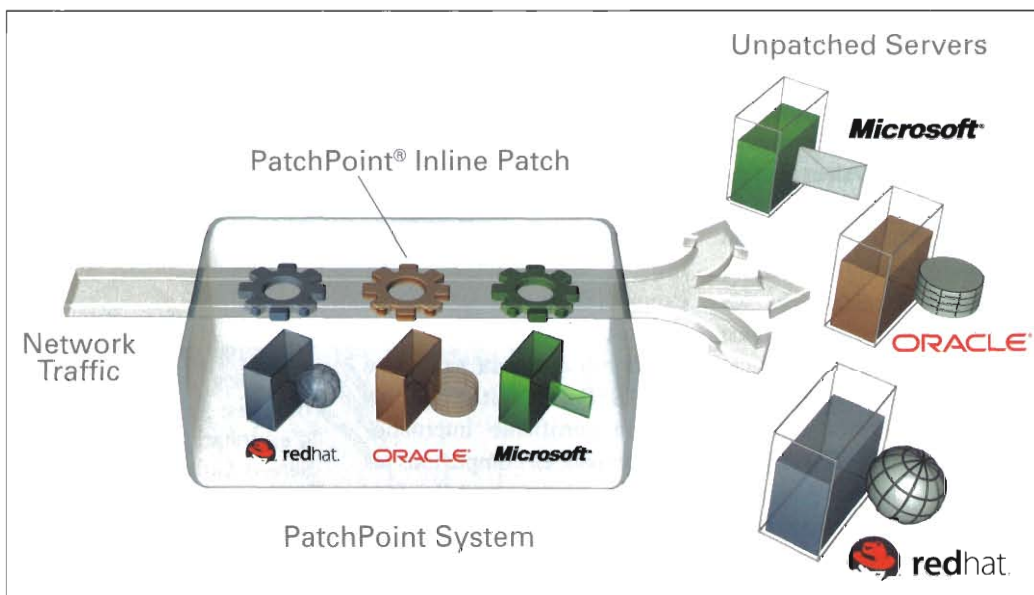


Un article de Navixia

# Le patching virtuel, ou la fin du cauchemar

**SECURITE.** Dans les entreprises, les vulnérabilités exposent de plus en plus les serveurs, les systèmes d'exploitation et les applications stratégiques. Comment se protéger au mieux?



perturbation de fonctionnement peut s'avérer critique. Mais faut-il courir le risque de laisser un serveur vulnérable aux attaques, ou vaut-il mieux risquer que le patch perturbe son fonctionnement et ses applications? Et puis, faut-il patcher tout de suite ou plus tard? Protéger dans l'urgence, ou tester les patches au préalable?

Autre problème connu : les systèmes les plus critiques pour une société sont souvent les plus anciens, car ils contiennent le noyau des informations de l'entreprise. Plus ils vieillissent, plus il devient délicat d'y toucher sans prendre le risque de les déstabiliser.

**A**ppliquer un patch de sécurité au serveur de production... Cette notion fait grincer des dents chaque responsable informatique, non seulement à cause des perturbations que cela cause à l'activité de l'entreprise, mais à cause des effets négatifs que le patch le plus innocent peut avoir sur les applications importantes.

Pour toutes les entreprises, les vulnérabilités exposent de plus en plus les serveurs, les systèmes d'exploitation et les applications stratégiques. Et on le sait, quelques jours suffisent désormais aux pirates pour exploiter une faille. D'où la publication fréquente de patches de sécurité par les éditeurs de logiciels pour pallier les failles identifiées – avec plus ou

moins de bonheur, puisque la correction de la faille entraîne parfois d'autres incidents fonctionnels désagréables et imprévus sur le serveur ou les applications concernés.

### Un gros souci

Microsoft publie ses patches chaque mois, alors qu'Oracle impose à ses utilisateurs tous les trois mois souvent plus de 80 correctifs, qu'il faut tester et installer dans l'urgence. Les autres éditeurs ont tendance à publier leurs correctifs au fur et à mesure des besoins, en fonction de la gravité de la faille constatée.

Dans tous les cas, l'installation des patches est un gros souci pour les responsables informatiques. S'il s'agit d'un serveur de production, toute

### Un exemple

Pour illustrer ce cas de figure fréquent, prenons en exemple une société lambda dont le réseau informatique voit transiter beaucoup d'informations sensibles. Cette société doit garantir le fonctionnement d'une ancienne base de données dont la vulnérabilité est reconnue, mais qui n'est plus supportée par l'éditeur depuis plusieurs années. La base doit être maintenue car elle contient des données financières que la société doit légalement conserver encore plusieurs années. Migrer vers une nouvelle version est impossible car on ne peut évaluer l'impact potentiel d'un changement sur l'application existante.

