PRÉFET
DE LA RÉUNION
Liberté
Égalité
Fraternité

COMMUNIQUÉ DE PRESSE

Saint-Denis, le 22 avril 2024

Face au risque cyber à La Réunion : l'État renforce sa mobilisation

S'informer, se protéger et réagir

Les cyberattaques sont de plus en plus nombreuses, au plan international et national et La Réunion n'échappe pas à cette tendance. Le centre hospitalier universitaire Nord de Saint-Denis, la commune de Saint-Philippe et plusieurs entreprises en ont été victimes en 2023 et ce début d'année 2024 occasionnant d'importants préjudices financiers. **À La Réunion, 14 incidents ont été remontés à l'agence nationale de sécurité des systèmes d'information (ANSSI) en 2023, contre 11 en 2022,** chiffre bien inférieur au nombre réel de cyberattaques puisque de nombreuses entités n'ont pas connaissance de cyberattaques subies ou ne se signalent pas.

Ces attaques prennent des formes diverses : rançongiciels, déni de service, hameçonnage, usurpation d'identité, vols de données personnelles et concernent des acteurs divers : entreprises, collectivités, administrations, associations, particuliers.

Cette année, avec les élections européennes et les Jeux olympiques et paralympiques la France est particulièrement exposée.

L'État est le chef de file en matière de politique de cybersécurité avec l'ANSI, rattachée aux services du Premier ministre. L'État accompagne en ce sens les acteurs économiques et les collectivités dans le renforcement de leur sécurité informatique et dans la réponse aux incidents.

S'informer, se préparer et se protéger

Face à la hausse des cyberattaques sur le territoire, le préfet de La Réunion, Jérôme Filippini, tient à **sensibiliser** l'ensemble des usagers sur la présence de ce risque, afin que chacun prenne les mesures nécessaires pour **prévenir et se protéger** en adoptant les bons réflexes : anti-virus, sécurité des mots de passe, VPN, sauvegarde régulière des données, etc.

Un travail de **prévention** est mené notamment auprès des élèves, des associations et des entreprises par la police nationale et la gendarmerie nationale, qui procèdent également à des sensibilisations et des diagnostics cyber auprès des collectivités (7 communes depuis 2022).

L'ANSSI met à disposition des collectivités et des entreprises **des formations et des outils de sécurité numérique** (« MonAideCyber », guides…) pour développer leur sécurité numérique. Ainsi, 21 structures réunionnaises ont notamment bénéficié d'une montée en compétence en

Service régional de la communication interministérielle
Téléphone : 0262 407 419 / 434 / 457
Courriel : communication@reunion.gouv.fr
Internet : www.reunion.gouv.fr / Twitter – Facebook – Instagram - LinkedIn : @Prefet974
Sollicitations presse : https://wkf.ms/3kc53kb

termes de cybersécurité grâce au dispositif « parcours de cybersécurité ».

Des financements d'outils et de formations sont aussi proposés par l'ANSSI, qui a aussi déployé **un appel à projets dans le cadre de France 2030** visant à soutenir la sécurisation des réseaux, avec un taux de subvention pouvant atteindre 70% : https://cyber.gouv.fr/actualites/lanssi-lance-un-appel-projet-de-cybersecurite-dans-le-cadre-de-france-2030

Pour développer ses compétences en la matière et renforcer sa sécurité informatique, l'État propose deux sites internet complémentaires, mettant à disposition de la documentation ainsi que des outils de formation et d'accompagnement :

- **Pour les particuliers, associations, TPE, etc. : www.cybermalveillance.gouv.fr**
- **Pour les grandes entreprises et les collectivités : www.cyber.gouv.fr**

L'Union européenne et l'État financent la création d'un **centre de ressources en cybersécurité** porté par le conseil régional via l'établissement public Réunion THD. Il permettra, à la fin de l'année 2024, d'accompagner les collectivités et les TPE/PME dans la consolidation de leurs réseaux et la réponse aux incidents avec pour missions principales la sensibilisation et la formation, le soutien aux projets locaux visant à structure et développer l'offre et la demande en cybersécurité et la mise en place d'une réponse aux incidents de premier niveau pour les structures qui font face à un incident de cybersécurité.

Réagir en cas d'attaque

L'une des premières mesures à prendre est de **porter plainte**, car trop peu d'attaques sont connues par les pouvoirs publics, ce qui minimise la connaissance du risque. Cette démarche est notamment nécessaire afin de pouvoir poursuivre les auteurs et souvent obligatoire afin de pouvoir bénéficier d'une indemnisation de son assureur.

À La Réunion, la gendarmerie nationale à La Réunion possède une antenne dédiée à la lutte contre les criminalités numériques, avec des enquêteurs experts notamment en technologie financière et en cyberdéfense des TPE/PME.

Au sein de la police nationale de La Réunion, une antenne de l'office anti-cybercriminalité a été créée début 2024 et comptera 7 personnels dédiés à traiter les cyberattaques, les infractions à la pédopornographie en ligne, ou encore les dossiers d'usurpation d'identité sur Internet.

Par ailleurs, en cas de cyberattaque, l'État met à disposition deux plateformes d'accompagnement :

- La plateforme de l'ANSSI « CERT-FR », joignable 7j/7, 24h/24 par téléphone au +33 (0)9 70 83 32 18 ou cert-fr@ssi.gouv.fr ;
- La plateforme Cybermalvaillance : https://www.cybermalveillance.gouv.fr/

Il convient enfin également de saisir la Commission nationale informatique et liberté (CNIL) en cas de violation des données personnelles.