COMMUNIQUÉ DE PRESSE - *08 octobre 2021*

Empreinte environnementale et sécurité des logiciels Microsoft

Le 5 octobre 2021, Microsoft a lancé officiellement la nouvelle version de son système d'exploitation phare, Windows 11. Nos quatre associations, Beltug, Cigref, CIO Platform Nederland et VOICE saisissent cette occasion pour appeler l'éditeur à mettre en cohérence son discours public et la réalité de sa politique commerciale. D'une part, alors que Microsoft communique largement sur ses engagements en matière de *sustainability*, **le cycle de vie de ses produits et services provoque une implacable logique d'obsolescence programmée de parcs d'équipements parfaitement fonctionnels**. D'autre part, Microsoft, comme de nombreux autres éditeurs, **fait reposer sur les seuls utilisateurs la gestion des vulnérabilités de ses produits et services**. En raison de sa position de leader du marché des produits et services numériques aux entreprises, nos associations attendent de la part de Microsoft un comportement exemplaire en matière d'empreinte environnementale et de sécurité.

Une politique de montées de version de Windows et d'Office qui accélère le remplacement des postes de travail en entreprise

Microsoft lance régulièrement sur le marché de nouvelles versions de ses logiciels et arrête la maintenance des versions antérieures au terme d'une période de cohabitation, période jugée beaucoup trop brève par les entreprises utilisatrices.

Outre le caractère contestable de ces montées de version au regard de la valeur qu'elles apportent au client, **l'installation de ces nouveaux logiciels requiert des performances matérielles plus importantes.** Elles engendrent ainsi la mise au rebut de parcs entiers d'ordinateurs parfaitement fonctionnels.

Le déploiement progressif de Windows 11 en entreprise engendrera le remplacement des ordinateurs de plus de 3-4 ans, en raison de la puissance de calcul et la mémoire vive requises pour fonctionner (puce Trusted Platform Module - TPM en version 2.0 et 4Go de RAM contre 2Go précédemment).

Cette stratégie de remplacement accéléré des logiciels garantit à Microsoft une croissance mécanique de son chiffre d'affaires dans un marché déjà bien équipé. Ces montées de version sont majoritairement adoptées par les utilisateurs professionnels car le support des versions antérieures du logiciel n'est plus assuré au bout de quelques années.

Les membres de nos associations considèrent que la politique de versioning logiciel de Microsoft participe de l'obsolescence matérielle et logicielle programmée, en contradiction avec le discours et les engagements de développement durable et de numérique responsable du fournisseur :

- ➔ Nos associations demandent à Microsoft de garantir à ses clients le maintien des services de support et des correctifs de sécurité sur ses logiciels sans limitation de durée, et ce, en contrepartie d'un effort financier raisonnable pour le client. Le Cigref soutient par ailleurs la proposition de loi Chaize, en cours de relecture par le Sénat et l'Assemblée nationale, de dissocier les mises à jour de sécurité des mises à jour fonctionnelles. Cette demande était déjà formulée par le Cigref et ses associations sœurs belge et néerlandaise dans leur communiqué de presse d'avril 2020 : *« Minimizing patch management in crisis situation: call from digital service user associations to major providers »*

- ➔ En l'absence d'engagement de Microsoft à assurer la maintenance de ses produits et services, nos associations demandent à l'éditeur de s'engager à permettre à des organismes tiers de les maintenir au profit des utilisateurs n'ayant pas d'intérêt fonctionnel à changer de version.

CONTACT PRESSE
Baptiste CHAUVEAU - Chargé de communication & RP - bchauveau@cigref.fr - +33 6 70 41 06 92

➔ Nos associations s'engagent auprès du régulateur européen pour que celui-ci prenne en considération les contraintes de renouvellement de matériels et d'infrastructures imposé aux utilisateurs professionnels de logiciels et services numériques, dans le cadre du Pacte Vert pour l'Europe. Le Cigref publiera prochainement des propositions d'engagement pour lutter contre le phénomène d'obsolescence logicielle et matérielle à l'intention des fournisseurs.

Une sécurité intrinsèque insuffisante et un effort correctif à la charge des clients

Nos associations demandent **que les produits et services numériques - notamment les logiciels - qui entrent sur le marché européen soient manifestement sûrs et répondent à des normes de sécurité numérique.** Comme toutes les autres industries (agroalimentaire, pharmaceutique, chimique, équipements électriques, automobile, etc.), l'industrie des produits et services numérique doit être soumise à de telles normes afin que la responsabilité ne repose pas exclusivement sur l'utilisateur professionnel et puisse être partagée avec le fournisseur en cas de défaut de conception et de maintien en condition de sécurité.

Cette position des utilisateurs a été récemment exprimée par VOICE, l'association des organisations utilisatrices allemandes, dans un communiqué de presse : *« Stratégie de cybersécurité du gouvernement fédéral : VOICE appelle à une plus grande responsabilité de la part des fournisseurs de logiciels et des fournisseurs de cloud ».*

L'absence d'obligation de sécurité native des produits et services numériques engage les éditeurs dans des stratégies systémiques de publication de correctifs de sécurité. En particulier, l'effort de *patching*, c'est-à-dire la vérification et le déploiement sur tout le parc informatique des correctifs de sécurité de Microsoft, représente une mobilisation croissante de ressources chez les clients de l'éditeur pour pallier les défauts de qualité et de sécurité de ses produits et services.

À titre d'exemple, une entreprise disposant de 150 000 collaborateurs dans le monde et l'équivalent en licences Office 365, mobilise en moyenne une quinzaine d'ETP/an pour réaliser les opérations courantes de corrections des failles de sécurité des logiciels et de la console de contrôle de Microsoft. Cela équivaut à une dépense moyenne supérieure à 1 million d'euros/an, à la charge du client, pour compenser les failles de sécurité intrinsèques des produits de Microsoft. Plus récemment, la gestion de la faille dite « PrintNightmare » a représenté à elle seule 300 jours x hommes à la DSI de cette société.

Les membres de nos associations dénoncent les défauts intrinsèques de qualité et de sécurité des produits et services de Microsoft, qui contraignent ses clients à des efforts croissants :

➔ Nos associations demandent à Microsoft de prendre ses responsabilités, en termes de garantie constructeur, et de participer aux surcoûts engendrés par sa politique de correctifs de sécurité.

➔ Nos associations rappellent qu'elles s'engagent auprès du régulateur européen pour que celui-ci se saisisse des recommandations en la matière du rapport de l'OCDE publié le 9 février 2021, présentant une boîte à outil des politiques publiques en faveur du renforcement de la sécurité des produits et services numériques.

Associations d'utilisateurs de services numériques, Beltug, Cigref, CIO Platform Nederland et VOICE représentent ensemble plusieurs milliers d'organisations privées et publiques en Belgique, en France, aux Pays-Bas et en Allemagne.

CONTACT PRESSE
Baptiste CHAUVEAU - Chargé de communication & RP - bchauveau@cigref.fr - +33 6 70 41 06 92