DATA LEAK PREVENTION (DLP) :

ÉTAT DES LIEUX

Oussama EL SAMAD

LES NOTES STRATÉGIQUES

Les notes σtratégiques

Les notes stratégiques

Policy Papers – Research Papers

A propos de l'auteur
Consultant senior « cybersécurité » chez CEIS, Oussama EL SAMAD est ingénieur télécommunication et réseaux de formation. Après diverses expériences dans le conseil et dans la banque, il intervient dans le cadre de missions d'audit et de conseil technique, d'analyses de marché et de veille « sécurité ».

A propos de CEIS

- CEIS est une société de conseil en stratégie dont les actions couvrent l'ensemble de la chaîne de valeur du circuit de décision : de la réflexion stratégique à la mise en œuvre opérationnelle.

- La spécificité de CEIS est de s'appuyer sur un fort socle informationnel pour accompagner ses clients dans le développement et la sécurisation de leurs activités en France et à l'international grâce à des solutions innovantes de business & market intelligence, de gouvernance des risques et de management de l'innovation.

- CEIS intervient à 80 % pour des clients privés (grands groupes, clusters et pôles de compétitivité, PME-PMI) et à 20 % pour des clients publics (ministères, administrations françaises et européennes, collectivités territoriales). Elle a notamment développé des expertises dans les secteurs suivants : défense et sécurité, IT, transport et logistique, énergie, industrie pharmaceutique, grande distribution, agro-alimentaire, banque et assurance.

- CEIS comprend une centaine de consultants et est implantée à Paris, Lille et Metz. Elle possède par ailleurs des bureaux ou filiales à Bruxelles, Moscou, Kiev, Pékin, Astana (Kazakhstan), Doha (Qatar) et Abou Dhabi (Emirats arabes unis).

Sommaire

Introduction 6

Un cadre légal et règlementaire de plus en plus contraignant 8

Le marché du DLP 10

Comment déployer un dispositif de DLP ? 15

Règles d'Or 18

Pour aller plus loin 18

Introduction

Dans un contexte où les systèmes d'informations sont de plus en plus ouverts, et où l'information irrigue l'ensemble de l'entreprise, la protection contre les fuites de données doit être une préoccupation majeure en matière de sécurité informatique. Au fur et à mesure du développement de nouveaux usages et de l'émergence de nouvelles technologies (réseaux sociaux, Web 2.0, mobilité, Cloud, Big Data…), cette protection devient cependant de plus en plus complexe.

L'information a une valeur marchande

La cybercriminalité s'oriente de plus en plus vers le vol et/ou le détournement de données compte tenu de la valeur marchande que représente l'information.
Quelques exemples récents de fuite de données :

- Shell - Février 2010 - une base contenant des informations personnelles sur plus de 176000 employés, sous-traitants et prestataires est transférée à des organisations et lobbyistes opposés à la société ;

- HSBC - Décembre 2009 - des informations sur les comptes et transactions bancaires de près de 3 000 clients sont divulguées par un ancien responsable du support informatique. Un fichier clients, un bilan, des données personnelles, ou encore un savoir-faire, se monnaient aisément et chers sur les marchés parallèles.

L'entreprise se doit donc de protéger ses données. Elle y est conduite par un cadre législatif de plus en plus contraignant.

Les outils traditionnels sont insuffisants

Les outils « traditionnels » de sécurité (firewall, IPS, anti-virus…) ne sont plus adaptés. Ils se concentrent sur la protection des infrastructures (réseaux, serveurs, postes de travail…) et n'ont pas vocation à protéger des utilisations et des transferts illégitimes de données. Les organisations doivent désormais déployer des solutions spécifiques pour prévenir les fuites de données.

Des conséquences désastreuses

Qu'elle soit provoquée par une malveillance ou par une erreur, la fuite de données est susceptible de déstabiliser l'activité d'une entreprise. En fonction de la sensibilité des données concernées, les conséquences d'une seule fuite d'information peuvent être désastreuses :

- Perte de revenus,
- Amendes sévères,
- Réputation de l'entreprise entachée,
- Perte de la confiance des clients.

Objectifs de l'étude

Les objectifs de cette étude sont :

- De sensibiliser les entreprises à la nécessité de protéger les données sensibles,
- De rappeler le cadre légal et règlementaire entourant les fuites de données,
- De réaliser une analyse du marché des solutions de DLP ou « Data Leak Prevention »,
- De rappeler quelques bonnes pratiques en matière de mise en place de dispositif de DLP.

