Violences intrafamiliales
Crampons, scie et menaces
page 5

Ramassage des déchets
Fin de la grève à la SPL Sudec
page 6

Le Quotidien
DE LA RÉUNION ET DE L'OCÉAN INDIEN

www.lequotidien.re

Mardi 29 juillet 2025 - N° 16220 - 49e année - Prix : 1,20 €

www.lequotidien.re

CYBER MENACES

Même plus peur !

Alors que les grands groupes se sont prémunis contre les attaques numériques, les petites structures étaient les grandes oubliées de la cybersécurité. Ce n'est désormais plus le cas.

pages 2-3

Vos pages vacances

Mes JO, un an après.
Richardson a tout changé
Documentaire.
Les femmes debout !
+ 2 pages jeux

pages 12 à 15

Politique
Naillet s'attaque à Bayrou
page 6

Jazz dann Port
Le succès au rendez-vous
page 9

CYBERSÉCURITÉ : POUR LES TPE, PME, ASSOCIATIONS, COLLECTIVITÉS...

Protéger aussi les petits

Avant un exercice national en septembre, la préfecture de La Réunion sensibilise les petites structures aux cybermenaces, qui mettent à mal l'économie et la cohésion du territoire.

Il y a les attaques très médiatiques, celles sur le groupe automobile Leal et sur le centre hospitalier universitaire nord de Saint-Denis en 2023, celles sur le groupe Cirano (Antenne Réunion) et le Conseil départemental en 2024, et puis il y a toutes celles qui visent de petites entités. Elles sont moins médiatisées. Pourtant, elles peuvent mettre à mal une entreprise, une association ou une collectivité, avec de graves conséquences.

Des petites structures qui sont, par définition, plus faciles à atteindre pour les hackers. Ce qui fait considérablement augmenter les statistiques à La Réunion : alors que 22 incidents ont été remontés à l'agence nationale de sécurité des systèmes d'information (ANSSI) en 2024, rien que pour les premier et deuxième trimestres 2025, on en compte 26. La courbe des incidents s'annonce donc exponentielle.

Faire un diagnostic

Et encore : il ne s'agit que des cyberattaques signalées à l'ANSSI. Les chiffres publiés sont en effet *«bien inférieurs au nombre réel de cyberattaques puisque de nombreuses entités n'ont pas connaissance de cyberattaques subies ou ne se signalent pas»*, indiquait le préfet de La Réunion il y a un an.

À propos des 26 cyberattaques aux premier et deuxième trimestres 2025, Denis Fabrègue, directeur de Réunion THD, ajoute : *«On est à peu près certain que les 26 responsables de structures qui se sont faits attaquer sont, de fait, sensibilisés aux risques cyber. Ils vont naturellement chercher à mieux se protéger, faire le diagnostic, mettre en place des mesures de protection. Ce qui est important pour notre tissu économique aujourd'hui, c'est de faire en sorte que ces chefs d'entreprise soient sensibilisés en amont avant l'attaque. Et c'est pour cela que c'est bien de faire la promotion de ce dispositif de diagnostic cyber pour qu'un maximum de chefs d'entreprise anticipe, intègre le risque cyber avant de se faire attaquer»*.

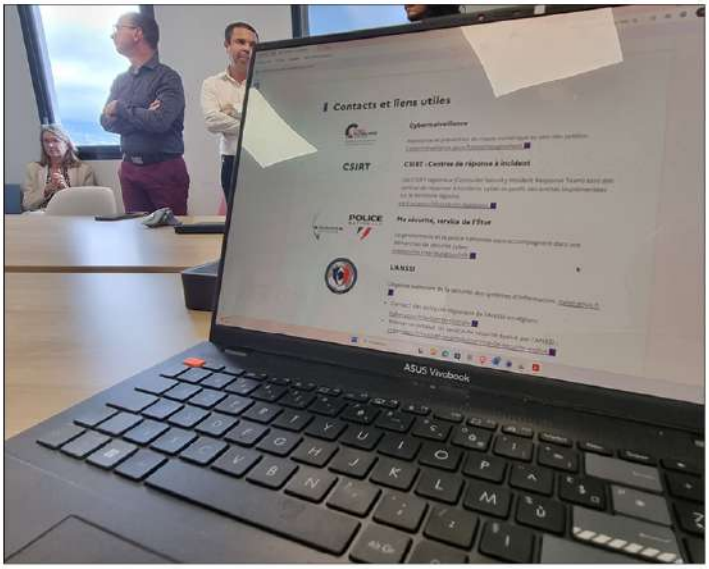
MonAideCyber, un outil gratuit

Le dispositif de diagnostic cyber que Denis Fabrègue évoque, c'est MonAideCyber, un outil gratuit pour renforcer la cyber sécurité des entreprises et des collectivités. Cet outil clé en main proposé par l'ANSSI, la communauté des «aidants cyber», réalise un diagnostic complet et gratuit, à travers des actions rapides à mettre en place, pour aider les entités souhaitant se protéger contre les cyberattaques.

