12

Les Bonnes pratiques pour un serveur web sécurisé

CENTRE DE RECHERCHE
SUR L'INFORMATION
SCIENTIFIQUE ET TECHNIQUE
cerist

LES BONNES PRATIQUES POUR UN SERVEUR WEB SÉCURISÉ

Diverses attaques de piratage de grande envergure ont démontré que la sécurité web reste le problème le plus critique pour toute entreprise qui exerce ses activités en ligne. Les serveurs Web et en raison des données sensibles qu'ils hébergent habituellement sont l'un des visages publics les plus ciblés d'une organisation. Sécuriser un serveur web est aussi important que la sécurisation du site ou d'une application Web elle-même et du réseau qui l'entoure. Si vous avez une application Web sécurisée et un serveur Web non sécurisé, ou vice versa, votre entreprise court un risque énorme. La sécurité de votre entreprise est son point fort comme étant son maillon le plus faible. Voici une liste des tâches que l'on doit suivre lors de la sécurisation d'un serveur Web.

1. Suppression des services inutiles

L'installation du système d'exploitation par défaut et sa configuration, ne sont pas sécurisés. Dans une installation par défaut, de nombreux services réseau qui seront inutiles dans une configuration serveur Web sont installés. Plus il y a des services fonctionnant sur un système d'exploitation, plus y aura des ports ouverts, laissant ainsi des portes ouvertes pour les utilisateurs malveillants. Désactiver les services inutiles libérera des ressources matérielles et rendra votre serveur plus performant.

2. Accès à distance

Les administrateurs des serveurs Web doivent se connecter localement. Si l'accès à distance est nécessaire, il faut s'assurer que la connexion est réalisée correctement, à l'aide de protocoles de tunneling et de chiffrement (TLS ,SSH). L'accès à distance doit également être limité seulement à des comptes et un nombre d'adresses IP spécifiques. Il est également très important de ne pas utiliser des ordinateurs publics ou des réseaux publics pour accéder aux serveurs d'entreprise à distance.

3. Séparer les environnements développement, test, et production

Comme il est plus facile et plus rapide pour un développeur de développer une nouvelle version d'une application Web sur un serveur de production, il est assez fréquent que le développement et le test d'applications web se font directement sur le serveur de production. Et comme ces applications web sont dans leurs premiers stades de développement, ils ont tendance à avoir un certain nombre de vulnérabilités, ce qui peut facilement être découvert et exploité par un utilisateur malveillant, en utilisant des outils disponibles gratuitement sur Internet. Idéalement, le développement et le test des applications Web doivent toujours être effectués sur des serveurs isolés d'internet, et ne devraient jamais utiliser ou se connecter à des bases de données réelles.

4. Contenu Web et scripts côté serveur

Les fichiers de site Web et les scripts doivent toujours être sur une partition autre que celle du système d'exploitation, des logs et tout autre fichier système. Puisque les expériences montrent que les pirates, ayant obtenu un accès au répertoire racine du serveur web, ont été en mesure d'exploiter d'autres vulnérabilités, et ont réussi à aller plus loin et d'élever leurs privilèges. Ils peuvent ainsi exécuter n'importe quelle commande du système d'exploitation, ce qui entraîne un contrôle complet du serveur web.

