

GESTION DES VULNERABILITES

Interview de Marc Picovsky, responsable du marketing produit chez DenyAll

A l'heure où les entreprises continuent de déployer un nombre croissant d'applications Web afin d'automatiser leurs processus, de la «supply chain» aux ressources humaines, l'ouverture de leur système d'information aux clients, fournisseurs et partenaires 24x7x365 représente un risque majeur en terme de sécurité. Les attaques exploitant les failles des applications Web sont devenues la principale menace pour les entreprises. Les solutions de sécurité traditionnelles à base de firewall simples et d'antivirus ne sont pas capables de détecter et de bloquer ces attaques au niveau applicatif. D'où



Marc Picovsky, DenyAll

ruptures de service, vols d'informations confidentielles, détournements de transactions financières, atteintes à l'image de marque de l'entreprise. Autant d'incidents que la société française DenyAll, un des pionniers du secteur, entend contrer avec sa gamme de firewalls applicatifs rWeb. Marc Picovsky, responsable du marketing produit chez Deny All détaille les technologies et leur application dans le contexte de PCI DSS. Un des axes de développement de la société.

- Diriez-vous que le marché de la sécurité des applications Web devient mature ?

Parfaitement. Alors que la sécurité des applications Web était perçue il y a peu comme une nouveauté, elle passe de plus en plus dans les mœurs. Avec les échéances de conformité aux standards PCI et l'avènement du

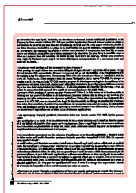
Web 2.0, il y a un net regain d'intérêt pour les firewalls applicatifs. D'ailleurs, nous lançons un portail PCI (www.pci.denyall.com) qui sera disponible fin mai. La version 3.8 de notre solution rWeb, disponible depuis fin janvier 2009, apporte de nombreuses fonctionnalités parmi lesquelles la compatibilité PCI, le chiffrement ou le contrôle d'intégrité. Nous avons aussi amélioré les performances et la possibilité de déployer les solutions avec plus de transparence. Les exigences de PCI et l'accroissement des menaces rendent la protection des applications web au niveau applicatif indispensable. Ce contexte général est favorable pour un pionnier comme DenyAll qui a plus de dix ans d'expérience de développement dans ce secteur. Le marché devient mature, mais la sécurité des applications Web reste un sujet sensible.

- Quels sont les réelles nouveautés techniques introduites avec la version rWeb 3.8 de votre firewall ?

Avec l'introduction de rWeb 3.8, DenyAll fournit les outils pour satisfaire aux exigences de PCI DSS avec l'ensemble le plus complet d'option de sécurité. La performance générale est également prise en charge grâce à un mécanisme d'optimisation dans l'accélération et la sécurité. Pour aider les entreprises à atteindre le meilleur niveau de sécurité pour leurs applications, les modèles de listes noires ont été améliorés avec la notion de groupe. Avec plus de 10 ans de production de fichiers de signatures, la vérification de l'ensemble des règles est devenue un défi pour les entreprises. Avec le modèle de groupe, une requête est vérifiée seulement avec les signatures de groupe, ce qui rend la transaction plus sûre et plus rapide. Les mécanismes de listes grises, que DenyAll appelle «liste de notation», tire aussi avantage de ces nouveaux développements. Si bien que rWeb 3.8 fournit la possibilité de calculer automatiquement le poids de référence pour une application basée à la fois sur le fichier interne de connaissances et les journaux spécifiques de connexion. Le résultat de ce calcul est une échelle de référence correspondant exactement au comportement de l'application, évitant les fausses protections contre les demandes qui ne correspondent pas exactement au comportement attendu. Pour le modèle de sécurité positive, les listes blanches ont été optimisées avec l'introduction de nouvelles règles de filtrage qui supportent un grand nombre de paramètres, ce qui permet de définir des ensembles de paramètres autorisés et des valeurs dans une seule interface. La solution rWeb 3.8 étend également les possibilités d'intégration dans l'architecture du client de manière transparente et donc sans modification aucune à l'infrastructure existante.

- Les vols de données chez RBS WorldPay et Heartland ont mis en exergue les limites de PCI DSS. Les congrès américain a dénoncé la responsabilité de PCI dans ces vols intervenus chez des opérateurs pourtant réputés 'compliant'. Quel regard un acteur français comme DenyAll jette-il sur cette situation ?

Le problème vient de la compréhension et de l'utilisation qui est faite des certifications de sécurité. Ces dernières ont essentiellement pour objectif de fournir un guide de bonnes pratiques de sécurité. Elles vont établir la liste des outils qui devraient être mis en œuvre ainsi que les principaux processus



qui devraient être appliqués. Toutefois, ces dernières ne donnent aucune contrainte qualitative. A titre d'exemple, il est mentionné dans PCI DSS que les Web Application Firewall doivent mettre en place un mécanisme de sécurité par liste blanche (modèle de sécurité positif), mais aucun critère de qualité de ces listes blanches n'est défini. Le piège de la certification est que de nombreux responsables sécurité se «contentent» de respecter les critères a minima sans chercher à comprendre leur finalité, et encore moins les menaces auxquelles ces critères permettent de répondre. On peut faire le parallèle avec un élève qui prépare tous les exercices de maths de son livre avant un examen, obtient une excellente note mais n'a finalement pas acquis les bases théoriques correspondantes. Il a une bonne note mais reste nul en maths...