«On est sur un référentiel national qui est incontestable. Par ailleurs, sous l'impulsion de la Région, on a répondu à un appel à projet avec un consortium local. Il s'agit d'un appel à projet EDIH (European digital innovation hubs network, N.D.L.R), *pôle d'innovation numérique européen en cybersécurité, et l'idée était d'apporter de la cohérence. Ce dispositif vise à accompagner les mêmes publics: TPE, PME, collectivités territoriales et associations»*, explique Matthieu Druilhe, directeur adjoint à la cybersécurité chez Réunion THD.

L'intérêt du projet EDIH, *«c'est de pouvoir subventionner la mise en œuvre des mesures de cybersécurité. Et donc, d'avoir un levier de financement commun à la Commission européenne et à la Région pour pouvoir accompagner les entreprises tant sur des mesures organisationnelles avec de la formation, de la sensibilisation, qu'avec des mesures techniques qui seront déployées par des entreprises réunionnaises»*.

Dans ce cadre, un appel à manifestation d'intérêt a été lancé et 42 entreprises réunionnaises offreuses de solutions de prestation en cybersécurité ont candidaté. *«On est en train de finir le dépouillement et on en a déjà notifié 34 sur ce sujet pour un démarrage opérationnel à venir»*.



MonAideCyber vise à protéger l'ensemble du tissu économique, en prenant en compte les petites structures. (Photo AG)

26

C'est le nombre d'incidents à La Réunion remontés à l'Agence nationale de sécurité des systèmes d'information (ANSSI) au cours des premier et deuxième trimestres 2025. C'est plus que toute l'année 2024 au cours de laquelle 22 incidents avaient été enregistrés.

Mesures «d'hygiène» quotidienne

Avant d'investir dans des outils qui ont prouvé leur efficacité en matière de cybersécurité, les petites structures doivent appliquer des mesures «d'hygiène» quotidiennes : mettre en place des sauvegardes, de la sensibilisation en direction des collaborateurs, des bonnes pratiques sur les mots de passe, ou encore avoir une vision globale de leurs systèmes d'information. Finalement, on protège bien que ce qu'on connaît bien.

«L'idée, c'est vraiment de prendre conscience des risques cyber pour les petites entreprises», reprend le directeur de cabinet du préfet, Vincent Bernard-Lafoucrière, *«parce que même si chaque petite entreprise n'est pas touchée tous les jours, quand elle est touchée, elle peut ne pas s'en relever et souvent c'est le cas»*.

Preuve que les petites structures sont aux avant-postes : depuis le début de l'année, il n'y a pas eu de grandes attaques sur des structures importantes. Pourtant, le nombre de cyberattaques est bien en augmentation par rapport aux années précédentes.

«Les grandes entreprises et les grandes collectivités, elles arrivent à être sensibilisées et à développer des moyens de protection», souligne le directeur de cabinet du préfet. *«Maintenant, on vise vraiment, avec un outil comme MonAideCyber, à protéger l'ensemble du tissu économique. Les TPE, les PME, les associations comme Agorah, elles n'ont pas l'infrastructure, les services informatiques. Tout le monde n'a pas ces ressources en interne. C'est la raison pour laquelle l'État, et notamment l'ANSSI, a développé ce produit, qui a vocation à être diffusé dans toutes les entreprises grâce à des aidants, des tiers de confiance tels que Cyber Réunion et la Chambre de commerce et d'industrie»*.

Antoine GESLIN

Déjà un exercice en 2024 pour les hôpitaux

En 2024, les services de santé et la préfecture ont testé leurs capacités à répondre à une attaque massive. (Photo ARS)

Un an après l'attaque contre le CHU Nord de La Réunion, l'Agence régionale de santé (ARS) de La Réunion et la préfecture ont piloté un exercice cyber en février 2024 avec les équipes des établissements de santé publics (CHU, Chor, EPSMR et GHER), en lien avec d'autres acteurs de santé. *«Face à la multiplication des attaques informatiques qui touche les hôpitaux publics, la réalisation d'exercices de gestion de crise est essentielle»*.

Tester, évaluer, renforcer

La preuve ? Une semaine avant avait eu lieu une nouvelle cyberattaque visant l'hôpital d'Armentières, avec comme conséquence la fermeture des urgences pendant 24 heures. À La Réunion en 2023, *«une détection précoce [avait] permis d'assurer la continuité des soins»*.

L'ARS indique que *«l'impact d'une cyberattaque peut avoir des conséquences allant au-delà des limites de la structure touchée : prises en charge des patients par les urgences, protection des usagers, acheminement des patients vers des établissements de repli, mobilisation des services de l'état et des professionnels de santé…»*

Les objectifs de cet exercice l'an dernier étaient donc de tester la capacité de réponse des différents acteurs à des cyberattaques de grande ampleur, de renforcer la coordination des différents acteurs, d'évaluer la coordination entre structures de soins et de tester la résilience du système de santé réunionnais. *«Cet exercice a permis d'identifier les forces et les points d'amélioration de l'organisation en gestion de crise. Il s'agit désormais de travailler conjointement à renforcer les actions»*, indique sobrement l'ARS.

