watchfire
an IBM company

SÉCURITÉ DES APPLICATIONS WEB – LE GUIDE ESSENTIEL

DANNY ALLAN, ANALYSTE SPÉCIALISÉ EN RECHERCHE STRATÉGIQUE

Un livre blanc d'IBM

TABLE DES MATIÈRES

INTRODUCTION

La sécurité des applications Web ne peut plus être ignorée. De plus en plus souvent, les vols de données et les incidents liés aux applications Web font la une de l'actualité de la sécurité. Non seulement les clients exigent une traçabilité de la part des entreprises, mais la législation, dont un exemple est la loi américaine *California Senate Bill 1386 (SB-1386)*, exigent d'avertir toutes les parties concernées en cas de violation de sécurité liée à des informations personnelles ou sensibles.

Au cours des cinq dernières années, deux grandes tendances ont émergé sur le marché de la sécurité :

1. L'agresseur n'attaque plus pour des motifs de prestige personnel, mais est mû par l'appât du gain ou agit dans un dessein de vol ; et
2. les logiciels, et plus spécialement les applications Web, sont désormais la cible commune des piratages

MÉTHODOLOGIE D'ÉVALUATION

Autrefois, les entreprises pouvaient compter sur leurs dispositifs de défense périphérique pour assurer leur sécurité. Malheureusement, les pare-feux des réseaux et les outils d'analyse de vulnérabilité des réseaux n'offrent aucune protection contre les offensives au niveau des applications. Les applications Web sont conçues de telle façon qu'elles peuvent permettre à des utilisateurs inconnus d'interagir avec les données et les systèmes d'une entreprise. Ce type d'interactions parvient à franchir les mécanismes de défense réseau tels que les pare-feux et les systèmes de détection des intrusions.

Gartner estime que 75 % des offensives ciblent désormais les applications. Les enquêtes menées par Watchfire indiquent que 90 % des sites Web sont vulnérables à ce type d'attaques. De toute évidence, la sécurité des applications Web ne peut plus être ignorée.

NORMES ET RÉGLEMENTATIONS ÉMERGENTES

Face à l'aggravation des violations de sécurité liées aux applications Web, à l'augmentation de leur nombre et des difficultés qu'elles posent, la rigueur des réglementations et standards industriels s'est renforcée. De nouvelles normes telles que la norme de sécurité des données PCI (Payment Card Industry) intègrent désormais la sécurité des applications Web.

Ces réglementations officielles stipulent que les entreprises doivent assurer le développement et la maintenance de systèmes et d'applications sécurisés, et ciblent tout particulièrement les vulnérabilités des applications Web. De telles réglementations surgissent aujourd'hui et font l'objet de définitions car les protections réseau traditionnelles sont insuffisantes contre ce type d'offensives.

MISE EN PLACE D'UN CONTRÔLE DE GESTION DES RISQUES LIÉS AUX APPLICATIONS WEB

Plusieurs grandes initiatives doivent être mises en place et développées dans trois domaines : les personnes, les processus et la technologie.

Les personnes : Il est impératif que les responsables du développement et du déploiement des applications Web maîtrisent les fondamentaux des principes de la conception sécurisée et des menaces contre la sécurité.

La technologie : L'utilisation d'outils automatisés pour la sécurité des applications Web apporte des avantages d'échelle et de coût. Un outil automatisé permet d'analyser les vulnérabilités de la sécurité des applications Web de façon cohérente, fiable et évolutive dans des environnements diversifiés de grande envergure. En outre, un outil automatisé permet de communiquer des recommandations cohérentes et pertinentes en adéquation avec la stratégie de l'entreprise et les réglementations officielles.

Les processus : L'intégration des tests de sécurité des applications Web au cycle de vie du développement logiciel est une initiative fondamentale pour mettre en œuvre une gestion des risques saine. Si cette démarche doit certes être confiée à une équipe d'évaluation compétente et spécialisée dans la sécurité lors de la phase finale, elle doit aussi être incorporée à un stade précoce du développement d'applications afin de cerner les problèmes de sécurité dès leur apparition et de réaliser des économies en termes de temps et de coûts.

En l'absence d'une évaluation et d'une visibilité satisfaisante de ces initiatives, il est impossible de déterminer si des protections adaptées ont été effectivement implémentées pour atténuer les risques. Ces métriques doivent inclure les principaux facteurs tels que les menaces, les vulnérabilités, les actions correctives et le degré de gravité, tout en définissant des lignes directives et un historique sur une période donnée.

LES SOLUTIONS D'IBM RATIONAL (WATCHFIRE)

A travers son acquisition de la compagnie Watchfire, IBM est un leader reconnu sur le marché des logiciels d'évaluation de la vulnérabilité des applications Web. Son offre comprend des progiciels de sécurité qui vont des outils d'assistance aux auditeurs spécialisés en sécurité à une plate-forme destinée aux très grandes entreprises. Ces produits fournissent des informations précises sur les vulnérabilités des applications Web. Le tableau suivant décrit en détail quelques-uns des enjeux concernés :

Menace	Exemple d'impact pour l'entreprise	Pourcentage moyen des applications Web vulnérables
Scriptage inter-sites	Usurpation d'identité	80%
Injection de code SQL	Altération de la totalité des données	62%
Falsification de paramètres	Fraude, modification des distributions	60%
Empoisonnement de cookie	Usurpation d'identité	37%

IBM, à travers de sa gamme de produits IBM Rational AppScan propose une solution de reporting destinée aux dirigeants, aux manageurs et aux développeurs, définie spécialement pour une fonction et une personne en particulier. En effet, alors qu'un auditeur de sécurité s'intéressera surtout aux problèmes de sécurité d'un secteur d'activité donné, le responsable de la conformité souhaitera plutôt recevoir un reporting concernant les critères de conformité qu'il est chargé de gérer. La plate-forme de livraison de logiciel IBM pour les entreprises comporte également des fonctions stratégiques telles que la gestion des problèmes, des accès basés sur les rôles, la personnalisation et de puissantes API d'intégration.

Outre ses solutions de reconnaissance, d'évaluation et de reporting des applications Web d'une entreprise, IBM facilite aussi la formation interne des collaborateurs par le biais de prestations de conseil détaillées et des recommandations de corrections personnalisées. Grâce à sa branche de services aux clients, IBM assure également des formations à la sécurité et aux produits qui ciblent spécifiquement le segment vertical du secteur d'activité concerné.

SYNTHÈSE

Face à des applications Web dont la taille, la complexité et l'omniprésence ne cessent de croître, les mécanismes de défense et les protections correspondantes doivent eux aussi évoluer. Les entreprises doivent implémenter des règles et des contrôles capables de prendre en charge des environnements distribués tout entiers ; elles doivent aussi faire face à la complexité des technologies modernes et se synchroniser avec le cycle de développement logiciel interne de l'entreprise. En outre, elles doivent être prêtes à fournir à leur Direction, aux auditeurs officiels et aux clients des métriques et des informations sur la planification et la stratégie de sécurité adoptées. Négliger de telles mesures est une prise de risque dangereuse sur le marché actuel.

Copyright d'IBM