Mesures anti-effraction pour un Endpoint DLP

Angela Lepadatu 2 avril 2016 Prévention des pertes de données

Les outils de prévention des pertes de données, comme tout autre logiciel, nécessitent des fonctions de sécurité. Ils garantissent qu'aucun pirate informatique, individu malveillant ou personnage curieux ne les contournent et parviennent à divulguer les données sensibles d'une organisation. Outre les capacités DLP spécifiques, les performances et le prix, la sécurité de la solution. Les mesures antieffraction sont également des critères clés qui rendent une solution DLP complète et puissante. Voici les principales caractéristiques de sécurité sur lesquelles la plupart des OSC s'enquièrent et que vous devriez également rechercher dans une solution DLP de point d'extrémité :

Protection contre la désinstallation du client

Notre DLP possède une architecture Client- Serveur. La partie serveur est la partie de gestion des politiques de sécurité, le logiciel client est installé sur chaque ordinateur du réseau qui met en application les politiques du serveur et collecte les flux concernant les transferts de données sensibles. Pour empêcher les utilisateurs de désinstaller le logiciel client, coupant ainsi la communication avec le serveur et révoquant les politiques DLP, le logiciel doit fournir la possibilité de configurer un mot de passe pour la désinstallation du client. Une autre des mesures de sécurité est de masquer l'icône de l'agent de la barre d'état système, de sorte que l'utilisateur ne peut pas identifier quel logiciel bloque les transferts de données spécifiques. C'est un must pour toute solution de prévention des pertes de données ; il va sans dire que sans l'agent, la DLP (politique de prévention des pertes de données) du poste connecté est inutile.

Vérification de l'intégrité du client

Étroitement lié à la fonctionnalité précédente, le contrôle d'intégrité du client vérifie si les utilisateurs tentent d'arrêter les agents, tout comme ils pourraient le faire avec n'importe quel service du gestionnaire de tâches. Cette fonction permet au client de vérifier et d'analyser automatiquement l'intégrité de ses composants. Immédiatement, le serveur reçoit par le biais des journaux d'action sur le poste la tentative d'arrêt du service, l'administrateur est informé par courriel de la tentative de contournement des politiques de sécurité, cela lui permet de d'activer immédiatement les actions adaptées. Un mécanisme de protection puissant ne permet pas de tuer ou d'arrêter le logiciel du client. Dans notre solution Endpoint Protector, si le processus est arrêté, il redémarre automatiquement.

Communication sécurisée entre le serveur et le client

Le protocole HTTPS ou tout autre protocole de communication sécurisé devrait être une norme pour la communication entre le serveur et le client. Cela afin de protéger les données contre toutes altérations durant le transport ou pour prévenir les attaques de tiers. Le HTTPS utilise des certificats uniques pour l'authentification. Ainsi, chaque fois que des modifications sont effectuées, le serveur demandera le certificat et le mot de passe corrects. Si ceux-ci ne correspondent pas, rien ne sera envoyé par le serveur. Nous utilisons TLS qui est plus sûr que SSL 1.0, 2.0 et 3.0. Seuls des chiffrages réputés sûrs sont utilisés pour la communication Client/Serveur.

Accès sécurisé via le protocole SSH

Un autre élément de sécurité à considérer lors de la mise en test d'une solution DLP. La première des actions est de définir avec votre partenaire Agréé ou Certifié, la politique et l'organigramme hiérarchique de votre DLP. Cela servira notamment de permettre un accès distant sécurisé à notre équipe de support. Ceci peut être établi via le protocole SSH, qui assure un canal de communication crypté dans une architecture Client/Serveur. De sorte qu'aucun tiers ne puisse intercepter les commandes du serveur DLP ou collecter les logs (enregistrement des actions et traçage des fichiers sur le poste client) réalisés par l'agents DLP.

Différentes permissions pour les administrateurs

Une partie importante des journaux enregistrés par les systèmes de prévention des pertes de données (DLP), comme par exemple les copies des fichiers transférés, les numéros de carte de crédit, les PII et autres actions ou fichiers ne pouvant être visible pour tous les administrateurs, Endpoint Protector, permet de configurer un compte Super Admin. Lui seul a accès à toutes les sections du serveur, mais il peut aussi limiter l'accès aux autres administrateurs pour les empêcher d'avoir une visibilité sur tous les onglets Rapports et Analyse.

Les fournisseurs de prévention des pertes de données ont pour mission de prévenir les fuites par tous les points de sortie possibles, de s'assurer que le système lui-même ne peut pas être contourné par des utilisateurs avancés, par des attaquants externes .etc..

Nous nous efforçons constamment de développer des fonctionnalités de sécurité pour nos solutions DLP et, comme toujours, nous nous tournons vers nos partenaires Distributeurs, revendeurs Certifiés, revendeurs Agréés qui remontent toutes les préoccupations sécuritaires de leurs clients pour optimiser notre solution DLP !

WaSaCa
128, Rue de la Boétie, 75008 PARIS
contact@wasaca.fr