



Article de Mathieu Grignon
Directeur des services de sécurité
ESI Technologies

Gestion des rustines : casse-tête pour les entreprises

De plus en plus d'entreprises se demandent comment s'y prendre pour faciliter la gestion fort complexe des correctifs s'appliquant aux divers logiciels qu'elles utilisent. Appelés rustines - ou patches en anglais - ces programmes de correction se multiplient au même rythme que les vulnérabilités affectant le monde de l'informatique. En 2002, celles-ci ont été dénombrées à 4000 par le CERT Coordination Center, organisme voué à la sécurité Internet et administré par la très sérieuse université Carnegie Mellon. Au cours du premier trimestre de cette année uniquement, le CERT en avait déjà rapporté 900.

De tels chiffres mettent les administrateurs de système dans l'obligation d'examiner quotidiennement une dizaine de problèmes potentiels. Normalement, une proportion élevée des rustines proposées ne s'applique pas à l'environnement d'une organisation, soit parce qu'elle n'utilise pas les fonctions considérées comme vulnérables, soit parce que ne sont pas réunies les conditions permettant à la menace de se concrétiser. Malgré tout, l'entreprise devra procéder à l'examen de chacune des rustines.

Méthode « manuelle »

Devant la prolifération des correctifs, l'application de ceux-ci au cas par cas représente une tâche herculéenne. Personnellement, la gestion des rustines requises pour les quelques ordinateurs utilisés par des membres de ma famille rapprochée m'apparaît très lourde. Inutile de dire le cauchemar que peut représenter une telle coordination au sein d'une entreprise comptant des centaines de postes de travail. Seules de très petites organisations pourront, exceptionnellement, s'en tirer de cette façon.

Le défi est d'autant plus grand que les rustines ne concernent pas que les seuls systèmes d'exploitation, mais les applications également. La plupart d'entre elles sont aujourd'hui munies de leur propre passerelle vers Internet afin de faciliter les communications externes. L'envers de la médaille est que les brèches de sécurité s'ouvrent plus facilement.

Les entreprises ayant recours à une méthode « manuelle » doivent s'en remettre à des membres du personnel des TI qui n'ont pas toujours la motivation nécessaire pour assumer cette responsabilité de manière fiable, ni ne sont pleinement conscients de l'impact que peut avoir cette question sur les affaires de l'entreprise.

Serveur de mise à jour de Microsoft

Une façon de s'en sortir est de faire appel au système de distribution des mises à jour de sécurité mis au point par Microsoft pour les utilisateurs de Windows. Il permet aux administrateurs de système de sélectionner les mises à jour s'appliquant à leur environnement et de les distribuer aux postes de travail de l'entreprise. Chaque utilisateur a la responsabilité de les installer, et peut choisir d'aller vérifier lui-même si des mises à jour sont disponibles ou d'obtenir un avis émis par le système.

Très efficace, cette méthode libère les administrateurs de la tâche fastidieuse consistant à déployer les rustines. Le hic, c'est que la solution ne s'applique qu'aux systèmes d'exploitation Windows. Elle ne peut servir à la distribution des rustines destinées aux divers autres programmes.

Logiciels de gestion des rustines

Heureusement, il existe aussi des logiciels de gestion pouvant aider les entreprises à sélectionner les correctifs et à les déployer. S'appliquant à de multiples domaines, et non pas seulement aux systèmes d'exploitation, les gestionnaires de rustines prennent donc en charge l'ensemble des programmes de correction de l'entreprise. Cette universalité, par contre, fait en sorte qu'ils perdent en précision lorsqu'on les compare au serveur de mises à jour de Microsoft.

Bien qu'il s'agisse d'un concept relativement nouveau, plusieurs gestionnaires de rustines sont offerts sur le marché. On peut les répartir entre ceux qui intègrent un agent logiciel et ceux qui n'en utilisent pas. L'agent permettra de délester le serveur en confiant le processus d'analyse au client, ce qui réduit l'incidence sur le trafic au sein du réseau. De plus, la plupart des agents autorisent une communication chiffrée entre le serveur et le client, conférant une sécurité accrue aux opérations de déploiement.

