Présentation de solution

Fuites de données : quelles solutions ?

La plupart des entreprises connaissent des fuites de données. Parfois le fait d'utilisateurs internes, ces vols de données sont généralement imputables à des personnes externes à l'entreprise. Les données quittent l'entreprise sous de nombreuses formes et via de multiples canaux. Les entreprises tentent d'endiguer ces fuites pour différentes raisons et avec plus ou moins de succès. Une grande étude a été réalisée à la demande d'Intel Security pour mieux comprendre et identifier les responsables des vols de données, les types de données ciblées et les méthodes d'exfiltration utilisées : *Intel Security 2016 Data Protection Benchmark Study* (Étude de référence 2016 d'Intel Security sur la protection des données).

Dans le *Rapport de McAfee Labs sur le paysage des menaces — Septembre 2016*, nous analysons les données de l'étude et présentons nos résultats. Cette étude a mis en lumière plusieurs éléments importants :

- Le délai entre les fuites de données et la découverte de la compromission s'allonge.
- Les prestataires de soins de santé et les fabricants sont des cibles faciles.
- L'approche préventive classique est de plus en plus inefficace au vu de l'évolution des cibles des vols de données.
- La plupart des entreprises ne surveillent pas le deuxième vecteur le plus courant des fuites de données.
- La prévention des fuites de données est implémentée pour les bonnes raisons.
- La visibilité est capitale.

Stratégies et procédures recommandées pour mettre en place une prévention des fuites de données efficace

Il est essentiel que les entreprises créent des stratégies et procédures de prévention des fuites de données pour éviter les transferts accidentels ou délibérés de données sensibles à des parties non autorisées. Un projet bien abouti de prévention des fuites de données commence par la planification et la définition des impératifs métier. Ainsi, en phase de planification, il est nécessaire d'aligner les stratégies de classification des données et de prévention des fuites de données sur les politiques de confidentialité et les normes de partage des données de l'entreprise. La définition d'impératifs métier rationnels et logiques permet de mieux délimiter le périmètre du projet de prévention des fuites de données et d'éviter la dérive des objectifs.

intel Security

Une étape importante du projet consiste à identifier les données sensibles dans l'entreprise. Les technologies d'analyse des serveurs et des terminaux permettent de classer les fichiers sur la base d'expressions régulières, de dictionnaires et de types de données non structurées. Les produits de prévention des fuites de données intègrent souvent des catégories de données sensibles, par exemple les données de cartes de paiement ou les données médicales personnelles, ce qui peut accélérer le processus de découverte. Il est également possible de créer un système de classification personnalisé pour identifier des types de données propres à l'entreprise.

L'exécution de cette étape peut être compliquée par l'hébergement dans le cloud d'applications approuvées et interdites par le service informatique, et leurs données connexes. En ce qui concerne les données approuvées hébergées dans le cloud, les données sensibles doivent idéalement être identifiées lors du processus d'abonnement au service cloud. Lorsque c'est le cas, la classification de ce type de données est relativement simple.

Cela dit, les groupes fonctionnels au sein des entreprises évitent parfois de passer par le service informatique pour satisfaire leurs objectifs métier et s'abonnent aux services cloud de leur propre chef. Si l'équipe informatique ne connaît pas l'existence de ces services et des données qu'ils hébergent, il existe un risque accru de fuites de données. Par conséquent, il est important, lors de cette étape, de collaborer avec les groupes fonctionnels afin d'identifier les emplacements des données dans le cloud et d'utiliser le processus décrit précédemment pour catégoriser celles-ci.

Au terme du processus de découverte des données sensibles, l'implémentation de solutions de prévention des fuites de données au sein du réseau approuvé et sur tous les terminaux peut offrir la visibilité et le contrôle requis sur les données importantes, au repos et en mouvement. Il est utile d'implémenter des stratégies pour détecter un accès ou un mouvement imprévu de données sensibles. Des événements tels que le transfert de données sensibles sur des clés USB ou via le réseau vers un emplacement externe peuvent être soit une activité normale, soit une action délibérée ou accidentelle susceptible d'entraîner des fuites de données.