Un cadre légal et règlementaire de plus en plus contraignant

Le cadre légal et règlementaire influe beaucoup sur l'approche des entreprises en matière de sécurité des systèmes d'informations en général et de protection contre les fuites de données en particulier. Les entreprises françaises ayant des activités à l'étranger peuvent être concernées par plusieurs cadres, différents selon les pays concernés.

Code Civil

Article 1382 : tout fait quelconque qui cause à autrui un dommage, oblige celui par la faute duquel il est arrivé, à le réparer.

Article 1384-1 : extension de l'article 1382, l'entreprise est responsable d'un dommage causé à autrui par un de ses salariés dans le cadre de sa mission.

Code Pénal

Article 226-22 : « Le fait, par toute personne qui a recueilli, à l'occasion de leur enregistrement, de leur classement, de leur transmission ou d'une autre forme de traitement, des données à caractère personnel dont la divulgation aurait pour effet de porter atteinte à la considération de l'intéressé ou à l'intimité de sa vie privée, de porter, sans autorisation de l'intéressé, ces données à la connaissance d'un tiers qui n'a pas qualité pour les recevoir est puni de cinq ans d'emprisonnement et de 300 000 Euros d'amende. La divulgation prévue à l'alinéa précédent est punie de trois ans d'emprisonnement et de 100 000 Euros d'amende lorsqu'elle a été commise par imprudence ou négligence.

Loi Godfrain

Les articles 462-2 à 462-7 considèrent comme délits les actes suivants et prévoient des sanctions sévères pour leurs auteurs :

- L'accès ou le maintien frauduleux dans un système informatique
- Mis en forme : Police :Gras
- L'atteinte volontaire au fonctionnement du système informatique (suppression ou modification des données…)
- La tentative de ces délits

CNIL

Loi du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés dite« Informatique et Libertés » (modifiée par la loi n°2004-801 du 6 août 2004relative à la protection des personnes physiques à l'égard des traitements de données à caractère personnel). Selon l'article 11 de la loi « Informatique et Libertés », tout traitement automatisé de données à caractère personnel doit être déclaré ou soumis à l'avis de la CNIL. L'article 34 impose aux entreprises de prendre les précautions nécessaires pour préserver la sécurité des données et empêcher qu'elles soient déformées, endommagées, ou que des tiers non autorisés y aient accès.

Directive européenne « Vie privée et communication électronique »

L'article 34 bis de la loi de 1978 transpose l'obligation de notification des violations de données à caractère personnel prévue par la directive 2002/58/CE modifiée dite «Paquet Télécom». Cette obligation a été insérée dans la loi informatique et libertés bien qu'elle ne concerne pas toutes les entreprises, mais seulement les fournisseurs de services de communications électroniques. Des mesures d'application ont été précisées par le décret n°2012-436 du 30 mars 2012.

Secret Bancaire

Article 57 : l'article 57 de la loi bancaire de 1984, protège l'intérêt privé du client ; Le banquier est tenu au secret professionnel et doit garder confidentiels tous les faits non publics que lui a confiés son client.

Loi de Sécurité Financière

Comme la loi américaine Sarbanes-Oxley, la Loi de Sécurité Financière repose principalement sur une responsabilité accrue des dirigeants, un renforcement du contrôle interne et une réduction des sources de conflits d'intérêt. L'environnement de contrôle interne doit garantir que l'ensemble des opérations s'est déroulé conformément aux procédures et doit correspondre à l'activité réelle de l'entreprise. Ceci implique une forte intégration des procédures de contrôle avec les systèmes d'information et les différents intervenants participant à la réalisation des processus comptables et financiers et leur contrôle.

Accords de Bâle (dernier Bâle 3)

L'objectif des accords de Bâle est de renforcer la résilience des grandes banques internationales et réduire les risques, pour ne pas revivre les crises successives qui ont secoué les marchés financiers ces dernières années. Des évolutions réglementaires qui ne sont pas sans conséquences sur les systèmes d'informations. Pour répondre aux exigences de Bâle 3, il est donc indispensable de disposer d'un système d'informations dont la gouvernance des données est au coeur des préoccupations, afin d'améliorer la transparence et la fiabilité de l'environnement.

Réforme Solvency II

Solvabilité II est une réforme réglementaire européenne du monde de l'assurance. Son objectif est de mieux adapter les fonds propres exigés des compagnies d'assurances et de réassurance avec les risques que celles-ci encourent dans leur activité. L'Autorité de Contrôle porte notamment son attention à l'auditabilité des modèles et à la qualité des données. Solvency II amène les sociétés d'assurance et leurs prestataires à repenser certains aspects de leurs organisations et mettre en place un système d'information performant afin de disposer de données de qualité, hautement sécurisées.

