Beltug Cigref SUCCEED WITH DIGITAL CIO PLATFORM NEDERLAND VOICE Bundesverband der IT-Anwender e.V.

PRESS RELEASE - 08 October 2021

Environmental footprint and security of Microsoft software

On 5 October 2021, Microsoft officially launched the new version of its flagship operating system, Windows 11. Our four associations, Beltug, Cigref, CIO Platform Nederland and VOICE are taking this opportunity to call on the software editors to bring its public discourse into line with the reality of its commercial policy. On the one hand, while Microsoft communicates widely on its commitment to sustainability, **the life cycle of its products and services leads to a relentless logic of programmed obsolescence of perfectly functional equipment.** On the other hand, Microsoft, like many other vendors, **places the management of vulnerabilities in its products and services solely on the users.** Because of its position as market leader in digital products and services for businesses, our associations expect Microsoft to behave in an exemplary manner in terms of environmental footprint and security.

A policy of version upgrades for Windows and Office that accelerates the replacement of workstations in companies

Microsoft regularly launches new versions of its software on the market and stops maintaining previous versions at the end of a cohabitation period, a period that user companies consider to be far too short.

In addition to the questionable nature of these version upgrades with regard to the value they bring to the customer, **the installation of these new software products requires greater hardware performance.** This results in the scrapping of entire fleets of perfectly functional computers.

The progressive deployment of Windows 11 in companies will lead to the replacement of computers that are more than 3-4 years old, due to the computing power and RAM required to operate (Trusted Platform Module - TPM chip in version 2.0 and 4GB of RAM compared to 2GB previously).

This strategy of accelerated software replacement guarantees Microsoft a mechanical growth in turnover in a market that is already well equipped. These version upgrades are mainly adopted by professional users because support for earlier versions of the software is no longer guaranteed after a few years.

Our associations' members consider that Microsoft's software versioning policy contributes to programmed hardware and software obsolescence, in contradiction with the vendor's statements and commitments to sustainable development and responsible digital technology:

- ➔ Our associations call on Microsoft to guarantee its customers continued support services and security patches for its software without time limits, in return for a reasonable financial effort on the part of the customer. Cigref, the French association, also supports the Chaize bill, currently being reviewed by the French Senate and the National Assembly, to separate security updates from functional updates. This request was already made by Cigref and its Belgian and Dutch sister associations in their April 2020 press release: "*Minimizing patch management in crisis situation: call from digital service user associations to major providers*"

- ➔ In the absence of a commitment from Microsoft to maintain its products and services, our associations ask the editor to commit to allowing third-party organisations to maintain them for the benefit of users who have no functional interest in changing versions.

- ➔ Our associations are working with the European regulator to ensure that it takes into consideration the hardware and infrastructure renewal constraints imposed on professional users of digital software and services, as part of the Green Pact for Europe. Cigref will soon publish proposed commitments for suppliers to combat the phenomenon of software and hardware obsolescence.

Insufficient intrinsic security and a corrective effort on the part of customers

Our user associations call for digital products and services - including software - entering the European market to be demonstrably safe and to meet digital safety standards. Like all other industries (food, pharmaceutical, chemical, electrical equipment, automotive, etc.), the digital products and services industry must be subject to such standards so that the responsibility does not rest exclusively on the professional user and can be shared with the supplier in the event of a design and safety maintenance defect.

This user position was recently expressed by VOICE, the German association, in a recent press release: "Federal government cybersecurity strategy: VOICE calls for greater responsibility on the part of software and cloud providers".

The absence of a native security obligation for digital products and services is leading editors to adopt systemic strategies for publishing security patches. In particular, the patching effort, i.e. the verification and deployment of Microsoft's security patches across the entire computer population, represents a growing mobilisation of resources on the part of the editor's customers to compensate for the quality and security defects of its products and services.

For example, a company with 150,000 employees worldwide and the equivalent in Office 365 licences, mobilises an average of fifteen FTEs/year to carry out the routine operations of correcting security flaws in Microsoft software and control console. This is equivalent to an average expenditure of more than 1 million euros/year, at the customer's expense, to compensate for the by-design security flaws in Microsoft's products. More recently, the management of the so-called "PrintNightmare" flaw alone represented 300 man-days for the company's IT department.

Our members denounce the intrinsic quality and security shortcomings of Microsoft's products and services, which force its customers to make increasing efforts:

- ➔ Our associations call on Microsoft to assume its responsibilities, in terms of manufacturer's warranty, and to contribute to the additional costs generated by its security patch policy.
- ➔ Our associations reiterate their commitment to the European regulator to take up the recommendations of the OECD report published on 9 February 2021, which presents a toolbox for public policies to strengthen the security of digital products and services.

Beltug, Cigref, CIO Platform Nederland and VOICE represent several thousand private and public organisations in Belgium, France, the Netherlands and Germany that use digital services.

PRESS CONTACT
Baptiste CHAUVEAU - Communication & PR Officer - bchauveau@cigref.fr - +33 6 70 41 06 92