L'absence d'agent, d'autre part, facilite le déploiement, surtout au sein de parcs informatiques importants. Le niveau de sécurité n'est cependant pas aussi élevé, car un ou plusieurs ports du client doivent demeurer libres. Et comme la plupart des agents ont la capacité de faire un appel de procédure à distance, une porte est laissée entrouverte aux vulnérabilités connues qui, ironiquement, sont combattues par le gestionnaire de rustines même.

Il est important de s'assurer que la solution envisagée aide à déterminer les rustines faisant défaut sur chaque système; qu'elle procure un moyen facile de déployer les correctifs applicables; et qu'elle produit des rapports permettant de contrôler les correctifs installés sur chaque poste de travail.

Les gestionnaires de rustines sont en pleine évolution. Les entreprises recherchent les services offerts par ces programmes, mais ne les ont pas encore adoptés massivement. Il est à prévoir que certains joueurs disparaîtront dans les années à venir et que les solutions offertes gagneront en efficacité.

Facteurs à considérer

Le choix de la solution convenant à l'entreprise dépendra évidemment du cadre d'exploitation. En priorité, la rentabilité devrait servir de critère dans cette décision. Une organisation pour qui la majorité des rustines concerne les systèmes Windows pourrait opter pour le serveur de mises à jour de Microsoft. Une telle solution, par contre, ne saurait servir les intérêts d'une entreprise exploitant un réseau hybride qui intègre à la fois Windows et Linux, par exemple. Les firmes proposant des gestionnaires de rustines exigent normalement une redevance pour le permis d'utilisation de chaque poste client. Parfois, des frais s'ajoutent pour les mises à jour. La facture se situe entre 20 \$ et 30 \$ par poste de travail.

Les administrateurs ne doivent pas négliger l'importance de soumettre les rustines à une évaluation rigoureuse. Ce principe de base permettra d'abord de s'assurer que des correctifs importants ne sont pas oubliés. Il fera en sorte également d'éviter que des mises à jour inutiles soient installées, réduisant du coup le risque de perturbation des systèmes.

Toute rustine peut potentiellement mettre en danger le fonctionnement harmonieux des opérations informatiques. Pour cette raison, il est souhaitable de disposer d'un environnement d'essai avant des les appliquer aux systèmes de production. Toutefois, la mise en place d'un environnement constituant un miroir parfait de celui qui est utilisé en mode production pose problème. Non seulement sera-t-il ardu de le reproduire avec précision, mais la facture qui en résulte peut être particulièrement élevée. Certains cadres d'exploitation se prêtent mieux à la création d'un environnement d'essai, par exemple un parc de serveurs, dont l'architecture est plus statique. Autre possibilité : réserver quelques machines devant servir de cobayes avant le déploiement. Quoique imparfaite, cette mesure permettra, dans de nombreux cas, de prévenir certaines difficultés.

Ici, l'entreprise devra peser le risque résultant de l'interruption d'un système de production et évaluer s'il est rentable d'installer des programmes de correction sans les avoir mis à l'essai au préalable. À cet égard, elle devra tenir compte de facteurs comme le nombre d'utilisateurs touchés, les conséquences pour la clientèle et les pertes monétaires.

La procédure de déploiement des rustines devrait, en tout cas, prévoir l'installation d'une seule d'entre elles à la fois. Il sera ainsi plus aisé de déterminer laquelle a causé un incident système, le cas échéant.

Gare au faux sentiment de sécurité! Cette mise en garde est primordiale, car trop souvent, on croit à tort qu'une méthode de déploiement des rustines constitue une protection complète de ses systèmes informatiques. En fait, une telle méthode s'inscrit dans la politique de sécurité qui doit être mise en place à la grandeur de l'organisation. Servant de complément aux mesures générales de sécurité, la méthode d'installation des correctifs se situe à la fois dans les trois phases de protection : prévention, surveillance et réaction.