E-mails corrompus, navigation hasardeuse… Le top 10 des menaces en PME

La problématique qui sonne souvent comme une **quadrature du cercle** pour les PME est qu'elles sont soumises aux mêmes menaces que les grandes sociétés mais disposent en général de moins de moyens pour assurer leur sécurité. Il s'avère quelques fois plus hasardeux pour elles de **sauvegarder leurs actifs**, données et informations clients.

Au top 10 des menaces relevées par la société Watchguard, entreprise spécialisée dans les appliances de sécurité réseau, on retrouve les « oublis » de mise à jour des systèmes : « *Bien que des correctifs soient publiés régulièrement,* ***une majorité des PME omettent de mettre à jour*** *leurs applications ou d'installer ces derniers au niveau de leurs systèmes les laissant vulnérables à des attaques qui peuvent être facilement stoppées* ». Signe que ce type d'action doit désormais entrer dans les habitudes d'utilisation du matériel professionnel.

Au second rang figurent les e-mails à risque. **Les liens qui figurent dans des mails corrompus** sont souvent vecteurs de malwares. Là aussi le rapport tente de se faire didactique : « *un mauvais clic peut vous conduire à l'installation et à l'exécution d'un programme malveillant (****drive by download****)*« .

Sur le podium figure la navigation « imprudente » sur Internet. Pêle-mêle, on retrouve les risques liés aux logiciels espion s, *keyloggers*et autres *spambots* hébergés sur des sites à priori sans danger. Dans la même veine, les **oublis de mise à jour des navigateurs** sont des vecteurs de risques de contagion.

En cinquième position du classement, on retrouve la **perte des appareils mobiles**. Traditionnellement chaque année, des données des PME sont compromises en raison de la **perte d'ordinateurs** portables, ou tout simplement de mauvais rangement d'appareils mobiles ou de clés USB égarées. Des situations déplaisantes qui grâce à un **cryptage** ou plus d'attention sont évitables.

Autre fait intéressant, figure dans ce classement l'utilisation imprudente des **bornes WiFi publiques**. Le risque est de se connecter à un accès sans fil non sécurisé, grâce à un « *packet sniffer*« , un pirate peut alors voir tout ce que l'employé voit …

Suivent ensuite les **menaces dues au domicile non sécurisé**, ou l'absence de politique de sécurité en dehors de l'entreprise, mais aussi les **identifiants par défaut inchangés** et le manque de plan de restauration.

Enfin, le **manque d'une politique de contrôle** ou de vérification régulière des accès aux systèmes réseaux est un fort risque de pertes de données qui peut parfois s'étaler sur de longues périodes.

Une gamme de menaces qui impliquent des ripostes et surtout une prise de conscience. Après cette rentrée, ressortez donc vos crayons et trousses, un peu de **pédagogie** ne fait jamais de mal.