Windows 10 et Surface Pro classifiés par la NSA

Microsoft va profiter de la RSA Conference, qui se déroule à San Francisco cette semaine (du 13 au 17), pour détailler les efforts que l'éditeur porte sur le développement de Windows en matière de sécurité. Pas moins de six points ont ainsi été présentés par Bob Lefferts, directeur de la gestion des programmes de Windows Enterprise and Security, en amont de la conférence. *« Notre objectif est de créer une plate-forme de sécurité holistique et agile, alimentée par le cloud, qui garantit une meilleure sécurité à nos clients – et à l'infrastructure de Microsoft – partout dans le monde »*, rappelle le responsable sur son billet de blog.

Une volonté qui se révèle déjà payante puisque Windows 10 et les terminaux Surface, modèles Pro 3, Pro 4 et Book, ont été retenus dans la liste des appareils que la NSA (National Security Agency) approuve pour des usages classifiés. Distinction d'autant intéressante à mettre en avant que les Surface sont les seuls terminaux mobiles équipés de Windows 10 à figurer dans la sélection de l'agence de sécurité américaine. En revanche, celles sous Android ne manquent pas tant chez LG que Samsung. Notons que les iPhone et iPad équipés d'un processeur A7, A8 et A8X sous iOS 9 y figurent également.

Oublier les mots de passe

Si la sécurité qui accompagne intrinsèquement l'OS et son terminal est quasiment indispensable, la capacité à pouvoir la gérer de manière simple est fortement appréciable. Sur ce point, Bob Lefferts se réjouit d'annoncer SEMM (Surface Enterprise Management Mode). *« SEMM permet à une organisation de prendre en charge, de modifier, de verrouiller et de contrôler la configuration matérielle, la sécurité et les comportements OS dans le firmware du périphérique »*, indique le responsable. Autrement dit, une solution pour activer ou désactiver la caméra, le Wifi, les ports USB, le lecteur de carte micro SF, les micros, le clavier TypeCover et autres périphériques selon des scénarios d'usage. Pratique pour interdire certaines fonctions de la tablette-PC en dehors du réseau de l'entreprise, par exemple, ou de bloquer son usage en cas d'échec d'authentification de l'utilisateur. La solution est déjà utilisée par des entreprises dans la santé, les services financiers ou du renseignement. Une offre qui devrait donc attirer l'attention des RSSI.

Autre point intéressant, la disparition de l'usage du mot de passe *« qui reste l'un des plus grands problèmes de sécurité auxquels nos clients sont confrontés aujourd'hui »* grâce à Windows Hello. Jusqu'à présent, le système d'identification biométrique était couplé au service Cloud d'Azure Active Directory. Avec Creators Update, l'imminente prochaine version majeure de Windows 10, Windows Hello fonctionnera aussi sur les environnements locaux avec Active Directory. Mais surtout, Microsoft s'appuiera sur les technologies d'Intel pour automatiser la sécurité des postes de travail. Dynamic Lock, qui permet de fermer une session lorsque son utilisateur n'est plus à proximité de sa machine, vient ainsi enrichir Windows Hello. Les premières machines équipées de la technologie d'authentification d'Intel devraient faire leurs premiers pas vers la fin de l'année.

Détecter les attaques anciennes

Creators Update va également enrichir Windows Defender Advanced Threat Protection (WDATP), l'outil de détection des menaces du système. Les utilisateurs auront désormais la possibilité d'ajouter des règles de détection personnalisées et d'effectuer celles-ci sur des données vieilles de six mois. *« Cela aide les clients à découvrir des attaques passées inaperçues »*, souligne le responsable de Microsoft. Il ajoute que WDATP sera déployé sur d'autres plates-formes, à commencer par Windows Server.

Enfin, à Sans Francisco, Microsoft reviendra sur Update Compliance. Le service de télémétrie qui mesure la conformité des mises à jour jusqu'alors disponible en *preview*, viendra enrichir Windows Analytics, l'outil de gestion de parc des terminaux Windows. Autant de nouveaux points qui devraient attirer l'attention des responsable sécurité des entreprises.

Lire également
Verrouillage et mode PiP pour Windows 10 Creators Update
Plus de vulnérabilités pour Windows 10 que Windows 7 en 2016
Comment Windows 10 Anniversary Update a détourné deux attaques zero day

crédit photot © Nikuwka – shutterstock