LUTTE CONTRE LE CHIKUNGUNYA P.4

Le préfet annonce 400 nouveaux contrats PEC

Le Quotidien
DE LA RÉUNION ET DE L'OCÉAN INDIEN
www.lequotidien.re
Mercredi 16 avril 2025 - N° 16132 - 49e année - Prix : 1,20 €

FREEDO Quotidien
1 000 €
À GAGNER AUJOURD'HUI

CYBERMENACES À LA RÉUNION

Même pas peur !

Dans son rapport sur l'état de la menace cyber dans l'océan Indien, Cyber Réunion fait un état des lieux et dresse des perspectives qui pourraient être positives pour le développement de La Réunion.

P.2-3

CAPITAL DE LA SAPMER P.6
Deux recours contre la prise de participation de la Région

SPL ESTIVAL P.7
Le quorum fait causer

ÉCONOMIE P.8
L'inquiétude de la CPME

AU COLLÈGE P.10
La pause numérique, testée, pas encore adoptée

TAEKWONDO P.17
Niclin, la carte européenne

NATATION P.18
Léon Marchand : « Je n'ai pas l'impression d'avoir changé »

Le fait du jour

CYBERMENACES

La Réunion, un territoire

Dans son rapport sur l'état de la menace cyber dans l'océan Indien, Cyber Réunion, en collaboration avec la société Own, offre une analyse pointue des cybermenaces auxquelles l'île est confrontée. Dans un monde en pleine mutation, La Réunion se situe à un carrefour de nombreux enjeux.

Les câbles sous-marins font l'objet de toutes les attentions, parfois malveillantes.

Notre territoire doit se préparer à des attaques cyber *«de plus en plus sophistiquées. L'accent est mis sur la nature polymorphe des menaces, allant des campagnes de phishing aux usurpations d'identité, en passant par les fuites de données sur le deep et dark web»*. De par sa position géographique et parce qu'elle est un département français, par ailleurs territoire le plus riche de la zone (avec un PIB à plus de 21 milliards d'euros en 2023), La Réunion est une cible privilégiée de la cybercriminalité et des menaces étatiques, notamment de la Chine et de la Russie.

Sur ce dernier point, *«l'île se distingue par son niveau de connectivité avancé, avec des infrastructures numériques cruciales, comme des câbles sous-marins reliant l'Afrique, l'Asie et l'Europe»*. Des infrastructures qui sont vulnérables aux accidents, cyberattaques et tentatives d'espionnage. Chacun se remémore ainsi les difficultés de connexion en août 2023 et en janvier 2024 aux services Internet fixe et mobile d'opérateurs réunionnais, surtout dans les zones de Saint-Denis, Saint-Paul, Le Port et La Possession. En cause : plusieurs incidents, pas forcément malveillants, sur les câbles sous-marins Safe et Lion.

Ces câbles sous-marins peuvent susciter aussi l'intérêt d'acteurs internationaux à la recherche de renseignements de tout ordre. En 2022, Pravin Jugnauth, l'ancien Premier ministre de l'île Maurice avait ainsi été mis en cause dans une affaire d'espionnage supposé sur les câbles reliant l'île Sœur à internet, impliquant trois techniciens indiens. Plus récemment, en novembre dernier, toujours à Maurice, des enregistrements téléphoniques privés de personnalités politiques et judiciaires avaient été diffusés sur les réseaux sociaux dans le contexte des élections générales.

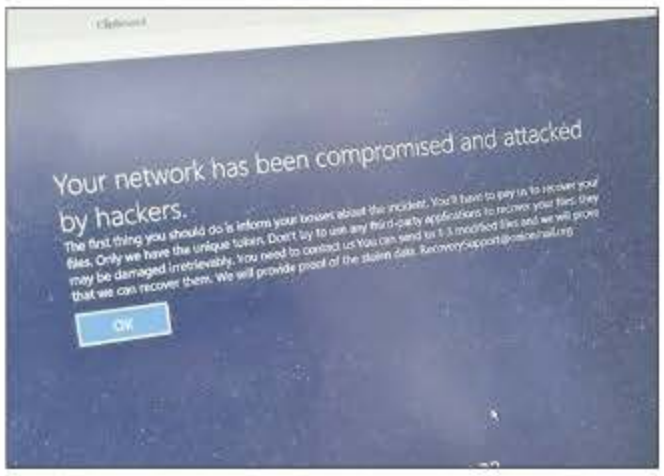
Des attaques en 2024

■ Le groupe Cirano (Antenne Réunion et radios)

