CAMPUS CYBER

CYBER MALVEILLANCE .GOUV.FR
Assistance et prévention en sécurité numérique

Cybersécurité : 5 RECOMMANDATIONS ESSENTIELLES POUR LES ENTREPRISES

L'actualité démontre que toute entreprise peut être victime d'une cyberattaque, quels que soient sa taille, son secteur d'activité ou sa localisation géographique. Ces cyberattaques peuvent aller jusqu'à les mettre totalement à l'arrêt pendant des jours, voire des mois. Ces situations ont toujours des impacts financiers, réputationnels, voire juridiques importants qui peuvent conduire les organisations les plus fragiles à la cessation de leur activité en cas d'attaque sévère. Pourtant, une grande partie de ces attaques pourraient être empêchées si des mesures simples et peu coûteuses étaient mises en place. À l'occasion du Cybermoi/s (mois européen de la cybersécurité), nous vous livrons 5 recommandations essentielles pour appréhender la cybersécurité dans votre organisation.

Une initiative du Campus Cyber et de Cybermalveillance.gouv.fr
avec le soutien du groupement Alliance du Numérique

Alliance Du Numérique
Groupement IT // Business et Solutions en commun

Licence Ouverte v2.0 (ETALAB)

CAMPUS CYBER

CYBER MALVEILLANCE .GOUV.FR
Assistance et prévention en sécurité numérique

→ 1 CHOISIR DES MOTS DE PASSE SOLIDES ET DIFFÉRENTS POUR CHAQUE SERVICE

Vos mots de passes sont les clés d'accès à vos systèmes, services et aux données qu'ils contiennent. Une mauvaise gestion des mots de passe dans votre organisation peut amener au vol, à la modification ou la suppression de vos données. Utilisez des mots de passe suffisamment longs (12 caractères minimum), impossibles à deviner, et surtout différents pour chaque service utilisé, afin que la divulgation ou le vol d'un de vos mots de passe ne puisse compromettre tout autre service sur lesquels vous pourriez l'utiliser. Pour renforcer la sécurité de vos comptes, activez également la double authentification sur tous les services qui le proposent.

https://www.cybermalveillance.gouv.fr/tous-nos-contenus/bonnes-pratiques/mots-de-passe

→ 2 FAIRE DES SAUVEGARDES RÉGULIÈRES ET DÉCONNECTÉES DE VOS DONNÉES

Lors de certaines cyberattaques, les cybercriminels chercheront à détruire vos données et leurs sauvegardes en ligne pour vous faire chanter. Faire des sauvegardes fréquentes de vos données que vous garderez déconnectées du réseau sera votre meilleure assurance pour redémarrer votre activité avec un minimum de perte en cas d'attaque.

https://www.cybermalveillance.gouv.fr/tous-nos-contenus/bonnes-pratiques/sauvegardes

→ 3 FAIRE SANS TARDER LES MISES À JOUR DE TOUS VOS ÉQUIPEMENTS ET SYSTÈMES

Les mises à jour corrigent des failles de sécurité dans vos matériels et logiciels, qui peuvent être utilisées par des cybercriminels pour vous attaquer. Faire les mises à jour de l'ensemble de ses équipements (ordinateurs, serveurs, téléphones mobiles, tablettes…), applications et logiciels, dès qu'elles vous sont proposées, est donc indispensable pour se protéger.

https://www.cybermalveillance.gouv.fr/tous-nos-contenus/bonnes-pratiques/mises-a-jour

→ 4 ÊTRE VIGILANT FACE AUX MESSAGES D'HAMEÇONNAGE (OU PHISHING)

Les messages d'hameçonnage par mail ou SMS sont l'un des principaux appâts des cybercriminels pour vous dérober des informations sensibles comme des mots de passe, pour vous faire installer un programme malveillant (virus...),ou encore vous faire réaliser un virement frauduleux. Pour vous en prémunir, sensibilisez l'ensemble de vos collaborateurs à cette menace et aux réflexes à adopter en cas d'attaque ou au moindre doute. La cybersécurité est l'affaire de tous, et chacun, à son niveau, peut y contribuer.

https://www.cybermalveillance.gouv.fr/tous-nos-contenus/fiches-reflexes/hameconnage-phishing

→ 5 SE FAIRE ACCOMPAGNER PAR DES PRESTATAIRES DE CONFIANCE

Que ce soit pour évaluer votre niveau de sécurité, vous aider à définir vos plans d'action, en vérifier la bonne réalisation, ou même vous assister en cas d'attaque, n'hésitez pas à vous faire accompagner par des prestataires informatiques dont l'expertise en cybersécurité est reconnue avec des certifications, ou labellisation telles qu'ExpertCyber, PRIS, PASSI…

https://www.cybermalveillance.gouv.fr/accompagnement