

Lettre Cyber 67

Décembre
2021

LA CYBERSECURITE:

La cybersécurité consiste à protéger les systèmes, les réseaux et les programmes contre toutes les formes d'attaques numériques. A l'heure où les équipements numériques sont supérieurs aux utilisateurs, il devient de plus en plus complexe d'assurer cette sécurité.

Les types de Cybermenaces les plus courantes :

1/ Le Phishing : Cette menace repose sur l'envoi massifs d'E-mail afin de voler des données sensibles telles que des numéros de comptes bancaires et de mots de passe.

2/ Le Ransomware : Blocage d'un ordinateur ou d'un réseau par cryptage partiel ou complet avec demande de rançon.

3/ Le Malware : Programme malveillant afin d'obtenir des backdoor ou causer des dommages.

4/ L'ingénierie sociale : Tactique de recueil d'informations sur une entité ou des personnes afin de faciliter la commission d'une escroquerie (Arnaque au Président / Faux ordres de virement).

Le Phishing touche pour un très grand nombre les particuliers. Les trois autres typologies visent plus les PME/PMI ainsi que les collectivités territoriales.

Le dispositif I.M.M.U.N.I.T.E Cyber : En partenariat avec l'Association des maires de France (A.M.F) et le dispositif Cybermalveillance.gouv.fr, la gendarmerie nationale met en place un outil de diagnostic simplifié au profit des collectivités territoriales. Cet outil diagnostic peut largement être étendu au PME/PMI ainsi que pour les particuliers qui le désirent. Cette plaquette est disponible en téléchargement ici : <https://www.cybermalveillance.gouv.fr/tous-nos-contenus/actualites/immunité-cyber-questionnaire-sensibiliser-elus-cybersecurite>



Évaluez la sécurité numérique de votre collectivité en 10 points

VÉRIFIER MON IMMUNITÉ CYBER

- I** INVENTAIRE COMPLET
- M** MOTS DE PASSE
- M** MISES À JOUR ET SAUVEGARDES
- U** UTILISATEURS SENSIBILISÉS
- N** NEUTRALISATION DES VIRUS
- I** INFORMATIQUE ET LIBERTÉS
- T** TÉLÉTRAVAIL EN SÉCURITÉ
- É** ÉVALUATION

CYBER ATTAQUES ANTICIPÉES

		OUI	NON ou NE SAIS PAS
1	Avez-vous un inventaire complet de tous vos systèmes numériques ?	<input type="checkbox"/>	<input type="checkbox"/>
2	Utilisez-vous des mots de passe solides et différents pour chaque service ?	<input type="checkbox"/>	<input type="checkbox"/>
3	Vos systèmes numériques sont-ils mis à jour en temps réel et faites-vous des sauvegardes régulières de toutes vos données ?	<input type="checkbox"/>	<input type="checkbox"/>
4	Avez-vous sensibilisé vos agents aux risques numériques ?	<input type="checkbox"/>	<input type="checkbox"/>
5	Vos postes et serveurs informatiques sont-ils protégés par un antivirus ?	<input type="checkbox"/>	<input type="checkbox"/>
6	Etes-vous en règle vis-à-vis du Règlement Général sur la Protection des Données (RGPD) ?	<input type="checkbox"/>	<input type="checkbox"/>
7	Vos agents sont-ils équipés de matériels sécurisés pour le télétravail ?	<input type="checkbox"/>	<input type="checkbox"/>
8	Faites-vous réaliser régulièrement des évaluations de votre sécurité numérique par des audits techniques ?	<input type="checkbox"/>	<input type="checkbox"/>
9	Avez-vous un plan de secours face aux cyberattaques ?	<input type="checkbox"/>	<input type="checkbox"/>
10	ACTION À MENER	<p>Vous êtes dans le VERT : Bravo ! Votre collectivité met en oeuvre les mesures essentielles. Pour aller encore plus loin et vous aider à perfectionner votre sécurité numérique, le réseau des cyber gendarmes est à votre service.</p> <p>Vous êtes dans le ROUGE : Attention, votre collectivité est peut-être en danger. La gendarmerie pour vous aider à faire un état des lieux de votre sécurité numérique et à établir un plan d'actions pour renforcer votre protection.</p>	

UNE HÉSITATION ? UN DOUTE ?
Contactez votre GENDARMERIE pour un ACCOMPAGNEMENT DÉTAILLÉ

Recevoir cette lettre info par mail, envoyez-nous votre demande :

Arnaud.schweitzer@gendarmerie.interieur.gouv.fr ou patrick.wolfert@gendarmerie.interieur.gouv.fr