Le 21 août 2024, des attaques par rançongiciels ont frappé les médias du groupe Cirano. «Ces cyberattaques ont paralysé les systèmes de diffusion.» Conséquence : silence des radios et perturbations sur Antenne Réunion pendant quelques heures. Par ailleurs, une fuite de données massive a été constatée, impliquant une archive de 146 Go contenant des informations sensibles. «Parmi les données compromises figurent des copies de cartes d'identité, des documents de facturation et des fichiers relatifs à la taxe d'habitation. L'attaque a été revendiquée sur le blog du groupe de rançongiciels Sarcoma, qui serait affilié à l'acteur connu sous les pseudonymes «Katy West» ou »Mont4na« (il pourrait s'agir d'un groupe d'individus plutôt que d'un acteur isolé). Le 24 octobre 2024, les données fuitées étaient encore accessibles sur le dark web.»

■ Le Conseil départemental

«Le 13 novembre 2024, le Département a subi une cyberattaque qui a perturbé ses services informatiques. L'attaque a été revendiquée par le groupe Termite. Apparu en novembre 2024, Termite est un opérateur de rançongiciels spécialisé dans la double extorsion. Après avoir chiffré les fichiers de ses victimes, il menace de divulguer les données volées via un site dédié sur le dark web, où il mène également ses négociations. Le rançongiciel utilise un chiffrement robuste […] et applique l'extension ».termite« aux fichiers chiffrés. En complément du chiffrement, Termite laisse une note de rançon, généralement intitulée »How To Restore Your Files. txt«, sur les systèmes compromis. Cette note contient un lien vers un site sécurisé de fuite de données, des adresses e-mail ProtonMail pour la communication, ainsi qu'un token unique (solution d'authentification forte, N.D.L.R.) permettant à la victime de négocier et d'effectuer le paiement.»



En août 2024, les systèmes du groupe Cirano avaient été attaqués et la direction avait reçu ce message. (Photo AG)

La Réunion au centre d'un jeu de pouvoirs

La Réunion se situe à l'intersection des câbles Lion (Lower Indian Ocean Network), Metiss (MEltingpoT Indianoceanic Submarine System) et Safe (South Africa Far East), qui permettent de relier notamment Madagascar, Maurice, l'Afrique du Sud, l'Inde et la Malaisie. Preuve que l'océan Indien devient un des pivots des échanges mondiaux de données, le géant américain Google a lancé un chantier titanesque, le projet Umoja («Unité» en swahili), première connexion sous-marine par fibre optique qui partira du Kenya et traversera l'Ouganda, le Rwanda, la République démocratique du Congo, la Zambie, le Zimbabwe et l'Afrique du Sud, avant de plonger dans l'océan Indien jusqu'en Australie.

Google n'a pas communiqué de détails quant à sa mise en service, mais les experts estiment qu'il pourrait l'être dès 2026. En désenclavant une partie du continent africain, avec des liaisons vers l'Europe puis le reste du monde, il va ouvrir de nouvelles perspectives en termes de développement. Mais également de cybermenaces. *«Ces nouvelles routes numériques deviennent des artères vitales de l'économie mondiale»*, souligne le rapport de Cyber Réunion. Et à ce titre, autant de cibles pour les pirates. Quels qu'ils soient.

Antoine GESLIN

Téléchargez le rapport complet sur l'état de la menace cyber dans l'océan Indien.

