# Pratique: comment contrôler la gestion des correctifs?

Les stratégies réactives de gestion des correctifs perturbent les processus normaux de gestion des changements applicatifs. Pour maintenir la disponibilité maximale de ses applications, sans remettre en cause sa sécurité, l'entreprise doit pouvoir compter sur l'expertise de détection anticipée des vulnérabilités de son fournisseur de solutions de sécurité.

Pour saisir l'ampleur du défi que représente la gestion des correctifs et des mises à jour critiques, il est nécessaire de comprendre deux aspects clés de l'évolution des systèmes d'information. D'une part, l'hétérogénéité des chaînes logicielles soutenant les fonctions-clés de l'entreprise est faite pour durer. Ces nouvelles architectures apportent plus de flexibilité et de performance aux systèmes d'information (SI), mais en augmentent aussi la complexité de gestion. D'autre part, les entreprises remplacent à un rythme accéléré les extensions propriétaires du SI par des composants standards basés sur des technologies largement diffusées telles que Java, .NET, XML? En matière de sécurité, plus une technologie est diffusée, plus elle suscite l'attention des cyberpirates. Plus l'entreprise met en ?uvre des technologies standards mais hétérogènes, plus le nombre de correctifs et de mises à jour critiques augmente, et plus ces changements continuels font peser un risque sur la disponibilité et les performances des chaînes applicatives critiques. **Les stratégies de gestion réactive des correctifs de sécurité conduisent à une impasse** A en croire les constructeurs, éditeurs et fournisseurs de technologies réactives de sécurité, l'entreprise n'a donc pas d'autre choix que de réagir toujours plus vite aux menaces de sécurité en appliquant les correctifs dès leur publication. Mais cette logique réactive conduit les entreprises à une impasse. Automatisée ou non, les mises à jour de sécurité ont tendance à échapper aux processus normaux de gestion du changement, ce qui va à l'encontre des exigences de traçabilité et d'auditabilité auxquelles doivent aujourd'hui se conformer toutes les entreprises. La raison la plus couramment invoquée est que ces processus industriels de conduite du changement sont trop lents par rapport au rythme d'apparition des menaces. Cet argument de l'urgence, contribue en réalité à masquer un défaut structurel majeur, des stratégies traditionnelles de gestion réactive des correctifs de sécurité. **Seul un expert peut établir le lien entre la menace théorique et la réalité des systèmes de production** L'entreprise est dès l'origine placée devant un non-choix, dont découlent ensuite toutes ses difficultés, ou presque. En dehors d'un message d'alerte décrivant la vulnérabilité exploitée et indiquant le risque encouru, la stratégie réactive de gestion des correctifs ne propose aux directions informatiques aucune alternative à l'obligation d'appliquer une mise à jour critique, sinon celle d'ignorer l'avertissement, à ses risques et périls. A son corps défendant, le constructeur ou l'éditeur ne peut en effet élaborer un correctif de sécurité qu'à partir de ce qu'il connaît, c'est-à-dire l'environnement théorique d'exploitation de son application. De plus, les correctifs publiés s'inscrivent souvent dans la stratégie de développement, propre à chaque constructeur. Or, celle-ci n'est pas nécessairement en cohérence avec la politique de gestion de l'entreprise utilisatrice. Pour concilier ces différences, les entreprises et les constructeurs doivent pouvoir compter sur un partenaire expert de la sécurité, seul capable d'établir le lien entre la menace théorique et la réalité des systèmes en production. Cette expertise est précisément celle du fournisseur de solutions de sécurité. Mais pour qu'il puisse pleinement remplir cette mission, le spécialiste de la sécurité doit