Un tel problème peut être résolu à l'aide d'une solution de «patching virtuel» qui permet d'appliquer les patches de sécurité immédiatement. Placée sur le flux, devant les serveurs, elle évite de toucher aux serveurs et aux applications.

### La seule solution

Le concept de patching virtuel a été développé pendant trois ans, dans le plus grand secret, par la société américaine Blue Lane qui l'a dévoilé à la fin de 2005. C'est la seule solution de patching virtuel disponible à ce jour. Mais vu son impact formidable sur les procédures d'exploitation, il est vraisemblable qu'elle sera rapidement imitée par d'autres...

La solution se présente sous la forme d'un boîtier appelé Patch-Point, qui comporte un port d'entrée, un port de sortie, et scanne le trafic du réseau au niveau des serveurs. Toutes les communications passent par ce boîtier, ce qui permet d'appliquer une protection pour un ordre donné. C'est un patch virtuel, simulé sur le flux de données. Le réseau peut être utilisé normalement, mais le boîtier établit une limitation de ce qu'on peut y faire. Pour cela, il n'est pas nécessaire de toucher les systèmes live, qui ne risquent

donc pas d'être déstabilisés, mais sont quand même totalement protégés et opérationnels.

Le patching virtuel permet ainsi de corriger les vulnérabilités sans prendre le risque de toucher aux serveurs et sans devoir les faire redémarrer. Surtout, il donne la possibilité de revenir en arrière si le correctif ne donne pas satisfaction. On peut ainsi corriger très rapidement les vulnérabilités et grouper les opérations de patching plus lourdes une ou deux fois par année. Entre-temps, le boîtier Patch-Point protège les serveurs exactement comme le feraient les correctifs de l'éditeur officiel.

Fonctionnellement, les patches fournis par Blue Lane sont équivalents à ceux des éditeurs. La société analyse chaque patch des éditeurs de manière très approfondie dès sa publication, en fonction de deux informations : comment l'éditeur détecte-t-il une exploitation de la vulnérabilité et quelle est l'action exacte du correctif. Ces informations permettent d'émuler le fonctionnement du patch de manière dynamique – mais sur les flux dirigés vers le serveur et non dans le système. Après l'annonce d'une nouvelle vulnérabilité, il faut en moyenne 24 heures à Blue Lane pour fournir le patch correspondant.

## Navixia

Basée à Ecublens et fondée en 2005, Navixia SA est une société suisse spécialisée dans le domaine de la sécurisation du système d'information. Ses fondateurs sont tous des experts de longue date dans le domaine de la sécurité, ce qui leur permet de proposer toute une gamme de solutions et services pertinents aux PME et aux multinationales de Suisse romande.

Navixia propose une approche flexible et personnalisée de la sécurité informatique, grâce à une structure légère, efficace et extrêmement expérimentée dans les domaines de l'analyse, de la limitation et de la gestion des risques ainsi que de la formation.

Dans ce domaine, les délais sont en effet critiques. Un exemple? Au mois d'août, Microsoft publiait l'une des séries de patches les plus importantes de son histoire. La vulnérabilité la plus critique, MS06-040, s'avérait particulièrement dangereuse puisqu'elle rendait possible l'exécution de code à distance. Blue Lane a réagi en mettant un patch à disposition quelques heures à peine après Microsoft.

L'impact du patching virtuel sur le temps de réponse est négligeable, de l'ordre de 150 microsecondes; il peut aller jusqu'à 0,5 milliseconde si le boîtier détecte une tentative d'exploitation d'une vulnérabilité et doit appliquer le patch dynamiquement sur le flux.

A ce jour, tous les systèmes d'exploitation serveurs de

Microsoft et les principales applications Microsoft sont supportés, ainsi qu'Oracle, Sun, Apache, Red Hat Enterprise Linux et diverses applications Unix. Il faut à Blue Lane entre trois et six mois de développement pour supporter un nouveau système.

Le patching virtuel répond à une vraie problématique d'entreprise. Il peut représenter une solution intéressante pour toute société où l'interruption d'un serveur, pour n'importe quelle raison, représente un problème commercial majeur; ou pour une entreprise qui doit maintenir des systèmes anciens sans vouloir les déstabiliser par une intervention directe.

**Patrick Zwahlen,  
Security Architect,  
Navixia**