Cyber Réunion, un réflexe local contre les cybermenaces

Cyber Réunion est la marque du pôle cybersécurité de Réunion THD, un établissement public de la Région Réunion. Depuis son lancement fin 2024, cette initiative permet de mettre en place des moyens techniques et organisationnels concrets pour aider les acteurs locaux (entreprises, collectivités et associations) à renforcer efficacement leur niveau de cybersécurité. Le rapport sur l'état de la menace cyber dans l'océan Indien, en collaboration avec la société Own, participe à cette montée en puissance de la cybersécurité à La Réunion.

Luttes informationnelles dans les territoires ultramarins

Comme nous le révélions dans notre édition du 24 janvier 2025, le rapport de Cyber Réunion confirme que le Baku Initiative Group, un organisme azerbaïdjanais se présentant comme une ONG dédiée à la lutte contre le colonialisme, a été à l'initiative d'opérations de manipulation de l'information, notamment via le mouvement réunionnais «Ka-Ubuntu». Après un Congrès des Colonies Françaises, organisé en Azerbaïdjan, «l'analyse des termes Colonisation, Décolonisation, colon, coloniale, politique coloniale, associés à des îles françaises comme Nouvelle-Calédonie, Martinique, Mayotte, La Réunion, Guadeloupe, a généré plus de 1 million de messages en septembre 2024 sur le réseau social X», indique le rapport de Cyber Réunion.

«Ces actions menées par l'Azerbaïdjan semblent être des mesures de rétorsion contre des politiques françaises jugées trop favorables aux intérêts arméniens.» Néanmoins, «les conséquences réelles de ces tentatives de déstabilisation restent actuellement limitées.»

Cyber Réunion entend répondre aux acteurs locaux qui seraient victimes d'une cyber-attaque.

Le Quotidien

LE QUOTIDIEN DE LA RÉUNION ET DE L'OCÉAN INDIEN
www.lequotidien.re

69 rue Sainte Anne,
97400 Saint-Denis
Tél : 0262.02.67.15

Jean-Jacques Dijoux,
président
Henri J. Nijdam,
directeur de la publication

Rédaction
Yves-Eric Houpert
rédacteur en chef
Tél : 0262.02.67.15
laredaction@lequotidien.re

Régie Commerciale
Tél : 0262.02.67.15
resa.regiepub@lequotidien.re
Maximin DUSSEL
Directeur Commercial
mdussel@lequotidien.re
Annonces classées
pa@lequotidien.re
Régie extra locale
Tél 01.53.64.58.60
p.delataille@media-outremer.fr
Abonnements
abonnements@lequotidien.re
Agences
NORD Saint-Denis
69 rue Sainte Anne,
97400 Saint-Denis
Tél : 0262.02.67.15
stdenis@lequotidien.re
SUD Saint Pierre
agence-sud@lequotidien.re
OUEST Saint-Gilles
agence-ouest@lequotidien.re
EST Saint-André
agence-est@lequotidien.re
Media Capital Réunion
SAS au capital de 1,000 € RCS 924 834 849 Saint-Denis de La Réunion,
Siège social :
103, rue du Général de Gaulle, St Gilles les bains 97434 - Saint Paul -
Président : Jean-Jacques Dijoux,
Directeur général: Henri J. Nijdam
CPPAP 06 26 C 87475 ISSN 0397-7994
Reproduction interdite
Tous droits réservés.
Imprimerie ICP ROTO
38 rue Claude Chappe
97420 Le Port

ACPM

N° 16132 - 49e année
Tirage : 15 000 exemplaires
DL 25.04.091P

stratégique particulièrement exposé

L'an dernier, les systèmes du groupe Cirano et du Conseil départemental ont été la cible d'attaques majeures. (Photo DR)

« La cybersécurité est un sujet de développement pour La Réunion »

Mathieu Druilhe de Cyber Réunion répond aux questions du Quotidien:

- Il s'agit du premier rapport sur l'état de la menace cyber dans l'océan Indien publié par Cyber Réunion. Pourquoi cette démarche ?

