Alerte Cyberattaque mondiale - Campagne rançongiciel

Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE

Mesdames, Messieurs,

Comme vous le savez nous traversons un épisode sans précédent en termes de gravité de diffusion d'un virus/ver de cryptovirus dont le nom de code est notamment « WanaCrypt0r ».

Afin de protéger notre environnement de travail et notamment la messagerie professionnelle contre la propagation de spam et virus, je vous demande de respecter scrupuleusement les consignes d'usage, en particulier d'accroitre plus que jamais votre vigilance sur l'ouverture de pièces jointes ou des liens suspects.

Ne pas cliquer sans vérification préalable sur les liens de messages et les pièces jointes.
Cela vous évitera d'exécuter des programmes malveillants tel que ce récent ransomware (logiciel de rançon) dont le nombre de victimes ne cesse de croître (Recensement Europol du 13/05 : 200 000 PC infectés et 150 pays touchés).

Certains des utilisateurs de la messagerie académique ont reçu ce week-end un mail frauduleux les informant d'un gain important à la loterie. Ce mail doit être supprimé sans ouvrir les pièces jointes.

En cas d'infection avérée vous devez impérativement :

- Déconnectez immédiatement le poste infecté du réseau
- **Ne pas payer la rançon**

Rappel des bonnes pratiques individuelles en sécurité informatique qui s'imposent en matière de cyber sécurité, chacun doit veiller à avoir :

- **Un ordinateur entretenu et à jour,**
- Utiliser un système à jour, activer le verrouillage automatique,
- Mettre à jour votre antivirus local régulièrement,
- Sécuriser physiquement les ordinateurs et ne pas les laisser sans surveillance.
- **Un comportement responsable est indispensable dans ce contexte sensible, soyez encore plus vigilant.**

- Utiliser des mots de passe robustes, variés et ne jamais les communiquer même aux administrateurs.
- Ne pas réagir trop vite aux messages, se méfier des offres trop alléchantes (propositions lucratives et/ou sites de rencontres) et n'ouvrir que les pièces jointes légitimes.
- Utiliser une messagerie adaptée aux échanges (professionnelle ou personnelle) et ne jamais faire suivre les canulars et les spams.
- Naviguer sur Internet avec prudence, éviter les sites peu connus ou douteux. Contrôler la diffusion d'informations, car tout ce qui apparait sur Internet y demeure longtemps.
- **Effectuer des sauvegardes régulières sur les réseaux locaux et sur des supports amovibles, et vérifier la restauration des informations.**
- Signaler tous les incidents et les dysfonctionnements relatifs à la sécurité informatique à ***l'assistance par téléphone : 0596 52 25 25 et/ou par mail assistance.informatique@ac-martinique.fr***

Pour informations, je vous prie de trouver ci-après quelques sources officielles du gouvernement :

Alerte ANSSI
http://www.cert.ssi.gouv.fr/site/CERTFR-2017-AVI-082/index.html

Alerte CERT-FR
http://www.cert.ssi.gouv.fr/site/CERTFR-2017-ALE-010/index.html

MS17-010 - CERTFR-2017-AVI-082 : http://www.cert.ssi.gouv.fr/site/CERTFR-2017-AVI-082/index.html

D'avance merci pour votre vigilance.

Cordialement,

Fabienne LOUIS-SIDNEY
Division des Systèmes d'information
Bureau des Infrastructures et de la production
Responsable de la Sécurité des Systèmes d'Information

fabienne.louis-sidney@ac-martinique.fr
Tél : 0596.522840
Fax : 0596.522829
www.ac-martinique.fr
Rectorat de la Martinique - Les Hauts de Terreville - 97279 Schoelcher Cedex