

<http://www.journaldunet.com/solutions/securite/cas/07/1217-mcdonalds-france-vulnerabilite-qualys.shtml>

McDonald's met les vulnérabilités à la diète

Pour l'accompagner dans sa mise en conformité avec la loi Sarbanes-Oxley et la norme PCI-DSS sur les cartes bancaires, McDonald's France audite les vulnérabilités de ses serveurs critiques via un service en ASP.

Multinationale de plus de 20 milliards de dollars de chiffre d'affaires, McDonald's, McDo pour les habitués, compte plus de 30 000 restaurants à travers le monde, dont un peu plus de 1 100 sur le seul territoire français.

En savoir plus

- **Cas** : Le choix de l'audit de vulnérabilité en mode SaaS
- **Dossier** : Failles de sécurité

En tant que filiale d'un groupe américain côté en bourse, McDonald's France doit répondre à des exigences de conformité, notamment à l'égard de la loi Sarbanes-Oxley (SOX) et de la norme PCI DSS (Payment Card Industry Data Security Standard).

"Notre besoin initial était au moins triple. D'abord de suivi de l'exposition de nos serveurs de production, dont le niveau de sécurité fluctue, notamment au gré de la découverte de nouvelles failles applicatives. Deuxièmement, la conformité à SOX qui se traduit annuellement par un double audit. Troisièmement : PCI", explique le responsable systèmes et sécurité de l'enseigne, Wilfried Delcambre (*lire l'analyse "Standard PCI-DSS : un bienfait pour la sécurité de l'e-commerce ?" du 19/11/2007*).

"Même si PCI ne s'applique pas encore en France, il est souhaitable dès aujourd'hui de s'interroger sur les processus de traitement de l'information bancaire. Des sociétés spécialisées viennent nous auditer pour la conformité PCI DSS", complète-t-il.

Pour répondre à ces exigences de conformité et disposer d'une vue exhaustive sur le niveau de vulnérabilité de ses serveurs de production, McDonald's France décide fin 2004 de mettre en place un audit automatisé. L'enseigne retient pour cela la sonde de vulnérabilité de Qualys. Celle-ci lui permet, en faisant office de tiers de confiance, de fournir les données nécessaires à plusieurs points de contrôle SOX comme l'état des patches.

Les rapports techniques PCI émis à partir d'un même boîtier géré par l'éditeur

La sonde QualysGuard déployée sur le réseau interne audite ainsi une trentaine de serveurs de production critiques pour l'activité du restaurateur.

Des scans sont effectués de manière hebdomadaire et les rapports sont exploités pour la politique de patch management. D'autres audits sont amorcés manuellement après l'installation de nouveaux serveurs ou le déploiement d'applicatifs afin d'en valider le niveau de sécurité.

En complément de QualysGuard, McDonald's France a souscrit l'offre en ASP. L'audit s'effectue alors depuis des sondes situées sur le réseau de l'éditeur et apporte à l'entreprise une vision depuis l'extérieur de ses systèmes.

"La tarification se fait à l'adresse IP. Le boîtier nous est mis à disposition par Qualys. Au final, nous achetons uniquement un service, Qualys assurant la gestion du matériel", apprécie Wilfried Delcambre.

En savoir plus

En 2007, McDonald's France a également testé QualysGuard PCI, en fait un service supplémentaire implémenté sur le boîtier déjà en place sur le réseau.

- **Cas** : Le choix de l'audit de vulnérabilité en mode SaaS
- **Dossier** : Failles de sécurité

Utilisé "à blanc" cette année, le service devrait dès 2008 être exploité pour générer les rapports traitant chacun des points du questionnaire technique PCI. Les rapports ainsi créés doivent en effet faire foi vis-à-vis des instances PCI. Ils pourront donc être exploités dans le cadre de l'audit PCI auquel est soumise la filiale France du groupe de restauration rapide.

Le projet en bref

Entreprise	McDonald's France
Solutions retenues	QualysGuard et QualysGuard PCI
Début du projet	2006

Christophe AUFFRAY, JDN Solutions

Copyright 2007 69-71 avenue Pierre Grenier 92517 Boulogne Billancourt Cedex, FRANCE

Lancer l'impression