- Comment rWeb protège-t-il des attaques les plus récentes ?

rWeb protège les applications des nouvelles attaques de type Nihaorr 1 apparues début 2008. Il s'agit d'une Injection SQL automatisée. Nihaorr 1 ne permet pas un vol de données, mais l'exploitation d'informations à des fins détournées. Chaque page Web d'un site infecté par Nihaorr 1 infectera à son tour le PC de l'internaute. Cette attaque remet en cause l'intégration de la norme PCI-DSS. Le danger ne s'arrête pas là : la mesure 6 de PCI DSS requiert en outre de développer et de gérer des systèmes et des applications sécurisés (correctifs, mises à jours officielles, évolutions de configurations, failles courantes). Or, si les sites Web sont infectés par Nihaorr 1, il devient possible de contrôler les données. Ainsi, des codes de cartes de crédit peuvent être copiés et communiqués sur des pages Web...

Comment rWeb protège-t-il contre ce type d'attaques? Grâce à la liste noire et la fonctionnalité de 'scoring list' qui permet de définir et de hiérarchiser plusieurs critères afin de bloquer des familles d'attaques et non plus uniquement une signature spécifique. Notre offre répond donc aux exigences de la mesure 6 de PCI DSS avec un éventail très large de fonctionnalités de filtrage (normalisation d'adresse, liste noire, liste pondérée, liste blanche, surveillance de comportement, suivi de session, fonctionnalités XML) qui protègent contre les attaques connues et certaines attaques non référencées, ainsi qu'envers les modifications logicielles non validées et les évolutions applicatives.

- Les commerces français semblent néanmoins faire une fronde contre PCI DSS. Qu'en pensez-vous ?

Une certification a un coût. Et les investissements en sécurité se font toujours à reculons dans la mesure où il est difficile de justifier d'un retour sur investissement. Dans une période de crise comme celle que nous traversons, ce phénomène est amplifié. Ainsi, toute contrainte visant à imposer un investissement supplémentaire est nécessairement mal perçue.

- Les consultants reprochent aux fournisseurs d'appiances et de firewall applicatifs, y compris Cisco, de faire croire qu'il suffit d'installer quelques firewalls pour être 'compliant' à PCI DSS. Ce reproche vous paraît-il fondé ?

La certification peut être obtenue soit en installant un firewall applicatif, soit en effectuant un audit de code. Par conséquent, chaque acteur prêche pour sa paroisse. Les cabinets de consultants vont défendre la seconde solution, les éditeurs la première. Encore une fois, le problème est essentiellement qu'aucun critère de qualité n'est défini. En effet, rien ne garantit que l'audit de code a été fait correctement par des gens compétents, ni que le firewall applicatif est suffisamment efficace ou bien configuré. Le consultant international Bruce Schneier a souvent martelé que la sécurité n'était pas un produit, mais un processus. Cette assertion reste vraie. La certification indique quelles sont les solutions nécessaires à un niveau de sécurité spécifique. Ce n'est pas une condition suffisante. Il reste à la charge des responsables sécurité de s'assurer de la qualité et de la cohérence de leur mise en œuvre.

- Comment un acteur français se positionne-t-il face aux grands opérateurs du monde des réseaux ?

DenyAll a été le premier éditeur à offrir des solutions firewall applicatif. Notre implantation depuis de



nombreuses années dans la plupart des grands comptes français est une garantie d'expertise et d'expérience dans un secteur en constante évolution. Cette reconnaissance du marché nous aide à valoriser un savoir-faire et des acquis uniques. En outre, la société DenyAll est depuis sa création uniquement axée sur la sécurité. Cette focalisation volontaire est un gage de compétence dans le domaine. Au delà de notre positionnement technologique, nous avons aussi une stratégie de conquête des marchés européens qui représentent la moitié de notre activité. Après deux années passées à nous restructurer, nous avons décidé de développer une véritable stratégie marketing et de renforcer nos marchés historiques. Aujourd'hui, nous avons donc entrepris de nous renforcer en Allemagne, en Espagne, au Benelux, pays dans lesquels nous avons déjà des équipes. La filiale allemande de DenyAll s'est vu confier plusieurs projets d'envergure par de grandes entreprises allemandes.

http://www.denyall.com/index.html?option=com_form_download&cfidid=10&Itemid=200

http://www.denyall.com/data/pdf/fr_rweb_fiche_produit.pdf

Propos recueillis par Jo COHEN