VIRTUAL PATCHING : L'ANTIDOTE QUI VOUS PROTÉGE DES VULNÉRABILITÉS

L'essentiel sur le Virtual Patching

Qu'est-ce qu'un patch logiciel ?

Un patch a pour but de résoudre une problématique ou de combler une faille de sécurité dans un logiciel informatique.

Quel est l'intérêt des patchs logiciels ?

Les logiciels sont souvent complexes. Windows Vista, par exemple, compterait plus de 50 millions de lignes de code. Les cybercriminels tentent d'identifier des failles, principalement pour prendre le contrôle de machines vulnérables. En ne déployant pas les patchs nécessaires, le risque est de laisser une porte ouverte via laquelle les attaquants s'immisceront.

Qu'est-ce que le Virtual Patching?

Un patch virtuel est, en réalité, une règle de sécurité qui prévient toute tentative de tirer partie d'une faille ou d'une vulnérabilité connue. Le patch virtuel contrôle les échanges entrants et sortants d'un programme logiciel vulnérable, pour neutraliser les tentatives de piratage.

Virtual Patching : les bonnes questions à se poser

1) A quelle fréquence déployez-vous vos patchs de sécurité ? Avez-vous déjà déployé des patchs en urgence ?

Les patchs critiques sont nombreux et fréquents ce qui rend quasi-impossible, pour les entreprises, de garder le rythme. Le déploiement de patchs est chronophage et fastidieux, mais les risques sont importants si ces patchs ne sont pas installés.

2) Pouvez-vous rendre vos applications métiers indisponibles pour le patching ?

Le déploiement de patchs implique souvent un redémarrage, ce qui induit une indisponibilité temporaire des applications critiques. Cet arrêt applicatif, dans l'urgence, n'est pas toujours possible. Le Virtual Patching offre donc du temps pour tester les patchs et les déployer avec un minimum d'impact sur les applications.

3) Disposez-vous de systèmes d'exploitation qui ne sont plus sous maintenance ?

Certains systèmes, (tels que Windows 2000 Server, Windows XP et prochainement Windows 2003 Server) ne sont plus pris en charge par leur éditeur et ne disposent plus de nouveaux patchs. Les contrats de support personnalisés sont, par ailleurs, particulièrement onéreux. Le Virtual Patching règle justement cette problématique.

Le Virtual Patching proposé par les solutions Deep Security & Vulnerability Protection

Le Virtual Patching pallie les vulnérabilités sur les systèmes critiques : vous disposez ainsi de temps pour obtenir, tester et déployer les patchs proposés par les éditeurs, et vous êtes protégés même si un patch n'est pas encore disponible.

Le Virtual Patching pour qui ?

Ce sont les équipes d'exploitation informatique qui se montreront les plus intéressées par le Virtual Patching, le patching relevant souvent de leurs attributions. Le Responsable de la sécurité est également susceptible de s'intéresser à la dimension stratégique du Virtual Patching.

Les avantages du Virtual Patching

- **Meilleure sécurité :** les vulnérabilités sont souvent découvertes avant qu'un patch soit disponible, et pour les systèmes obsolètes, les patchs ne sont généralement plus sont rarement plus fournis. Les patchs virtuels peuvent alors être déployés rapidement, ce qui accélère l'activation d'une protection.
- **Une administration plus simple :** contrairement aux patchs logiciels, les patchs virtuels se déploient rapidement et n'entraînent aucune indisponibilité des applications métier.
- **Prise en charge étendue des applications :** une sécurité prête à l'emploi pour près de 300 systèmes d'exploitation, applications ou bases de données.
- **Compatibilité avec de nombreux systèmes d'exploitation actuels ou hérités :** vous disposez d'un moyen économique pour protéger les serveurs hérités et obsolètes.
- **Analyse de recommandation :** recommandation automatique de règles devant être déployées pour protéger un système. Cette fonction permet de n'activer que les règles nécessaires, et ce, de façon automatique. Le déploiement de patchs peut également être automatisée.
- **Une équipe d'experts en sécurité chez Trend Micro,** surveille en permanence les multiples vulnérabilités pouvant donner lieu à un piratage de données, pour une prise en charge proactive des vulnérabilités.

VIRTUAL PATCHING : L'ANTIDOTE QUI VOUS PROTÈGE DES VULNÉRABILITÉS

Le Virtual Patching pour quoi ?

Le Virtual Patching prend en charge de multiples systèmes d'exploitation , applications et bases de données, parmi lesquels* :

Système d'exploitation	Windows (2000, XP, 2003, Vista, 2008, 7, 2012, 8/8.1), Sun Solaris (8, 9, 10), Red Hat EL (4, 5, 6, 7), SuSE Linux (10, 11)
Bases de données	Oracle, MySQL, Microsoft SQL Server, Ingres, PostgreSQL, IBM, SAP
Serveurs et applications Web	Microsoft IIS, Apache, Apache Tomcat, Domino, Adobe ColdFusion, Microsoft SharePoint
Serveurs email	Microsoft Exchange Server, Merak, IBM Lotus Domino, Mdaemon, Ipswitch, IMail, MailEnable Professional, sendmail
Serveurs FTP	Ipswitch, War FTPd, Allied Telesis, ProFRPD, OracleXDB, NetTerm, Linux, IIS, 3Com
Serveurs de sauvegarde	Computer Associates, Symantec, EMC, Veritas, IBM
Serveur de gestion du stockage	Symantec, Veritas
Serveurs DHCP	Microsoft, ISC DHCPD
Applications desktop	Microsoft (Office, Visual Studio, Visual Basic, Access, Visio, Publisher, Excel Viewer, Windows Media Player, DirectX), Kodak Image Viewer, Adobe (Acrobat, Flash, Shockwave, Photoshop), Apple (Quicktime, iTunes), RealNetworks RealPlayer, SUN Java, Yahoo (Messenger, Player...), VLC, OpenOffice, Skype
Clients email	Outlook Express, MS Outlook, Windows Vista Mail, IBM Lotus Notes, Ipswitch IMail Client
Navigateurs Web	Internet Explorer, Mozilla Firefox, Apple Safari, Opera, Google Chrome
Antivirus	Clam AV, CA, Symantec, Norton, Trend Micro, Microsoft, McAfee, ClamAV, BitDefender, Kadpersky
Autres applications	Samba, IBM Websphere, IBM Lotus Domino Web Access, X.Org, X Font Server prior, Rsync, OpenSSL, Novell Client, Asterisk, HP OV, LANDesk, Squid, VMware, VoIP, LDAP

* Liste non exhaustive

TREND MICRO™

Trend Micro SA
85, avenue Albert 1er
92500 Rueil Malmaison
Tél : +33 (0) 1 76 68 65 00
Email : sales@trendmicro.fr

Retrouvez-nous sur le Web & les réseaux sociaux

www.trendmicro.fr
blog.trendmicro.fr
www.facebook.com/TrendMicroFrance
twitter.com/TrendMicroFR