L’antivirus, la version gratuite ou payante?
Par Éric Durez, directeur TI

Depuis le début des années 90, nous sommes sans cesse influencés par la phrase : « vous avez besoin d’un antivirus pour protéger votre ordinateur ». Donc vous l’installez vous-même sur votre ordinateur, vous le faites installer par un technicien ou mieux encore le manufacturier vous fournit une version gratuite de 30 jours. D’autres diront : « heureusement, moi j’ai un MAC, je n’ai pas besoin d’un antivirus ». Ensuite, nous oublions que nous avons un antivirus, car maintenant qu’il est installé, nous croyons qu’il fonctionne tout seul et la vie est belle ! Eh bien non, détrompez-vous, et c’est justement ce comportement que les pirates informatiques attendent de vous.

En effet, votre antivirus ne bloque pas tous les virus. Un ver informatique, un cheval de Troie, un rançongiciel, l’hameçonnage, pour ne nommer que ceux-ci, ne sont pas des virus informatiques.

Un virus informatique n’est qu’un code qui s’attache à un programme légitime exécutable et attend qu’un utilisateur l’active. Un ver informatique ne requiert pas d’intervention de l’utilisateur, car c’est un code fonctionnel par lui-même. Le cheval de Troie est un programme anodin qui cache une fonction d’accès dérobé. Le rançongiciel chiffre les données et fait une demande de rançon. L’hameçonnage n’est ni un logiciel ni un code. Donc, non ce ne sont pas tous des virus informatiques. Tous les maliciels utilisent une panoplie différente de vecteurs d’attaque, et non, l’antivirus ne les bloque pas tous.

L’antivirus informatique est comparable à un vaccin contre la grippe. Les vaccins ne nous protègent pas de tous les rhumes et surtout pas de toutes les grippes. Est-ce que la performance du vaccin est reliée à son prix ou à la compagnie pharmaceutique qui l’a conçu ?

En informatique, les maliciels ont tous leurs particularités et n’attaquent pas uniquement votre ordinateur, mais aussi tout ce qui est connecté à votre réseau informatique (avec un fil ou en Wifi), ou joignable par l’Internet. Ainsi, vos téléphones IP, vos haut-parleurs, vos téléviseurs intelligents, vos caméras, vos accessoires connectés, etc., sont tous exposés aux attaques des maliciels.

Il existe une multitude de maliciels qui tentent par tous les moyens de détruire vos données, de dérober des informations sensibles, comme vos dossiers patients, de vous arnaquer ou de détourner votre argent. Ce sont des robots infatigables, à l’affût 24 heures sur 24, de la moindre faille ou du petit changement pour l’exploiter, quelle que soit la destination. Ils ne font pas la différence entre une station orbitale, une centrale nucléaire, une institution financière, votre cabinet ou votre résidence. Le rapport de SonicWall « 2020 — SonicWall-cyber-threat-report » a recensé 9,9 milliards d’attaques de maliciels en 2019. À cela, on peut ajouter les 4 trillions de tentatives d’intrusion, et les 34,3 millions d’attaques sur les accessoires connectés. Un antivirus, c’est un vérificateur qui vérifie les zones sensibles déjà connues à la recherche des signatures de maliciels qu’il connait. L’antivirus est plus orienté vers les virus, chevaux de Troie, et vers. Depuis 1987, les développeurs d’antivirus et de maliciels cherchent à les bloquer et les contourner. Les développeurs de maliciels ciblent de plus en plus les comportements des utilisateurs pour infecter les systèmes et utiliser les accessoires connectés comme nouveau vecteur d’attaque.

Depuis sa mise en marché, le système d’exploitation Windows 10, développé par Microsoft, comporte un antivirus et même un pare-feu local. D’origine, pour Apple, les IOS ont toujours eu dans leur code une

fonctionnalité apparentée à l'antivirus. Aussi longtemps que votre antivirus provient d'un éditeur reconnu et qu'il est à jour, que ce soit une version gratuite ou payante, l'ANTIVIRUS reste majoritairement similaire. Les versions payantes des éditeurs reconnus sont enrichies par des consoles de gestion centralisée, des VPN, des pare-feu, des fonctionnalités de protection des mots de passe et autres. La majorité de ces fonctionnalités n'améliore en rien l'antivirus. Aucun de ces mécanismes, ainsi que l'antivirus, ne vous protège complètement contre toutes les actions humaines exécutées par un simple clic, ou des failles exploitables sur vos accessoires connectés. Cela s'applique à tous les systèmes d'exploitation que ce soit Apple, Linux, Microsoft ou autre.

La sécurité informatique ne doit pas être réalisée par un seul produit, que l'on installe et que l'on oublie. Elle doit être prise très au sérieux et contrôlée par un ensemble de services surveillés et mis à jour régulièrement. L'antivirus en fait partie, de même que les services fournis par Net+ ACDQ, tels que le VPN, le pare-feu SonicWall et ses composantes de sécurité de calibre industriel. Ils surveillent le trafic entrant et sortant vers l'Internet. Cette vigie effectuée par l'équipement du réseau Net+ ACDQ constitue des couches de sécurité supplémentaires qui vous protègent et chacune d'elles renforce votre sécurité informatique.

Contourner ces services, pour satisfaire vos techniciens, pour augmenter la vitesse de consultation de divers sites ou pages Web ainsi que l'utilisation des réseaux sociaux par votre personnel, revient à exposer vos données électroniques aux pirates informatiques. Cela fait partie des failles pour lesquelles les maliciels restent à l'affût. Il ne faut pas oublier que c'est vous, Docteur(e), qui êtes imputable de la sécurité des dossiers de vos patients, pas votre technicien, ni votre personnel, ni le gestionnaire du cabinet et encore moins votre service infonuagique. Cela fait partie de vos droits et obligations de bien comprendre comment sont protégées vos données sensibles.

Ne faites pas partie du risque, mais de la solution. En cas de doute, n'oubliez pas que nos agents sont disponibles pour vous guider.