PCI-DSS

Le Payment Card Industry Data Security Standard (PCI DSS) est un standard de sécurité des données pour les industries de carte de paiement créé par le comité PCI SSC pour les plus importantes entreprises de carte de débit et crédit. Les établissements manipulant des données de cartes bancaires doivent être conformes au standard PCI-DSS sous peine d'amendes qui peuvent très lourdes en cas d'incident provoquant la divulgation de données.

Banque de France

Règlement CRBF 97-02 : exigences en matière de contrôle interne et contrôle de conformité. Impacts directs sur la sécurité des systèmes d'informations.

Le marché du DLP

Le marché américain est en avance

Ayant vu le jour il y a douze ans, le marché américain du DLP est aujourd'hui le plus développé et le plus mature. Non seulement la plupart des principaux fournisseurs de solutions de DLP sont américains (comme le montre le tableau), mais la majorité de leurs références clients actuels se situent outre-Atlantique. En Europe, c'est en Grande-Bretagne que l'on retrouve le plus de références.

Nom fournisseur	Pays
Bull	France
CA	USA
Checkpoint	Israël
Cisco	USA
Code Green Networks	USA
Covertix	Israël
Credant	Israël
EMC (RSA)	USA
IBM	USA
Intel (McAfee)	USA
Lumension	USA
Microsoft	USA
NetApp	USA
NetWitness	USA
Symantec	USA
Syncsort	USA
Trend Micro	USA
Trustwave	USA
Varonis	USA
Verdasys	USA
Wave	USA
Websense	USA

Stratégie d'attente

Jusqu'à présent, la stratégie des entreprises françaises a souvent été une stratégie d'attente :

- Une attente de l'incident, en pensant que les fuites de données n'arrivent qu'aux autres,
- Une attente de maturité du marché et des produits,
- Une attente de la mise en place d'une stratégie complète de protection des données, sans laquelle aucune technologie DLP ne permettra d'atteindre l'objectif recherché.

Prise de conscience

Les facteurs de développement du marché du DLP sont nombreux : explosion du volume des données, externalisation, cloud computing, réseaux sociaux, BYOD... Mais la prise de conscience des conséquences que peut avoir une fuite de données sensibles reste le principal élément déclencheur de l'intérêt d'une entreprise pour ce type de solutions.

Un frémissement du marché ?

Le DLP n'a pour l'instant pas décollé en France. Les déploiements restent rares et parcellaires. La mise en place de démonstrateurs ou de pilotes ainsi que la multiplication des offres témoignent cependant d'un frémissement du marché. Même des petits éditeurs de solutions antivirales comme GData tentent de pénétrer le marché avec un produit comme GData End Point Protection.

Les opérations de M&A sur le marché du DLP ont été très nombreuses ces dernières années, ce qui prouve un regain d'intérêt pour ce type de solutions de la part des grands acteurs de la sécurité informatique, qui ont à ce jour quasiment tous des solutions de DLP à leur catalogue.

Dernières opérations de M&A réalisées dans le secteur du DLP : Vontu racheté par Symantec, Vericept par Trustwave, Reconnex par McAfee, Port Authority par Websense, Tablus Content Sentinel par EMC, Orchestria par CA, Provilla Data DNA par Trend Micro.

Côté solutions, Symantec, CA, McAfee, RSA et Websense sont les leaders du marché mais leurs solutions s'adressent avant tout aux grandes entreprises disposant de capacités/ressources internes importantes et de processus aboutis et opérationnels. Source Gartner - juin 2011

Source Gartner - juin 2011

Le DLP en chiffres

- 40 % des entreprises commencent par faire du DLP sur les flux réseau uniquement,
- 20 % commencent par du Data Discovery,
- 40 % commencent par du End Point,
- En France, en 2010, 9 % des entreprises ont déployé et utilisent du DLP (source Clusif).

Zoom sur deux des principaux acteurs

RSA

Nom de la solution : RSA Data Loss Prevention Suite.

Nombre de références clients France / Monde : 5 / 800.

Principal client : Microsoft.

Points forts : intégration complète avec VMware vShield Zones, Microsoft et Cisc IronPort. Outil intéressant de classification des données par niveau de sensibilité.

Points faibles : solution disponible en langue anglaise uniquement.

Prix : à partir de 500€ pour 10 utilisateurs maintenance incluse.