- Le premier objectif, c'est de tordre le cou aux gens qui pourraient pratiquer le marketing par la peur. Derrière, il y a des intérêts financiers d'entreprise, que ça soit les vendeurs d'antivirus, que ça soit les prestataires. La cybersécurité, ce n'est pas un produit, c'est un processus, c'est une vision un peu globale. Les chefs d'entreprise ont l'habitude de gérer les risques financiers, les risques humains, les risques organisationnels, et il faut juste réussir à les culturer sur une thématique de risque qui peut paraître extrêmement technique de prime à bord, mais qui ne l'est pas tant que ça.

Cyber Réunion est investi de cette mission de manière très claire. Un des sujets aussi qu'on essaie de faire transparaître dans le document, c'est le fait qu'on ne peut pas parler que de l'île de la Réunion. On est obligé de la considérer dans son écosystème, dans son environnement régional. Il nous paraît intéressant, avec deux représentations françaises dans l'océan Indien, de pouvoir commencer à construire un narratif et une histoire là-dessus.

«Sujets géostratégiques»

Parce que la cybersécurité est une menace, on est en train de poser les fondations d'une solution régionale d'accompagnement sur ces sujets-là, mais la cybersécurité constitue aussi potentiellement une opportunité de développement économique. L'idée est de positionner le savoir-faire, l'excellence européenne, nationale et locale dans le cadre du développement économique de cette activité.

- À travers le rapport de Cyber Réunion, on se rend compte que La Réunion a un rôle majeur à jouer.

- On a des choses à dire et à partager avec les États de la zone et derrière ça, c'est une forme de soft power réunionnais. Dans le rapport, on parle de sujets géostratégiques avec les câbles, on parle de sujets sur la désinformation, de ce qui s'est passé à Maurice avec les écoutes, avec les espionnages des câbles.

Ces sujets sont quand même sérieux, sensibles. On parle des campagnes de déstabilisation qu'il a pu y avoir en outremer, qui se sont poursuivis encore récemment avec Mayotte où il y a des influences russes assez fortes. On vit des moments de tension internationale qui sont hallucinants.

Donc, il faut aussi comprendre et intégrer ces sujets de cybersécurité, de cybermenaces, dans l'échiquier régional, et les luttes d'influence qu'il peut y avoir. On sait tous que la zone océan Indien est un carrefour historique des échanges internationaux, et ce n'est pas près de s'arrêter.

- Comment analysez-vous la réponse du groupe Cirano lorsqu'il a été attaqué, avec une forte communication, en ouvrant ses portes aux journalistes notamment ?

Mathieu Druilhe, de Cyber Réunion (à droite). (Photo Ludovic Prouvost)

-Une victime, et ce n'est pas uniquement dans les sujets cyber, a énormément de difficultés à judiciariser, et puis, ça fait honte. On est sur un petit territoire où tout le monde se connaît.

J'ai trouvé la communication du groupe Cirano absolument admirable sur ces sujets. On a eu des retours de Sylvain Péguillan (le CEO du groupe, N.D.L.R.). Je l'ai vu dans des documents vidéos qui sont sortis et il est intervenu dans des conférences avec des retours d'expérience où il était extrêmement lucide, où il disait : «on était sur des trucs qu'on était sur le point de faire, mais on traînait.

Mon conseil, c'est de dire à tout le monde: faites de l'authentification forte. Ce n'est plus uniquement un identifiant et un mot de passe. Il faut mettre en place des mécanismes qui permettent d'authentifier de manière plus sécurisée la personne. Je pense que l'un des sujets derrière l'élévation de la maturité cyber du territoire, c'est aussi l'élévation de la maturité informatique du territoire.

On est sur le podium des trois territoires les mieux fibrés de France. On a des infrastructures de câbles sous-marins. Il faut maintenant qu'on prenne conscience de tout cela et que la mise en œuvre de ces technologies soit raisonnée, qu'elle soit faite dans un contexte durable. Il y a un vrai sujet, c'est la formation.

Depuis des années, on déploie des technologies qu'il faut accompagner en formant les gens. Ça doit se faire de manière logique, en respectant les temps d'assimilation, d'apprentissage.

