

Mises à jour : pourquoi elles n'attendent pas

Chaque mise à jour repoussée est une faille connue laissée ouverte. Comment s'organiser sans subir.

9 min de lecture · Niveau Essentiel · cyberionis.fr/ressources/mises-a-jour

La majorité des attaques réussies exploitent des failles... déjà corrigées par les éditeurs. Repousser une mise à jour, c'est laisser ouverte une porte dont les cambrioleurs ont le plan.

1. Ce qu'il faut maintenir à jour

- Systèmes d'exploitation (Windows, macOS, Linux) des postes et serveurs
- Navigateurs et clients de messagerie
- Logiciels métier, antivirus/EDR
- Smartphones et tablettes professionnels
- Équipements réseau : box, routeurs, pare-feu, NAS, imprimantes
- Site web : CMS (WordPress...), extensions et thèmes

2. S'organiser sans casser la production

Activez les mises à jour automatiques partout où c'est possible pour les postes de travail. Pour les serveurs et logiciels métier sensibles, planifiez une fenêtre de maintenance régulière (par exemple un soir par mois) avec sauvegarde préalable — ainsi une mise à jour problématique se rattrape sans stress.

Attention au matériel en fin de vie : un système qui ne reçoit plus de correctifs (Windows obsolète, vieux NAS...) est une faille permanente. Planifiez son remplacement ou isolez-le du réseau.

3. Savoir quand une faille est critique

Toutes les failles ne se valent pas. Certaines, activement exploitées, imposent d'agir dans la journée : ce sont celles qui font l'objet d'alertes du CERT-FR (l'organisme d'État qui publie les bulletins de sécurité). S'abonner à ses alertes — ou déléguer cette veille à votre prestataire — permet de distinguer la mise à jour de routine de celle qui n'attend pas la fenêtre de maintenance mensuelle.

4. Gérer la fin de vie des systèmes

Tout logiciel et tout matériel a une date de fin de support, après laquelle plus aucune faille n'est corrigée. Continuer à l'utiliser tel quel revient à accumuler des vulnérabilités connues de tous.

- Inventorier les dates de fin de support de vos systèmes critiques (Windows, serveurs, NAS, pare-feu) et les inscrire au budget avant l'échéance
- Si un système obsolète est irremplaçable (machine industrielle pilotée par un vieux Windows, logiciel métier abandonné) : l'isoler du réseau et d'Internet, et compenser par une surveillance renforcée
- Attention aux équipements « invisibles » : imprimantes, caméras, box et objets connectés ont aussi des

CAS CONCRET

Les grandes épidémies de ransomware de l'histoire (WannaCry, NotPetya) exploitaient une faille Windows corrigée des semaines ou des mois plus tôt. Les centaines de milliers de victimes avaient un point commun : la mise à jour disponible, mais pas appliquée.

L'essentiel à retenir

- 01 Activer les mises à jour automatiques sur tous les postes
 - 02 Planifier une fenêtre de maintenance mensuelle pour les serveurs
 - 03 Sauvegarder avant toute mise à jour majeure
 - 04 Mettre à jour le CMS et les extensions du site web chaque mois
 - 05 Inventorier les équipements qui ne reçoivent plus de correctifs
 - 06 Isoler du réseau ce qui ne peut plus être mis à jour
 - 07 Organiser une veille sur les failles critiques (alertes CERT-FR)
-

Questions fréquentes

Une mise à jour peut-elle casser mes logiciels métier ?

C'est possible, surtout sur les serveurs — c'est pourquoi on distingue : mises à jour automatiques immédiates sur les postes et navigateurs (risque très faible, gain immédiat), et fenêtre de maintenance planifiée avec sauvegarde préalable pour les serveurs et applications sensibles. Le risque d'une mise à jour se rattrape ; celui d'une faille exploitée, rarement.

Windows me propose une mise à jour en pleine journée, que faire ?

Configurez les heures d'activité pour que les redémarrages aient lieu la nuit — et surtout, ne repoussez pas indéfiniment. Un redémarrage de 10 minutes planifié vaut mieux qu'un poste vulnérable pendant des semaines.

Comment savoir si une faille est « critique » pour nous ?

Trois questions : le logiciel concerné est-il chez nous ? Est-il exposé à Internet (VPN, pare-feu, messagerie, site web) ? La faille est-elle activement exploitée (les alertes CERT-FR le précisent) ? Trois oui = on met à jour dans la journée, pas à la prochaine fenêtre de maintenance.

Qui doit s'occuper des mises à jour dans une petite structure ?

L'automatisation fait 80 % du travail sans personne. Pour le reste (serveurs, équipements réseau, site web, veille), désignez un responsable interne ou déléguez à un prestataire via un contrat de maintenance — c'est typiquement le genre de tâche récurrente qui se sous-traite bien.

Pour aller plus loin

CERT-FR — alertes de sécurité de l'ANSSI — www.cert.ssi.gouv.fr/alerte/

Cybermalveillance.gouv.fr — bonnes pratiques de mises à jour — www.cybermalveillance.gouv.fr/tous-nos-contenus/bonnes-pratiques/mises-a-jour

Besoin d'aide pour le mettre en place ?

Audit, durcissement, accompagnement : Cyberionis sécurise les TPE, PME et collectivités, à Nancy, Lure et à distance.

contact@cyberionis.fr · 06 64 90 07 74 · cyberionis.fr