Websense

Nom de la solution : Websense Data Security Suite.

Nombre de références clients France / Monde : 10 / 600.

Principaux clients français : Lafarge, Toyota.

Points forts : intégration complète avec des outils de SIEM (HP ArcSight), et de supervision (ex. HPOV). Offre DLP as a Service (SaaS). Agent disponible sur Linux. Forte expérience, l'un des premiers acteurs dans le domaine du DLP.

Points faibles : solution disponible en langue anglaise uniquement.

Quelles évolutions ?

Devant la réticence des décideurs et afin de relancer le marché, les éditeurs de DLP misent sur l'innovation. De nouvelles fonctionnalités devraient ainsi voir le jour dans les prochaines versions des solutions. Parmi ces futures fonctionnalités, les éditeurs ont actuellement dans leurs plans de développement :

- L'intégration aux autres modules de protection du SI (antivirus, DRM…),
- L'intégration aux solutions de collecte de logs et de reporting,
- L'intégration aux modules de gestion des identités et des habilitations,
- L'extension aux équipements mobiles, notamment les smartphones,
- Le chiffrement automatique des données sensibles découvertes par le moteur DLP.

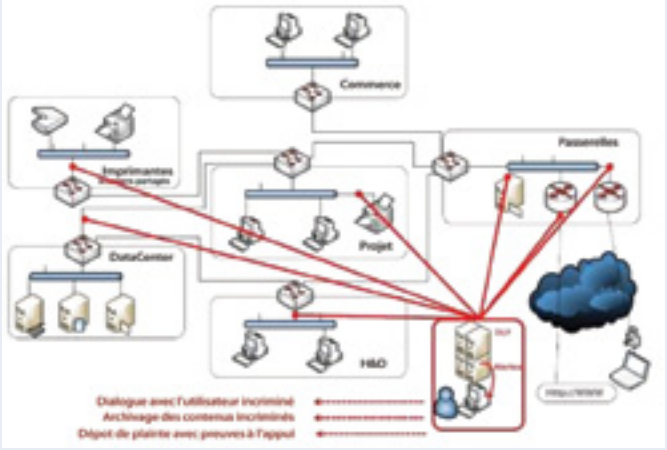
Pour ce faire, les éditeurs de solutions de DLP ont multiplié accords et partenariats. Avec pour résultat que certaines de ces fonctionnalités sont aujourd'hui proposées ou en cours de maturation.
Les plus actifs sont McAfee, Symantec, CA, Liquid Machines, et même Microsoft.

Zoom sur BullWatch

La solution DLP du fournisseur français Bull est baptisée BullWatch. L'architecture BullWatch est constituée d'un ensemble de capteurs d'information disséminés dans l'entreprise, qui remontent les informations utiles à une console d'administration, exploitée par le référent DLP de l'organisation. La reconnaissance de contenus confidentiels se fera sur mots-clés, expressions ou marqueurs préalablement positionnés, mais également par comparaison de tous les contenus textuels (documents bureautiques, corps de messages, discussions…) avec des contenus de référence.

Les capteurs peuvent s'adapter à n'importe quel segment du réseau de l'organisation ; le traitement se fera éventuellement sur place si le flux est important, afin d'éviter que trop d'informations ne soient dupliquées vers le coeur de la solution :

- Sur les liens raccordant l'organisation à Internet ou à d'autres implantations,
- Sur les points d'entrée des Data Centers ou des pools d'imprimantes,
- Sur des points particuliers à définir.



Au passage, le projet DLP pourra amener l'organisation ciblée à rationaliser l'usage de l'outil numérique dans un objectif de contrôle des communications :

- Les accès aux ressources d'impression, de stockage seront regroupés,
- Seuls les moyens de chiffrement déclarés seront autorisés,
- Les flux non-identifiés pourront faire l'objet d'investigations.

A noter : le moteur d'inspection des contenus peut décoder plus de 200 protocoles et applications différentes (les messageries d'entreprise et « Web », les forums, les chats, les réseaux sociaux, les flux d'impression) ; il peut être envisageable de lui adjoindre un composant de « speech-to-text » afin d'inspecter également les conversations vocales.