5. Permissions et privilèges

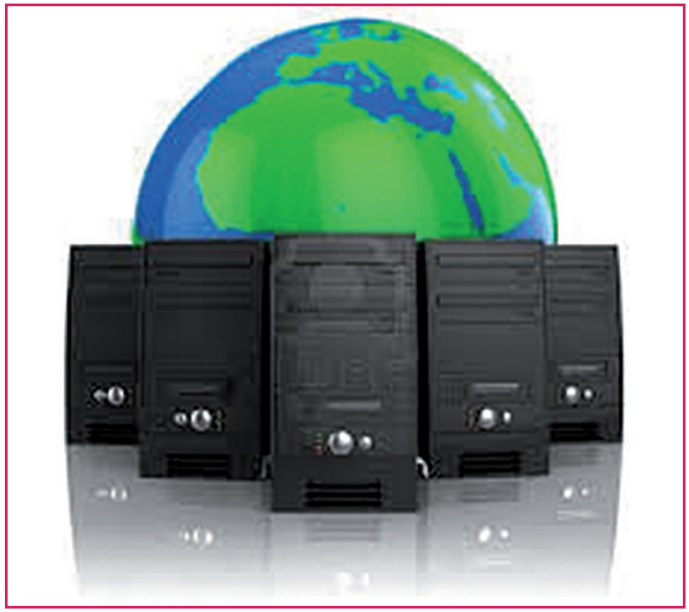
Les permissions sur les fichiers et les services réseau jouent un rôle essentiel dans la sécurité du serveur web. Attribuer le minimum de privilèges nécessaires pour le fonctionnement d'un service réseau spécifique. Il est également très important d'attribuer le minimum de privilèges aux utilisateurs pour accéder au site Web, et à toutes les données cotés serveur.

6. Correctifs de sécurité à jour

Un logiciel entièrement mis à jour ne signifie pas nécessairement que votre sevrveur est totalement sécurisé, il est toujours très important de mettre à jour votre système d'exploitation et tout autre logiciel fonctionnant sur votre machine avec les derniers correctifs de sécurité. Jusqu'à aujourd'hui, des incidents de piratage continuent à se produire à cause des serveurs et logiciels non mis à jour.

7. Les comptes d'utilisateurs

Lors de l'installation d'un système d'exploitation, des comptes utilisateurs inutilisés sont créés, ceux-ci doivent être vérifiés en leur affectant les autorisations nécessaires. Le compte administrateur doit être renommé et ne doit pas être utilisé. Chaque administrateur accédant au serveur Web doit disposer de son propre compte utilisateur, avec les privilèges adéquats nécessaires. Une bonne pratique en matière de sécurité est de ne pas partager les comptes utilisateurs.



8. Désactiver les modules inutilisés

Lors de l'installation d'un serveur web, un certain nombre de modules prédéfinis est activé, et ne sont jamais utilisés pour un serveur Web. Désactiver ces modules pour prévenir les attaques qui les ciblent. Par exemple le serveur Web de Microsoft (IIS) est configuré par défaut pour servir un grand nombre de types d'applications, (ASP, ASP.NET,...). La liste des extensions ne doit contenir que celles qui seront utilisées par le site ou l'application Web.

9. Utiliser les outils de sécurité fournis avec le serveur Web

Les éditeurs de serveurs web publient des outils pour aider les administrateurs à sécuriser l'installation des serveurs Web, on peut citer du coté de Microsoft l'outil URL scan. Aussi pour Apache un module appelé mod_security est fourni pour ce but. Bien que la configuration de ces outils est un processus fastidieux et peut prendre du temps, surtout avec des applications Web personnalisées, ils ajoutent un peu plus de sécurité et de tranquillité à l'esprit.

10. Surveiller et auditer votre serveur

Tous les logs de services réseau, d'accès au site Web, de serveur de base de données (Microsoft SQL Server, MySQL, Oracle,..) , et ceux du système d'exploitation doivent être surveillés et contrôlés fréquemment. Les fichiers logs ont tendance à donner toutes les informations sur une tentative d'attaque, et même d'une attaque réussie, mais la plupart du temps celles-ci sont ignorées.

11. Rester informé

Aujourd'hui, des informations et des conseils sur le système d'exploitation et les logiciels utilisés peuvent être trouvés gratuitement sur Internet. Il est très important de rester informé à propos des nouvelles attaques et les nouveaux outils, en lisant des revues liées à la sécurité (hakin9, MISC,..), la souscription aux newsletters (Deny All, CIV,..) forums ou tout autre type de communauté.

12. Utiliser des scanners

Les scanners sont des outils pratiques qui aident à automatiser et faciliter le processus de sécurisation d'un serveur et application web. Livrés souvent avec un scanner de port, scanner de sécurité réseau, vérificateur d'injection SQL, XSS, vérificateurs de problèmes de configuration, et d'autres outils très utiles pour se prémunir d'avantage.