Fin du support de Windows XP : les solutions pour s'en sortir

Si vous lisez ces lignes depuis un ordinateur sous Windows XP, vous n'être certainement pas sans savoir que, après un ultime patch de sécurité, Microsoft a cessé le support de son OS phare de la précédente décennie (tout comme celui d'Office 2003). Autrement dit, l'éditeur **n'assure plus l'édition des correctifs de sécurité**. Seules les mises à jour des signatures de son antivirus Microsoft Essentials sont prolongées jusqu'au 14 juillet 2015.

Avec plus de 29% du marché mondial (selon NetApp MarketShare), pas moins de 500 millions de systèmes seraient concernées dans le monde. Rappelons aussi que 95% des distributeurs automatiques de billets (DAB) tournent sous l'OS de Microsoft. Des particuliers, essentiellement, mais aussi les entreprises qui, faute d'intérêt, de moyens, de temps ou de compatibilité applicative, restent sous l'ère XP. Selon Forrester Research, cela concernerait **20% des organisations professionnelles**, avec des pointes à 23% dans le secteur public, la santé et la vente.

Risques d'attaque et de non conformité

Les risques sont pourtant énormes. A moins de ne pas se connecter à Internet (et encore ; des DAB ont été piratés localement depuis une clé USB dotée d'un programme malveillant), entreprises et particuliers s'exposent à laisser les cybercriminels pénétrer leurs machines et, derrière, le système informatique de l'organisation ouvrant ainsi l'accès aux données ou au contrôle de pans entiers de l'infrastructure.

Au-delà des risques de sécurité, les entreprises se confrontent à des problèmes de conformité. Déjà en octobre 2002, une jurisprudence de la cour d'Appel de Paris indiquait : *« une société qui ne respecterait pas l'obligation de sécurité se verrait **privée de tout recours contre la personne entrée illégalement** dans le système automatisé des données de l'entreprise. Le DSI peut alors être sanctionné pour faute grave »*, comme le rappelle **Adrien Wiatrowski**, consultant sécurité pour Lexsi. Autant dire que du *retail* à l'industrie en passant par la banque-assurance et la distribution, nombre de secteurs sont directement visés. En cas d'attaque de leur SI et de vols de données qui s'ensuivraient ou de déstabilisation de l'activité, les victimes pourront difficilement faire valoir qu'elles «□ne savaient pas□» que l'OS était faillible. Ainsi, les acteurs du secteur de la vente, dont les caisses enregistreuses tournent sous XP, risquent de **perdre leurs certifications PCI DSS** (Payment Card Industry Data Security Standard) si les terminaux deviennent vulnérables. Une conformité non garantie aussi dommageable pour l'entreprise que pour ses clients en cas d'attaque réussie.

Que faire pour se protéger□?

Face à ce risque, l'entreprise (et le particulier) a tout intérêt à migrer **vers un Windows plus à jour**. Ce qui représente un coût que le Gartner évalue **entre 1□274 à 2□069 dollars par poste** (pour 10□000 PC) et des délais de migration qui, selon le parc de machines, peuvent se compter en mois. Qui plus est, dans certaines industries sensibles comme l'énergie ou la Défense, les applications

doivent apporter une garantie de stabilité sur de très longues périodes. Un cadre contradictoire avec des migrations imposées.

Pour répondre à ce type de situation (et d'autres propres à chaque entreprise), Microsoft propose un support à la carte. Son **programme Custom Support** permet aux grands comptes (uniquement) de continuer à recevoir les patchs de sécurité. Une offre commercialisée **200 dollars (145 euros HT environ) par machine**, la première année, et le double chaque année suivante, rapporte notre confrère américain CIO. Une solution de transition qui prendra fin en 2017.

Une autre solution consisterait à **isoler les machines vulnérables dans une DMZ** (DeMilitarized Zone), où elles sont coupées d'Internet et du reste du réseau informatique de l'entreprise. Ce qui ne se relève pas forcément pertinent en matière de production. **L'éditeur vSentry** propose pour sa part une solution visant à virtualiser chaque tâche utilisateur à travers des micro machines virtuelles. En cas d'attaque, l'application resterait isolé du reste du système (CPU, mémoire et réseau) et le malware serait supprimé à la fermeture de la tâche, à l'image de ce qui se passe avec les technologies dites de bac-à-sable (sandbox).

Autre offre, celle de **Arkoon-Netasq** qui propose **ExtendedXP** aux entreprises pour qui la migration vers Windows 7 ou 8 n'est pas à l'ordre du jour. ExtendedXP combine protection contre les failles non patchées (technologie d'analyse comportementale HIPS – Host-based Intrusion Prevention System – de StormShield) et service de veille et d'alerte sur les nouvelles vulnérabilités publiées. Autant de solutions néanmoins complexes à mettre en œuvre techniquement qui ne peuvent s'inscrire que dans une stratégie de transition. En attendant, si XP n'est pas supporté, il n'en reste pas moins vivement recommandé de continuer les mises à jour de l'ensemble des logiciels de base présents sur la machine, des navigateurs aux environnements Flash ou Java en passant par les suites bureautiques.

crédit photo © Robert Hoetink – shutterstock

Lire également

À cinq jours de sa mise à mort, Windows XP reste le second OS desktop au monde
De profundis Windows XP ! (quiz)