



Cyber attaque : l'état de la menace à La Réunion, les conséquences d'une crise sur l'île et les réponses apportées.

Découvrez comment la cybermalveillance peut nuire à la santé



Intervenants



M. Gérard Cotellon
Directeur Général de l'ARS Réunion



M. Patrice Bigeard
FSSI Adjoint Ministère de la Santé
et de la Prévention



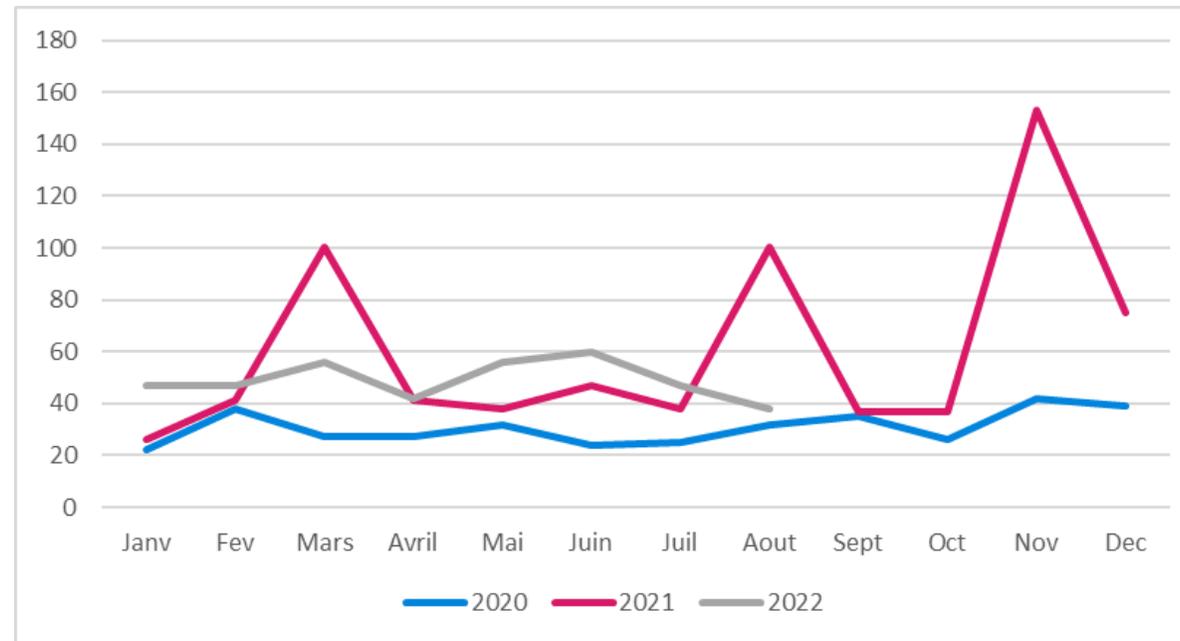
M. Lionel Calenge
Directeur Général du CHU
de La Réunion et du GHER
Président du Comité Stratégique du GHT



Dr Rachid Dekkak
Président CMG du GHT
de La Réunion



Une augmentation des incidents de sécurité entre 2022 et 2021





Des impacts à tous les niveaux

- **Impacts fonctionnels, techniques, financiers et humains !**
Durée des impacts : 2/3 semaines → plusieurs mois (selon la gravité de l'impact et le niveau de préparation)
- **Fort impact médiatique** des rançongiciels qui ne sont pas les seuls types d'attaques.



Focus sur les rançongiciels

Qu'est-ce qu'un rançongiciel ?

Technique de cyber attaque consistant à envoyer à la victime un logiciel malveillant qui rend incompréhensible l'ensemble de ses données (chiffrement) et lui demande une rançon en échange du mot de passe de déchiffrement.

- **Quelques vecteurs principaux des rançongiciels :**
 - × les vulnérabilités dans les systèmes bureautiques (dette technologique, mises à jour trop tardives);
 - × les failles sur les systèmes de messagerie;
 - × L'hameçonnage (mail malveillant);



Ce qu'il faut retenir

Numériquement, notre système de santé évolue, la **cybersécurité doit donc être considérée comme une exigence stratégique !**

Le constat reste alarmant :

- × **Des mauvaises pratiques informatiques** (mot de passe faible, clics sur des mails frauduleux, virus transmis via des clés usb branchées sur les outils numériques de l'établissement...)
- × Des équipes en SSI trop souvent sous-dimensionnées
- × Une **grande hétérogénéité des applications à administrer et sécuriser** (parfois plus de 200 applications au sein d'un seul GHT)
- × Des solutions **logicielles vulnérables**, pour les métiers de la santé comme pour les infrastructures des établissements



Quelles conséquences si cette menace s'aggravait et impactait une île comme La Réunion ?



Un label gage de cybersécurité, mais pas que...



Un label



Des experts



Des prestations



Une campagne d'affichage incisive mais pas que...

**Laisser entrer un intrus dans un bloc opératoire ?
Quelle idée !
Et sur votre ordinateur,
on en parle ?**



Quand je reçois un mail suspect :

Offre alléchante, apparence suspecte, pièce jointe inattendue, adresse d'expédition fantaisiste, demande de données confidentielles...

- Je ne clique pas sur les liens
- Je ne transmets pas mon mot de passe
- Je n'ouvre pas la pièce jointe



**Utiliser plusieurs fois la même seringue ? Quelle idée !
Et votre mot de passe,
on en parle ?**



Au bureau comme à la maison :

- Je ne partage jamais mon mot de passe
- J'utilise des mots de passe différents pour mes outils pros et persos
- Je crée des mots de passe complexes contenant chiffre, majuscule et caractère spécial



**Un pique-nique dans le bloc opératoire ? Quelle idée !
Et le mélange vie pro/vie perso,
on en parle ?**



Quand je suis au bureau :

- Je n'utilise pas mon adresse mail personnelle pour échanger au sujet des patients
- Je ne branche pas ma clé usb ou mon téléphone personnels aux ordinateurs
- Je ne stocke pas mes photos de vacances sur les postes de travail





Un eco-système à disposition des acteurs



UN LABEL



DES EXPERTS



DES PRESTATIONS



DE LA SENSIBILISATION

DES JEUX SÉRIEUX



Question pour un cyberchampion



Escape game



Code de la cyber sécurité



Phish me if you can

e-Nov



Merci de votre attention !