Une formation de sensibilisation à la sécurité bien conçue peut diminuer la probabilité de telles compromissions. Des écrans de justification peuvent rappeler aux utilisateurs de prendre les précautions appropriées lors du transfert de données sensibles et les sensibiliser aux stratégies de protection des données en vigueur tout au long de leurs journées de travail. Ainsi, un écran de justification peut avertir les utilisateurs que leur transfert de données sensibles est contraire à la politique d'entreprise et leur fournir des solutions alternatives, par exemple en leur conseillant de supprimer les données sensibles avant de réessayer le transfert.

Les propriétaires des données sont généralement les mieux placés pour déterminer comment celles-ci sont utilisées et quels sont les usages permis. Il serait donc préférable de leur confier la mission et la capacité d'effectuer le tri dans les incidents de fuites de données. La division des responsabilités entre les propriétaires de données et l'équipe de sécurité réduit la possibilité qu'une équipe contourne les stratégies de protection des données.

Après avoir déterminé les mouvements de données approuvés et intégré les stratégies contrôlant ces mouvements aux solutions de prévention des fuites de données, vous pouvez activer les stratégies de blocage des transferts non autorisés de données sensibles. Lorsque le blocage est activé, les utilisateurs ne sont pas en mesure d'effectuer des actions contraires aux stratégies définies. Selon les impératifs métier, il est possible d'optimiser les stratégies et les règles afin de garantir une certaine flexibilité et de laisser aux utilisateurs la possibilité d'accomplir leur travail tout en assurant la sécurité des données.

À mesure que le projet de prévention des fuites de données avance, il est important de valider et d'optimiser les stratégies à intervalles planifiés. Il arrive que les stratégies soient trop restrictives ou, au contraire, trop laxistes, les premières affectant la productivité tandis que les secondes posent un risque pour la sécurité.

Comment Intel Security peut vous aider à vous protéger contre les fuites de données

McAfee DLP Discover

Pour sécuriser efficacement vos données, la première étape consiste à comprendre où elles se trouvent et quelle est leur nature. McAfee DLP Discover simplifie cette étape grâce à plusieurs fonctionnalités de façon à vous protéger contre l'exfiltration de données :

- Identifiez les classifications à détecter au sein de l'environnement approuvé à l'aide de classifications intégrées (p. ex. HIPAA, PCI ou SOX) ou personnalisées.
- Effectuez une analyse d'inventaire et une évaluation à l'aide des classifications identifiées afin de comprendre quels types de données résident au sein de l'environnement approuvé et où elles se trouvent. Évaluez les infractions à la stratégie en place dans l'interface McAfee DLP Discover.
- Exécutez une analyse de correction afin de localiser les données stockées dans des emplacements non autorisés et de les transférer vers un emplacement approuvé.
- Les analyses d'inventaire et de correction peuvent être réalisées sur des ressources locales (telles que des partages réseau) ou de cloud (telles que Box).
- Élaborez de nouvelles stratégies de protection des données sur la base des résultats des analyses McAfee DLP Discover.

McAfee DLP Endpoint

McAfee DLP Endpoint surveille les données et empêche les exfiltrations en local, hors site et dans le cloud. En plus de surveiller rapidement les événements en temps réel, vous pouvez appliquer des stratégies de sécurité gérées de façon centralisée et générer des rapports détaillés en matière de prolifération et d'investigation numérique, le tout sans perturber les opérations habituelles.