Avec la transformation digitale, on est en train de constituer le système nerveux de demain des entreprises. On entend tout le monde parler d'intelligence artificielle: il va y avoir des impacts sur les emplois que peu de gens arrivent à identifier clairement. Il y a aussi des enjeux de souveraineté derrière ces sujets.

Propos recueillis par A.G.

Les menaces qui pèsent sur notre île

Cybercrimes

«La menace cybercriminelle a été évaluée comme un risque critique pour La Réunion», indique le rapport de Cyber Réunion. Les entreprises réunionnaises peuvent être exposées à des fuites de données, à des campagnes de phishing (hameçonnage de renseignements personnels afin de perpétrer une usurpation d'identité), et aux attaques par rançongiciels. «Ces menaces visent aussi bien les entreprises locales que les institutions publiques, souvent pour des gains financiers rapides. Le phishing et les ransomwares, par exemple, peuvent paralyser les systèmes, perturber les services essentiels et affecter gravement l'économie de l'île.» En 2024, les attaques informatiques à des fins d'extorsion se sont maintenues à un niveau élevé. «L'écosystème cybercriminel ne cesse de se diversifier», relève le rapport de Cyber Réunion, «notamment avec la diffusion de codes source de rançongiciels en open source et la multiplication d'outils accessibles à des acteurs disposant de compétences techniques limitées.»

Hacktivisme

En tant que département français avec un PIB de plus de 21 milliards par an, La Réunion est une cible privilégiée des cybercriminels. (Photo Yann Huet)

«Le hacktivisme a été évalué comme un risque sérieux pour La Réunion, plusieurs attaques ayant ciblé le territoire en réaction aux positions prises par la France», dans le cadre de l'invasion de l'Ukraine par la Russie et l'Ukraine, mais aussi de la guerre entre Israël et le Hamas, ou encore de l'arrestation du fondateur de Telegram, Pavel Durov, en France le 24 août 2024. «Lors de la campagne #FreeDurov, où des attaques ont visé des infrastructures locales pour protester contre l'arrestation de Pavel Durov, [...]. Ces attaques, souvent idéologiques, créent des perturbations temporaires, notamment dans les services publics. La Réunion, en tant que territoire français, reste vulnérable à ces campagnes à portée mondiale, qui peuvent avoir des impacts locaux significatifs.»

En lien avec la campagne de soutien à Durov, un groupe de hackers a attaqué le site internet de l'aéroport Roland Garros dans l'après-midi du 27 août 2024, «selon les preuves fournies par le groupe, le site serait resté inaccessible pendant près de 40 minutes», indique le rapport de Cyber Réunion, qui précise que, «initialement concentrées sur les institutions et entités gouvernementales, les cibles ont progressivement inclus d'autres secteurs tels que les transports, la logistique et la santé.»

De la même manière, quelques jours après l'attaque hacktiviste contre le site Internet de l'aéroport, une autre attaque a visé le site «Reunion Traffic Information», qui fournit des informations en temps réel sur les conditions de circulation à La Réunion (trafic, incidents, fermetures de routes, etc.). C'était le 2 septembre 2024, et le groupe à l'origine de ces attaques contre la France avait lancé ce raid suite à une réunion à la Maison Blanche, autour du soutien à l'Ukraine, impliquant notamment des représentants français.

Activités étatiques

«La menace d'origine étatique a été évaluée comme un risque mineur pour La Réunion. Bien que le territoire occupe une place stratégique, celle-ci doit être relativisée par rapport à d'autres territoires de la zone Asie-Pacifique, qui se trouvent davantage au cœur des tensions». Néanmoins, en tant que département français, La Réunion est un territoire très exposé «dans une région où les grandes puissances mondiales, notamment la Chine, l'Inde et les États-Unis, rivalisent pour étendre leur influence. Ces pays exercent un contrôle croissant sur cet espace maritime, matérialisé par des bases navales et militaires et des projets d'infrastructures majeurs [...]. Le rapport souligne que «dans la zone Asie-Pacifique, à laquelle appartient La Réunion», un certain nombre de groupes, notamment affiliés à la Chine, sont très actifs.