avoir développé une stratégie de protection préventive, basée sur une compréhension approfondie des vulnérabilités et de leurs méthodes d'exploitation. **Bâtir des stratégies de sécurité différentiées** Contrairement à l'approche réactive d'application en urgence des correctifs de sécurité, la méthode préventive restitue à l'entreprise la pleine maîtrise de sa stratégie de gestion des mises à jour. Appliquée à un segment de réseau ou bien à un serveur, ou encore sur chaque poste de travail, la méthode de protection préventive contre les vulnérabilités facilite la prise en compte de l'hétérogénéité des configurations dans un système d'information. Qu'il s'agisse de préserver l'intégrité d'une chaîne applicative sensible, de prendre le temps de planifier les mises à jour en fonction des impératifs d'exploitation, ou tout simplement de réduire les coûts, l'entreprise peut définir des stratégies différentiées de gestion des correctifs pour chaque segment critique du SI. Intégrée aux systèmes de protection contre les intrusions réseau, la technologie préventive permet par exemple de protéger virtuellement un ensemble de postes de travail d'une menace provenant du réseau. La même approche peut aussi permettre de circonscrire une infection virale au seul poste nomade infecté hors du réseau de l'entreprise, réduisant ainsi le coût et l'impact d'une attaque. Pour les serveurs hébergeant des composants d'applications critiques, la solution préventive garantit une étanchéité des systèmes à toute tentative d'exploitation d'une vulnérabilité, laissant à la direction informatique le temps d'évaluer en profondeur l'impact du correctif proposé par l'éditeur. En définissant des îlots de sécurité différentiés, les entreprises sont en mesure de réintégrer la gestion des correctifs de sécurité dans les processus normaux de conduite du changement, profitant par exemple d'une opération de mise à jour applicative pour déployer un correctif dûment testé. **L'offre d'Internet Security Systems**

Par la mise en pratique, avec Virtual Patch, de l'expertise acquise en découvrant les vulnérabilités des nouveaux logiciels, ISS aide efficacement l'entreprise à faire le tri dans les alertes de sécurité, et à conserver de bout en bout la maîtrise de sa politique de gestion des correctifs. Depuis 10 ans, l'équipe de recherche X-Force d'Internet Security Systems analyse en détail les logiciels (systèmes d'exploitation, applications, bases de données, ?) les plus répandus dans les entreprises (Windows, Cisco IOS, SAP, Oracle, ?) afin de découvrir les failles de sécurité susceptibles d'être exploitées. Couplée à une surveillance constante de l'activité des communautés de cyberpirates sur internet, depuis ses cinq centres opérationnels (SOC) à travers le monde, cette recherche des vulnérabilités permet à ISS de mettre à disposition des entreprises une expertise unique au monde. Selon une étude du cabinet Frost et Sullivan, les chercheurs de la X-Force d'ISS découvrent chaque année depuis cinq ans plus de 51% des vulnérabilités à haut risque, soit plus à eux seuls que tous leurs concurrents réunis. Une fois découvertes, les vulnérabilités sont classées selon le niveau de risque auquel elles exposent les entreprises (vol d'information, prise de contrôle, déni de service ?). A cette évaluation technique du risque, l'équipe de recherche X-Force ajoute une notion de priorité, en fonction du taux de diffusion de la version concernée du logiciel. A ce stade, les experts de la X-Force ont non seulement une idée précise de la nature du risque, de sa capacité de propagation, mais aussi des moyens de le combattre. En effectuant par anticipation le travail de détection des vulnérabilités, l'équipe de recherche X-Force identifie également les voies d'accès à disposition des cyberpirates. C'est sur cette expertise que repose la solution Virtual Patch d'ISS, qui consiste à détecter et à bloquer de façon préventive toutes les tentatives d'exploitation d'une vulnérabilité. Intégrées aux systèmes de protection contre les intrusions réseau (IPS) Proventia Network, ainsi qu'aux suites de sécurité pour les postes de travail et les serveurs, Proventia Desktop et Proventia Server, les règles d'analyse du trafic Virtual Patch éliminent sinon le besoin, au moins l'urgence de

mettre en ?uvre le correctif de sécurité proposé par le constructeur ou l’éditeur.