LES ENJEUX DE LA SÉCURITÉ DANS LES PME

GROUPE plenitude

4 SUR 10

ONT DÉJÀ SUBI UNE OU PLUSIEURS TENTATIVES D'ATTAQUE EN 2019 *

Face à des hackers de plus en plus inventifs et efficaces, la protection informatique est plus que jamais une priorité pour les PME. En 2020, les systèmes de sécurité centraux sont contournés en attaquant directement les maillons les plus vulnérables : les **postes de travail** et les **utilisateurs**

PROTÉGER

Une politique de mise à jour de sécurité récurrente garantit un niveau élevé de protection pour l'ensemble des postes de travail y compris ceux utilisés en dehors de l'entreprise par les télétravailleurs et les nomades

99,6 %

DES **VULNÉRABILITÉS SUR LES POSTES** SONT LIÉES À L'ABSENCE DE MISE À JOUR *

RESPONSABILISER

grâce à des actions de sensibilisation, tous vos collaborateurs sont formés aux bonnes pratiques pour limiter le risque de cyberattaque au sein de l'entreprise

+ 90 %

DES **INCIDENTS DE SÉCURITÉ** SONT PROVOQUÉS PAR UNE ERREUR HUMAINE *

ANTICIPER

Si malgré tout une attaque réussit, il vous faut une politique efficace de sauvegarde permettant de restaurer vos données des serveurs et postes et d'assurer ainsi la continuité de votre activité

EN 2020, UNE **CYBERATTAQUE COÛTE** EN MOYENNE

35 000 €

CONTRE **9 000 €** EN 2019 *

* Sources : Gartner, CPME, Kaspersky Lab, Hiscox

Face à ces enjeux, nous avons identifié et éprouvé des **solutions de prévention adaptées** pour **protéger les maillons les plus faibles**

SÉCURISER
LES POSTES DE TRAVAIL

Évoluer vers des solutions de nouvelle génération

au travers de **pares-feux** et **antivirus** qui permettent de détecter et de stopper de façon prédictive les cyberattaques

Effectuer des mises à jour de sécurité

récurrentes vous permet de réduire de 99.6% la surface d'attaque et les failles de sécurité de vos postes,* que vous soyez au bureau, en déplacement ou en télétravail

Sauvegarder vos postes *

fréquemment et de façon externalisée, afin d'éviter toute perte de données et d'assurer un maintien de votre activité en cas d'attaque

* et vos serveurs !

SENSIBILISER
LES UTILISATEURS

Rédiger une charte informatique

pour responsabiliser les collaborateurs et assurer une conscience collective des risques liés à l'informatique

Former vos collaborateurs

de façon continue, en présentiel ou en e-learning, aux bons comportements à adopter ainsi qu'aux risques de cyberattaques

Tester leur comportement

grâce à des tests de phishing réalistes et réguliers, pour mesurer l'impact des actions de sensibilisation mises en place

Contactez-nous

Respirez, nous prenons le relais...

GROUPE plenitude

+33 (0)1 55 04 74 74 | contact@plenitude-group.com | www.plenitude-group.com | Paris, Lille, Lyon, Marseille