- Au terme de la phase de découverte, élaborez des stratégies de protection des données, dont la violation éventuelle déclenchera la génération de rapports. Vous disposerez ainsi des informations nécessaires pour mieux comprendre les mouvements de données au sein de votre entreprise et pourrez appliquer des règles de blocage. McAfee DLP inclut des classifications intégrées (HIPAA, SOX, PCI et ITAR, p. ex.), que vous pouvez utiliser pour identifier les données au sein de votre entreprise.
- Créez des messages de sensibilisation pour permettre aux utilisateurs de mieux comprendre les stratégies de protection des données et d'en tenir compte lors des transferts journaliers de données. Ces fenêtres pop-up personnalisables sont très utiles en ce qu'elles réduisent les transferts de données risqués par les collaborateurs.
- Consultez le Gestionnaire d'incidents afin d'identifier les propriétés des données transférées vers des emplacements non autorisés, notamment la manière dont ces transferts se déroulent et les personnes à l'origine de ceux-ci.
- Une fois les stratégies de protection des données élaborées et adaptées aux besoins de l'entreprise, activez le blocage des transferts de données non autorisés.
- Activez les classifications manuelles de façon à permettre aux utilisateurs de classer les documents qu'ils créent. Étant propriétaires des données, ces utilisateurs seront normalement mieux à même de déterminer le niveau de sensibilité des documents lorsque le moteur de classification automatique se révèle incapable de détecter les données non structurées. Cette fonctionnalité intégrée à McAfee DLP Endpoint ne requiert aucun outil tiers supplémentaire.
- Pour empêcher l'accès à vos données sensibles par des applications inconnues et bénéficier ainsi d'une protection supplémentaire, créez et mettez en œuvre une règle de protection de l'accès des applications qui s'appuie sur McAfee Threat Intelligence Exchange. Une telle règle permet aux applications autorisées de transférer des données sensibles et empêche les applications non vérifiées ou malveillantes d'y accéder.

McAfee DLP Monitor
McAfee DLP Monitor collecte et suit les données en mouvement sur l'ensemble du réseau et génère les rapports correspondants. De cette façon, la solution détecte facilement les menaces inconnues susceptibles de cibler vos données et peut prendre les mesures requises pour les protéger.

- Détectez les violations potentielles au sein de votre réseau grâce à l'activation de stratégies et de règles intégrées pertinentes.
- Créez des stratégies et des règles personnalisées supplémentaires, notamment pour surveiller les transferts de données sensibles vers le cloud.
- Des investigations numériques permettent de mettre en corrélation les événements, passés et présents, associés à un risque, de détecter les tendances des risques et d'identifier les menaces. McAfee DLP Monitor permet à vos experts en sécurité d'appréhender rapidement la situation et d'élaborer des règles et stratégies pour y remédier.
- Créez des filtres de capture supplémentaires afin d'exclure les données non pertinentes et d'adapter les règles pour réduire les faux positifs.
- Configurez des alertes pour l'envoi de notifications à l'attention des expéditeurs, des destinataires, des propriétaires de données et des administrateurs système en cas de violation des stratégies.

McAfee DLP Prevent
McAfee DLP Prevent vous protège contre les fuites de données en s'assurant que les données ne quittent le réseau que lorsqu'elles y sont autorisées — que ce soit par le biais de la messagerie électronique, de la messagerie web, de la messagerie instantanée, de wikis, de blogs, de portails, de sites HTTP/HTTPS ou de transferts FTP. Identifier rapidement les tentatives d'exfiltration et y remédier dans les plus brefs délais est essentiel pour conserver les données importantes à l'abri des indélicats et se préserver des battages médiatiques qui accompagnent les compromissions.

- Pour empêcher les transferts de données non autorisés entre des passerelles de messagerie ou des serveurs proxy web, intégrez McAfee DLP Prevent avec des agents de transfert des messages ou des serveurs proxy web au moyen de stratégies intégrées.
- Créez des règles McAfee DLP Prevent pour autoriser ou bloquer les documents sensibles en fonction de leur pourcentage de correspondance.
- Utilisez les modèles DLP intégrés pour empêcher le transfert de données sensibles vers le cloud.
- Analysez les rapports sur les incidents de sécurité et adaptez les stratégies pour réduire les faux positifs et optimiser la continuité des activités.
- Configurez des alertes pour l'envoi de notifications à l'attention des expéditeurs, des destinataires, des propriétaires de données et des administrateurs système en cas de violation des stratégies.

Lectures complémentaires

Communauté Intel Security Expert Center

- McAfee Data Loss Prevention

McAfee. Part of Intel Security.
Tour Pacific
13, Cours Valmy - La Défense 7
92800 Puteaux
France
+33 1 47 62 56 09 (standard)
www.intelsecurity.com