Windows 7 : 1 PC sur 4 sera plus vulnérable aux ransomwares à partir de janvier 2020

Les PCs qui utiliseront toujours Windows 7 après l'arrêt complet de son support le 14 janvier prochain seront extrêmement vulnérables aux ransomwares. Selon les experts, 26% des PCs devraient toujours utiliser le l'OS Microsoft malgré la suspension du développement des patchs et des correctifs visant à résoudre bugs et vulnérabilités.

La vulnérabilité aux ransomwares des PCs exécutant des logiciels obsolètes a largement été démontrée lors de l'attaque par le ransomware WannaCry en 2017. Malgré la mise à jour des PCs avec des correctifs contre les crypto-virus, Europol a estimé que 200 000 appareils utilisant des logiciels obsolètes ont été infectés par WannaCry, et ce, dans 150 pays. Bien qu'il n'ait engendré que 130 000 dollars de rançon, son impact sur les entreprises aurait été beaucoup plus important : la perte de productivité due au matériel endommagé et à la perte de données auraient en effet couté aux entreprises plusieurs milliards de dollars.

Microsoft a mis fin au support de Windows 7 en 2015, donnant aux utilisateurs 5 ans pour se préparer à la fin de vie du logiciel.

Nous recommandons aux entreprises utilisant ce système d'exploitation de se préparer afin d'éviter toute vulnérabilité supplémentaire aux attaques par ransomwares, qui pourraient avoir à nouveau d'importantes conséquences sur leurs organisations. Voici 5 conseils pour bien se préparer :

Éduquez les employés - le plus grand risque concerne les données que les employés enregistrent à des emplacements non protégés. Assurez-vous que les utilisateurs connaissent et appliquent les bonnes pratiques concernant l'enregistrement des données afin qu'elles soient stockées en toute sécurité. Si ce n'est pas le cas, n'hésitez pas à organiser des sessions de formation ou de simulation. L'enregistrement des données importantes sur des stockages convenablement protégés va aider à réduire les risques.

Évaluez les risques en assurant la visibilité sur vos données - pour les entreprises, les solutions logicielles d'analyse peuvent aider à localiser les données clés et à s'assurer qu'elles sont conformes aux politiques de l'entreprise et aux réglementations sectorielles en vigueur. Cette visibilité est essentielle non seulement pour identifier les failles, mais aussi pour hiérarchiser le processus de récupération de données.

Envisagez une mise à jour logicielle - bien que difficile à mettre en oeuvre sur le court terme dans les grandes entreprises, une mise à jour logicielle est indispensable et doit s'inscrire dans une réelle stratégie à long terme. Concernant les PMEs, la solution la plus judicieuse pourrait simplement être de passer à un système d'exploitation sous support de son éditeur.

Installez les correctifs régulièrement - selon le Ponemon Institute, 60% des personnes interrogées ont déjà subi des attaques alors qu'un correctif était disponible et aurait pu les prémunir. Les entreprises doivent s'assurer de la mise à jour des systèmes aussi souvent que possible. Dans le cas d'impossibilité de mise à jour, ou pendant les phases de moigration, les utilisateurs peuvent également acheter des extensions de mises à jour de sécurité.

Assurez-vous de la sauvegarde de vos données - le ransomware repose sur l'idée que seul le paiement d'une rançon pourra permettre de récupérer les données en limitant les coûts. Cependant, les études montrent que moins de la moitié des victimes réussissent à récupérer leurs données. A

partir de ce constat, nous préconisons la règle dite des « 3,2,1 » : ayez 3 copies intégrales de vos données, stockez-en 2 sur des stockages différents et 1 sur un stockage hors site. Grâce au stockage hors-site, les entreprises ont ainsi une option plus fiable en cas d'attaque que la restauration de données locales.

WannaCry est un parfait exemple des dangers auxquels doivent faire face les entreprises lorsqu'elles utilisent des logiciels en fin de vie. En janvier 2020, un quart de l'ensemble des PCs seront particulièrement exposés. Il est essentiel pour les entreprises qui utilisent encore Windows 7 de connaître les risques auxquels elles sont exposées, mais aussi ce dont elles ont besoin pour les limiter. Ces attaques par ransomwares ont généralement un effet délétère sur les entreprises qui n'ont pas la possibilité de payer les rançons, comme c'est notamment le cas des institutions publiques. Il devient indispensable pour les entreprises utilisatrices de Windows 7 d'agir dès maintenant et d'établir des stratégies pour se protéger.

Pour limiter tous risques, les entreprises se doivent d'avoir une réelle visibilité sur leurs données pour s'assurer qu'elles sont stockées au bon endroit, de manière sécurisée, tout en restant accessibles aux utilisateurs.