La gestion des correctifs dans les PME

L'installation des mises à jour de sécurité est une mesure efficace pour corriger les vulnérabilités des systèmes numériques complexes. Une bonne gestion des correctifs permet leur déploiement à l'échelle de toute l'entreprise.

Principales informations à connaître :

- Définissez des plages horaires en dehors du temps de production pour l'entretien des systèmes.
- Les mises à jour de sécurité doivent provenir exclusivement de sources sûres.
- Vérifiez l'efficacité et les éventuels « effets secondaires » des mises à jour avant de les installer sur l'ensemble des systèmes productifs.
- Établissez un plan pour le déploiement des mises à jour sur vos systèmes.
- Assurez-vous de disposer toujours d'une sauvegarde actuelle et d'un plan B en cas de mauvaise surprise lors de la mise à jour.
- Documentez les travaux de maintenance effectués sur les différents systèmes.

Les mises à jour de sécurité

Les systèmes informatiques évoluent à une vitesse folle : les fonctionnalités des applications ne cessent d'augmenter et les cycles de vie des logiciels et du matériel informatique de raccourcir. C'est pour cette raison que les fabricants s'efforcent de mettre rapidement leurs dernières trouvailles en circulation à travers le système des mises à jour.

Dans le cas des PME, il convient cependant d'exercer une certaine prudence, dans la mesure où toutes les nouveautés ne pourront pas forcément être appliquées efficacement sur les processus opérationnels. La seule exception stricte concerne toutefois les mises à jour de sécurité qui doivent pour le coup être installées dans les plus brefs délais.

Tout système complexe recèle des erreurs cachées ou des failles. Celles-ci restent la plupart du temps inaperçues et donc sans conséquence. Une fois découvertes, elles se transforment en de véritables défaillances (que l'on appelle en langage informatique des **vulnérabilités**) et la course contre la montre commence avec les hackers d'une part, et les fabricants de l'autre.

Les premiers vont essayer de trouver le moyen d'exploiter ces failles pour leurs propres desseins et mettre au point les fameux **exploits**. C'est ainsi qu'en cas de réussite, ils parviennent à pirater des systèmes et des données.

Les fabricants travaillent quant à eux à l'élaboration de mises à jour de sécurité ou de correctifs visant à corriger les failles le plus vite possible et de les publier avant que les hackers n'aient eu le temps d'exploiter leurs exploits, voire même de les mettre au point.

La gestion des correctifs

En règle générale, les mises à jour de sécurité devraient être systématiquement installées et ce dans les délais

les plus brefs. Mais ce qui est ordinairement facile à réaliser sur un système privé autonome peut s'avérer plus compliqué dès lors qu'il s'agit de l'appliquer dans le contexte d'une PME, d'où la nécessité de disposer d'une procédure claire et structurée pour la gestion des correctifs.

Voici donc les différentes étapes à suivre pour l'installation des mises à jour de sécurité :

- identifier les systèmes concernés et des mises à jour de sécurité adaptées
- se procurer les mises à jour auprès d'une source fiable, notamment pour les systèmes ne disposant pas d'un accès direct à Internet.
- tester à l'avance l'efficacité et les éventuels « effets secondaires » des mises à jour de sécurité sur des systèmes non stratégiques.
- distribuer les mises à jour en fonction de la typologie des systèmes et planification de leur installation en dehors du temps de travail.
- pour les systèmes stratégiques : prévoir des solutions de rechange temporaires et des alternatives.
- documenter les modifications apportées.

Dans la mesure où il s'agit d'un processus qui se déroule en continu, il est recommandé de définir des plages horaires fixes et régulières pour les opérations de maintenance des systèmes. Les mises à jour de sécurité peuvent ainsi être collectées, vérifiées et préparées pendant une période de temps donnée, tandis que leur installation pourra être reportée à la prochaine fenêtre de temps disponible.

La gestion des correctifs de sécurité consiste à se procurer, tester et installer les mises à jour logicielles. L'objectif principal est de réparer les failles de sécurité présentes au niveau du système d'exploitation et des applications.

Pour en savoir plus

Plusieurs facteurs concourent à identifier les systèmes concernés et les mises à jour de sécurité adaptées. L'équipement informatique (hardware) lui-même joue un rôle. Dans ce cas, il s'agit principalement d'actualiser le firmware (ou micrologiciel) intégré dans le matériel informatique. Viennent ensuite le système d'exploitation et les applications installées sur le dispositif, pour lesquels il est nécessaire de vérifier la disponibilité de nouvelles mises à jour.

Pour les systèmes dotés d'une connexion directe à Internet, il existe des solutions automatisées qui dressent régulièrement un inventaire du matériel et des logiciels, puis recherchent en ligne les mises à jour disponibles. Dans les PME, ces systèmes devraient être tout au plus utilisés comme support, l'installation non supervisées des mises à jour étant en revanche fortement déconseillée. Un technicien devrait d'ailleurs être toujours présent pour contrôler le processus d'installation.

La récupération des mises à jour de sécurité peut également s'avérer un exercice délicat, car les mises à jour les plus faciles à trouver sur Internet ne sont pas forcément les bonnes. Dans ce cas, le risque est que ces prétendues mises à jour de sécurité véhiculent en réalité l'exploit qu'elles sont censées éviter pour l'introduire dans le système. Il convient donc, dans la mesure du possible, de toujours faire référence aux canaux de distribution officiels des fabricants.

Avant d'installer une mise à jour sur un système productif, voire stratégique, il convient par ailleurs de s'assurer qu'elle est compatible avec le système en question et avec son environnement. Il s'agit idéalement de tester l'efficacité et la présence éventuelle d'« effets secondaires » dans un environnement isolé et non productif. Or ce type d'environnement est rarement disponible dans les PME.

Il est donc recommandé de procéder graduellement à l'installation des mises à jour de sécurité en commençant par les systèmes les moins essentiels à l'activité de l'entreprise. Ce n'est qu'après une certaine période d'observation donnée et quelques tests qu'elles pourront être ensuite déployées sur les autres systèmes.

Des plages horaires suffisamment larges devraient être réservées en dehors des périodes de production pour l'installation des mises à jour, en particulier pour les systèmes stratégiques. Il convient également de prévoir des scénarios alternatifs passant notamment par des sauvegardes (https://www.ebas.ch/fr/la-sauvegarde-des-donnees-dans-les-pme/) ou autres solutions de rechange pour pouvoir réagir en cas d'échec de l'installation des mises à jour.

Les étapes du processus de mise à jour devraient par ailleurs être clairement explicitées dans un document. Un tel outil permettrait en effet de fournir des informations importantes sur les causes du problème dans le cas d'un dépannage successif.