Le nombre de cyberattaques à La Réunion augmente constamment. (Photo DR)

Rempar25 : au cœur d'une cellule de gestion de crise

«Vous êtes-vous déjà demandé ce qui se passerait si les fonctions clés de votre entreprise se retrouvaient en première ligne lors d'une cyberattaque ? Avec Rempar25, vous allez pouvoir le vivre… sans les dégâts !» Le 18 septembre prochain, pour la première fois en France, un exercice va être organisé sur tout le territoire national. *«Il va faire concourir des administrations publiques, l'Etat bien sûr, la préfecture de La Réunion y participera, mais aussi des entreprises, afin de s'entraîner pour être prêt à réagir le jour J»*, indique Charli Hoarau, chef de projet du centre de réponse aux incidents chez Cyber Réunion.

Plan Orsec cyber

«La Réunion au niveau outremer est l'un des départements qui est le plus représenté. On voit que le message de cybersécurité passe énormément. Le préfet a souhaité vraiment qu'on prenne part à cet exercice. On va jouer le rôle de centre opérationnel départemental, et aussi au niveau de l'annuaire national, ce qui fait que les autres sociétés qui vont jouer Rempar25 pourront nous solliciter en tant que préfecture et accompagnement», complète Cyriac Rouaud, le conseiller à la sécurité numérique de la préfecture.

Cet exercice Rempar25 se traduira *«comme une gestion de crise classique, avec une planification, une réflexion sur les risques, des procédures»*. À ce propos, afin que l'exercice soit le plus complet possible, il faut des participants: *«C'est un peu tout le monde qui est concerné par le sujet»*, souligne Charli Hoarau. Cyber Réunion, qui coordonne localement cet exercice immersif et collaboratif destiné aux TPE, PME et associations, invite donc les acteurs de la communication, du juridique, de la gestion et comptabilité et des ressources humaines, à se faire connaître pour y participer.

«C'est gratuit, réaliste et surtout très instructif. Rempar25 vous plonge dans une véritable cellule fictive de gestion de crise. Vous allez apprendre à prendre les bonnes décisions, à coopérer avec d'autres fonctions et à protéger la continuité de votre activité».

Pour s'inscrire, il faut envoyer sans tarder un courriel à rempar25@cyber-reunion.fr, en précisant ses nom, prénom, courriel, fonction, et organisation. Pour en savoir plus sur Cyber Réunion: cyber-reunion.fr.

Le centre opérationnel départemental ressemblera fortement à celui mis en place pendant les cyclones. (Photo AG)

Un pirate a tenté d'usurper le RIB de l'agence Agorah. (Photo AG)

L'agence de l'urbanisme Agorah ciblée par une attaque

«On a été victime d'une tentative d'attaque qui était ce genre d'attaque du quotidien, une tentative d'usurpation de mail pour essayer de remplacer le relevé d'identité bancaire de l'Agorah par un relevé d'identité bancaire d'une structure dont qu'on ne connaît pas le nom, mais qui semblait être affiliée à une banque en ligne quelque part».

Daniel David et Benoit Pribat, les co-directeurs de l'Agence d'urbanisme de La Réunion, confirment que *«ce genre d'attaque là, ce sont des attaques qui ne sont pas aussi médiatiques que les attaques d'ampleur qui ont pu toucher Cirano ou le Département, mais qui sont sûrement celles qui touchent le plus le tissu d'entreprises à La Réunion»*.

Intérêt financier et données sensibles

Si cette tentative contre l'Agorah n'avait pas échoué, *«s'il y a des milliers ou dizaines de milliers d'euros qui réussissent à être pris, ça nous met en danger clairement à très court terme»*.

Lors de cette tentative de piratage, l'Agorah était accompagnée de Cyber Réunion. *«C'est fondamental d'avoir quelqu'un vers qui se tourner quand on subit une tentative de piratage. Parce qu'on se sent un peu démuni et ça peut faire très peur pour les éléments financiers. D'avoir eu Cyber Réunion et MonAideCyber, ça nous a permis vraiment d'avoir des conseils très pratiques, des mesures à prendre de sécurisation, par exemple la double authentification des messageries, des choses simples finalement mais qui sont fondamentales pour bien se protéger contre les pirates»*.

Au-delà de l'aspect financier, l'Agorah manipule aussi des données sensibles. *«On fait office de portail de bancarisation de données pour toute la sphère partenariale réunionnaise. On stocke les données sur les prix des loyers, les transactions, les maisons, les terrains, les appartements, combien ça se vend, où est le foncier disponible. Tout cela, on le stocke ici»*. Or, toutes ces données peuvent présenter un vrai intérêt pour plus d'un acteur malveillant.