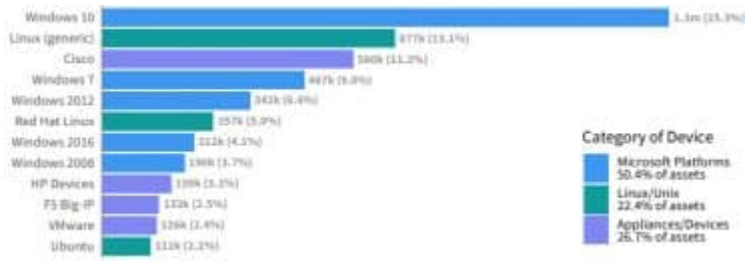
Cybersécurité : comment mesurer le profil de risque d'une infrastructure IT ?

Les infrastructures IT présentent-elles un profil de risque d'autant plus élevé qu'elles sont riches en systèmes Windows ? Tout dépend comment on appréhende la gestion dudit risque.

Le constat ressort d'une étude que l'entreprise américaine Cyentia a menée pour le compte de sa compatriote Kenna Security.

Celle-ci, spécialisée dans la gestion des vulnérabilités, a fourni des données importées sur sa plate-forme par « près de 450 organisations ».

Les quelque 9 millions d'actifs informatiques concernés* reposent en majorité sur un OS Windows. 50,4 %, en l'occurrence, dont environ la moitié sous Windows 10.
Un peu plus d'un quart sont des équipements réseau (26,7 %, dont environ 40 % de produits Cisco).
Les systèmes Linux/Unix représentent 22,4 % de l'échantillon ; les Mac, 0,5 %.



Windows : quantité de failles…

L'essentiel des résultats de l'étude sont délivrés sous le prisme de ces quatre catégories. À commencer par l'indicateur dit de « densité ». Il correspond au nombre moyen de vulnérabilités détectées par actif informatique, chaque mois sur un intervalle de deux ans.
La médiane sur les systèmes Windows est de 119. Elle s'élève à 32 sur Mac, à 7 sur Linux/Unix et à 4 sur les équipements réseau.

Plus importante, d'après Kenna Security, est la présence de vulnérabilités « à haut risque ». 71,6 % des systèmes Windows examinés en hébergeaient au moins une non corrigée, contre 40,8 % pour Linux/Unix, 31,4 % pour Mac et 30,5 % pour les solutions réseau.

En entrant dans les détails des plates-formes, c'est sur Windows 7 que la médiane de failles à haut risque est la plus haute : 18 par actif. On en est à 14 sur Windows 10, à 10 sur Windows Server 2008, à 5 pour Windows Server 2006, etc.

La densité apparaît plus grande côté client que côté serveur. Quant à la présence de Red Hat Linux Enterprise dans le haut du panier (médiane de 8), Kenna Security l'impute au nombre de logiciels tiers installés : la médiane est à 41 sur ces systèmes, contre une dizaine sur Windows.

… mais aussi de correctifs

Si les failles sont plus nombreuses sur les environnements Windows, elles se corrigent aussi nettement plus vite. Le délai médian pour corriger 50 % des failles constatées à un instant T est de 36 jours. Sur Mac, il faut 70 jours pour atteindre ce seuil, contre 254 sur Linux et 369 sur les équipements réseau.

Concernant les environnements Windows, 68 % des failles « natives » (liées à des composants Microsoft) sont éliminées sous 30 jours. Le taux baisse à 30 % pour les failles « non natives ».
Il devient toutefois beaucoup plus difficile de corriger les vulnérabilités dès lors qu'un OS Windows arrive en fin de vie.

Les auteurs de l'étude avancent deux explications eu égard au contraste avec Linux/Unix. D'un côté, des outils moins efficaces pour la gestion des parcs. De l'autre, des administrateurs moins rompus aux redémarrages de systèmes.

Autre indicateur : la capacité de remédiation. En d'autres termes, dans quelle mesure on est capable de colmater davantage de failles qu'on n'en découvre.

La proportion médiane de vulnérabilités éliminées chaque mois sur les systèmes Windows atteint 25,3 %. OS X suit à 22,6 %, devant Linux/Unix (10,2 %) et les équipements réseau (9,4 %).
Sur l'ensemble de ces catégories d'actifs, le ratio est positif. Même s'il est plus difficile de suivre le rythme sur Windows, au vu du nombre d'actifs et de failles.

** Tous ces actifs sont, par définition, intégrés dans un programme de gestion des vulnérabilités. Certains environnements ont tendance à y échapper, comme le cloud, les* datacenters *en production et les appareils mobiles (moins de 0,1 % de l'échantillon).*

Illustration principale © Isak55 – Shutterstock.com