de la sécurité des systèmes d'information Veolia Eau : « *La sensibilisation des collaborateurs ; la protection et la sécurisation des systèmes ; la détection grâce à des outils de surveillances performants ; et la préparation en ayant des sauvegardes sur un autre système.* » Vous pouvez aussi mener des tests d'intrusion ou essayer un programme de *bug bounty* où vous ouvrez votre système d'information à des hackers éthiques qui doivent trouver une faille car ils sont payés au résultat...

« *Comme on ne peut pas attaquer des hackers car c'est interdit...* sourit Nidhal Bel Aloui, chef d'escadron de réserve du groupement de Gendarmerie du Var, *l'état que l'on recherche est celui de la résilience. Les nouvelles technologies vont continuer d'évoluer avec leurs lots de vulnérabilités et il faudra s'adapter ou disparaître.* »

Heureusement, de nombreuses solutions de cyberdéfense existent, il faut juste une prise de conscience pour débloquer des budgets essentiels.

LOUISE TEMPIER
ltempier@nicematin

La Région Sud parée à la cyberattaque

« *Il y a un mois, les établissements scolaires étaient ciblés,* rappelle Denis Carreaux, directeur des rédactions du Groupe Nice-Matin et animateur de cette table ronde. *La semaine dernière, c'était l'hôpital de Cannes...* » Force est de constater que les cyberattaques sont entrées dans notre quotidien. François de Canson, vice-président de la Région Sud en charge de la cybersécurité, détaille l'épisode rencontré par les collèges et lycées : « *Les hackers ont pénétré le système Atrium, d'où ils ont envoyé 15 000 messages de menaces terroristes. On a alerté Orange Cyberdefense et il n'y avait pas eu de failles de la sécurité. Ce canular malsain nous a permis d'analyser la réactivité du système.* »

Soit un bilan positif important car la Région Sud est particulièrement exposée aux cyberattaques.

« *Il y a un contexte mondial particulier avec 70 élections cette année dont la présidentielle américaine et les Européennes, les Jeux à Paris et toujours la guerre en Ukraine,* détaille François de Canson. *Notre région est très exposée car c'est une terre de défense militaire, de tourisme, d'événements internationaux, d'industries et de nouvelles technologies (Marseille est le 5e hub mondial du trafic Internet). Nous sommes le 2e territoire français qui génère le plus de chiffres en termes de cybersécurité avec 3,3 milliards. Tout ceci fait de nous une cible privilégiée. Nous devons donc nous préparer.* » D'où la création d'Urgences Cyber Région Sud à Toulon [1], service gratuit d'accompagnement, dalerte et de réponse à un cyber incident.

1. Site : urgencecyber-regionsud.fr -- 0.805.036.083.

François de Canson, vice-président de la Région Sud en charge de la cybersécurité.

EN BREF

1 Français sur 2 a vu ses données personnelles compromises en 2023 (notamment via les attaques de France Travail et de deux opérateurs de tiers payant).

+35 % de plaintes enregistrées pour cyberattaques en 2023.

La France est le **2e pays d'Europe** le plus touché derrière les Pays-Bas.

+400 % d'actes de cybercriminalité entre 2020 et 2023 en France.

53 % des entreprises françaises ont signalé une cyberattaque en 2023. Des attaques multipliées par deux sur les PME (36 %). Le coût financier moyen pour une PME se situe entre 300k et 500k euros.

Une atteinte à la cybersécurité se produit **toutes les 39 secondes**. Dans 90 % des cas, les cyberattaques commencent par l'ouverture d'un mail frauduleux.

Sources : ANSSI, Cnil, Hiscox 2023.