EXPLOSION DES ACTES MALVEILLANTS

SUR LE NET

Les Echos

Les cyberattaques capitalisent sur le coronavirus

« Vol d'informations personnelles, d'argent, infection des ordinateurs avec des logiciels malveillants : les criminels profitent de la peur liée à l'épidémie pour mener des pratiques frauduleuses. »

Challenges

Coronavirus: les cyberattaques explosent à cause de la crise

« Les pirates informatiques profitent du stress provoqué par la crise du coronavirus, et du confinement quasi général, afin de voler des informations personnelles, infecter les ordinateurs de logiciels malveillants ou simplement voler de l'argent. »

Cybervigilance

Le site Cybermalveillance du gouvernement (https://www.cybermalveillance.gouv.fr/) appelle à un renforcement des mesures de vigilance en matière de cybersécurité pour faire face à l'explosion des actes malveillants sur le net.
Si les techniques utilisées ne sont pas différentes de celles précédemment constatées, elles ont toutes pour point commun d'exploiter la pandémie actuelle et la crainte des télétravailleurs, qui, face à l'urgence, sont moins méfiants et tombent parfois dans le panneau.

Télétravail

Nombreuses sont les entreprises qui ont déployé des dispositifs massifs de télétravail pour tenter d'atténuer les effets de la crise sur leurs activités.

Dans ce contexte de travail à domicile, les cyber menaces sont bien réelles et risques de lancer des attaques en plus grand nombre par l'intermédiaire des salariés et de leurs outils informatiques personnels. Ces attaques, de différentes formes (hameçonnage ou fishing, arnaques au coronavirus, campagnes de spearphishing, documents malveillants) peuvent avoir pour conséquence de nuire et corrompre des données de l'entreprise ciblée et de paralyser son activité en tout ou partie.

Agissez avant qu'il ne soit trop tard…

Quels bons réflexes à adopter ?

Un simple clic sur un lien infecté contenant des informations soi-disant importantes sur le virus peut avoir des incidences dramatiques.
Redoublez donc d'attention pour ne pas tomber dans les pièges des cybercriminels :

- **Vérifiez la fiabilité et la réputation des sites que vous visitez**.
  Exemple : faux sites de ventes de masque chirurgical, appels aux dons relatifs au coronavirus…

- **Soyez vigilants aux fausses informations**, pour rester informé sur la situation, référez-vous au site dédié du gouvernement.
  Exemple : sites non officiels proposant l'attestation de déplacement dérogatoire pour collecter vos données.

- **Méfiez-vous des mails sur le thème Covid-19** : ne cliquez pas sur les liens et n'ouvrez pas les pièces-jointes.
  Exemple : des cybercriminels ont usurpé l'identité du Conseil National du Barreau via une lettre d'information COVID 19, proposant à ses membres le paiement de la mise à jour des plugins de sécurité des clés avocats. Il s'agit évidemment d'une arnaque !

- **Gardez un esprit critique**, ne vous précipitez pas et prenez toujours le temps de la réflexion.

- **Ne téléchargez vos applications que depuis les sites officiels** des éditeurs et ne téléchargez jamais de programmes depuis un mail si vous n'êtes pas absolument certain de son origine.

- **Faites régulièrement des sauvegardes de vos données** et gardez une copie déconnectée.

- **Appliquez les mises à jour de sécurité** sur vos équipements connectés (serveurs, ordinateurs, téléphones, tablettes…) dès qu'elles sont disponibles.

- **Utilisez des mots de passe uniques et solides**, ne les communiquez jamais (qu'elle qu'en soit la raison) et activez la double authentification chaque fois que possible.

- **Soyez vigilants aux changements de RIB** de vos fournisseurs et faites un contre-appel à un numéro déjà référencé en cas de doute.

Et souscrivez sans attendre les garanties Cyber que nous proposons !