Avis d'expert – Les logs, cette mine d'informations pour les pirates

La plupart des entreprises s'appuient sur des applications web pour leurs activités, mais celles-ci sont aussi un vecteur d'attaques pour les pirates et les utilisateurs internes malveillants. Cet été, des actes d'accusation ont été portés à l'encontre de 5 cybercriminels, suspectés d'avoir piraté 17 grandes entreprises et organisations, parmi lesquelles le Nasdaq, 7-Eleven et JetBlue Airways. La méthode utilisée par ces hackers est l'injection SQL, technique bien connue pour compromettre les applications… mais ce n'est pas la seule ! Les attaques de cross-site scripting (une faille de sécurité permettant d'injecter du contenu dans une page) et celles par déni de service sont également utilisées pour cibler les applications web.

Les applications sont des programmes complexes capables de s'exécuter sur plusieurs types d'infrastructures. La plupart sont hébergées sur des serveurs web tandis que les données sont exécutées sur des serveurs de bases de données. Tous les périphériques réseaux se connectent au système d'information en associant des noms d'hôtes à des adresses IP ; alors que certains outils de sécurité protègent uniquement l'infrastructure.

Les **applications** sont devenues un **risque de sécurité majeur**. En étant au cœur de l'environnement utilisateur, elles représentent un point d'entrée pour les attaques malicieuses. Ainsi, les injections SQL, les attaques de cross-site scripting et les attaques par force brute sont quelques unes des nombreuses façons de rendre les applications vulnérables.

De précieuses informations sont dans mes logs

Les logs générés par les applications sont une riche source d'informations sur le comportement des applications en elles-mêmes, en allant de la performance et de la disponibilité des applications à l'échange de données. Cependant, pour obtenir une réelle visibilité, il est nécessaire d'examiner les logs de données, et pas uniquement l'application en elle-même. En effet, les logs peuvent contenir de précieuses informations sur :

– les authentifications et les autorisations qui permettent d'accéder à l'application et aux données,

– l'activité de l'utilisateur, y compris les connexions et les déconnexions, les échanges et les requêtes,

– la disponibilité et les performances de l'application, de ses modules, de la base de données alimentant les serveurs hébergeant l'application et les bases de données connexes, ainsi que la connectivité au réseau,

– les modifications apportées aux données, aux applications et aux paramètres du système.

Les logs et les données sensibles

Les logs qui fournissent ce type d'informations peuvent être générés par de nombreuses sources directement rattachées à l'application. Bien souvent, les logs sont standards (syslog ou Windows eventlogs). D'autres fois, ils sont spécifiques à l'application. Pour avoir une image précise de l'état et du niveau de sécurité des applications, il est nécessaire d'associer toutes ces données pour leur donner un sens. Les logs d'infrastructure, qui proviennent des périphériques réseaux et des systèmes d'exploitation, ne permettent pas de détecter les attaques au niveau des applications. De même, ceux au niveau de l'application ne peuvent donner une visibilité complète d'une attaque par déni de service (DoS) ; tandis que les logs au niveau de l'infrastructure peuvent montrer une activité réseau suspecte, comme une adresse IP envoyant une multitude de requêtes.

Les logs peuvent également contenir des données sensibles telles que les informations des cartes de crédit ou des noms d'utilisateurs associés à des mots de passe, ce qui est une mine d'or pour les pirates ou les individus malveillants. Supprimer les données sensibles sur le poste de travail avant de transférer les logs est la manière la plus adéquate de procéder. Si les données sensibles doivent être stockées dans des journaux de logs, il est essentiel que ces données soient cryptées lorsqu'elles sont transférées et stockées. Simplement crypter les données lors du transfert n'est pas suffisant ; celles stockées doivent également être cryptées.

Restreindre l'accès aux logs peut également réduire les risques. L'authentification forte et la gestion des autorisations peuvent empêcher les utilisateurs malveillants d'accéder aux données sensibles à partir des logs.

Les applications et les données qui en découlent, sont devenues critiques pour l'activité de l'ensemble des entreprises. Disposer d'une visibilité sur l'ensemble de l'écosystème de l'application est essentiel et cela commence par une approche globale de la gestion de logs.

Voir aussi

Silicon.fr étend son site dédié à l'emploi IT
Silicon.fr en direct sur les smartphones et tablettes