Source www.amesys.fr

Zoom sur SmartCipher

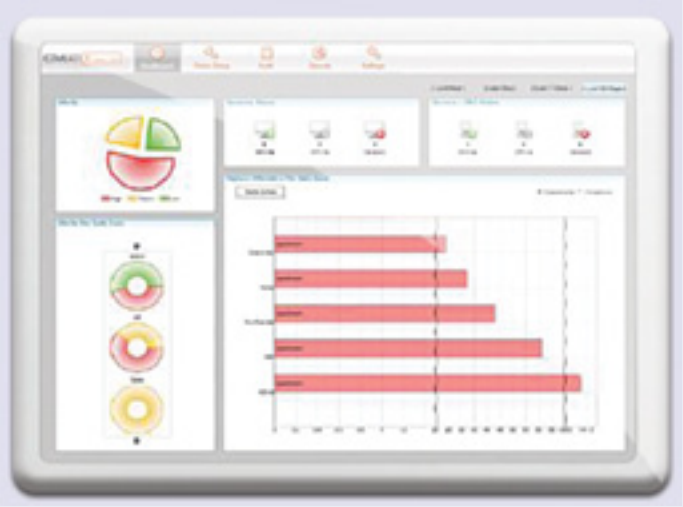
SmartCipher est une solution proposée par la société israélienne Covertix. Elle agit au niveau des fichiers en y associant une empreinte et une politique d'usage. Ces dernières circulent avec les fichiers au sein et en dehors de l'organisation. Le système marque automatiquement les fichiers en fonction de la localisation, du contenu et du contexte, sans implication nécessaire de l'utilisateur. Les informations sont alors suivies en permanence même lorsque l'utilisateur est hors ligne: la politique d'usage étant rattachée au fichier, une connexion au serveur n'est pas requise.

SmartCipher offre une vue claire et exhaustive de l'utilisation, légale ou frauduleuse, des données grâce des tableaux de bord. En cas de violation de la politique de sécurité, le système peut soit émettre une alerte soit bloquer la manipulation. Dès qu'un utilisateur autorisé quitte l'organisation, l'accès aux données sensibles lui est par exemple immédiatement impossible. Une solution « webisée » et sans installation de client nécessaire permet un partage de fichiers sécurisé avec les tiers ainsi que les utilisateurs de PDA et smartphones.

Trois modes opératoires sont prévus.

- Mode Découverte : la solution surveille les manipulations sur le fichier et fournit un panorama exhaustif de l'usage.
- Mode Simulation : la politique de protection est créée, mais pas mise en oeuvre.
- Mode Actif : activation des règles et politiques de l'organisation.

Tableau de bord SmartCipher



Source www.covertix.com

Comment déployer un dispositif de DLP ?

Une brique sécuritaire complémentaire

Le DLP n'est pas une solution miraculeuse qui permettrait de sécuriser dès son implémentation les données d'une entreprise et de prévenir leur fuite. Envisager un projet DLP avec cette idée en tête serait une perte de temps et d'argent.

En réalité, le DLP n'est qu'une brique sécuritaire complémentaire qui vient s'ajouter à une panoplie de solutions sécuritaires existantes. En d'autres termes, il faudra avoir déjà mis en place une panoplie de processus organisationnels et de solutions techniques cohérentes avant de s'occuper des fuites de données.

Le DLP doit intervenir après la mise en place d'une sécurité périmétrique solide, d'un contrôle d'accès et d'une gestion des habilitations efficaces, ainsi que d'une gestion des incidents de sécurité.

Le dispositif de DLP va ensuite s'appuyer sur l'ensemble de ces technologies et processus existants.

Par où commencer ?

C'est l'éternelle question lorsque l'on envisage de déployer un dispositif de DLP. Elle est d'autant plus légitime que le nombre de références clientes et de dispositifs matures sur le marché français est faible.

La première étape d'un tel chantier doit donc consister à déterminer la cible à couvrir et les risques susceptibles d'affecter celle-ci :

- Quelles sont les données qu'il est nécessaire de protéger ?
- Quels sont les principaux vecteurs de fuite empruntés par ces données ?

Trop de secret tue le secret

Toutes les données n'ayant pas la même sensibilité, il est nécessaire de bien cibler celles qui sont les plus sensibles et dont la fuite pourrait avoir d'importantes conséquences pour l'organisation. Ce sont ces données qui doivent être protégées dans un premier temps ; les autres suivront en fonction de leur sensibilité et de la maturation du dispositif.

Cette étape est nécessaire quel que soit le type de dispositif DLP envisagé. Démarrer avec les données les plus sensibles suppose d'avoir classifié les données de l'organisation. Dans le cas contraire, une démarche de classification est nécessaire. Il n'est pas raisonnable de démarrer un dispositif de DLP en voulant protéger contre la fuite l'ensemble des données de l'organisation.

Tagger la donnée à sa création

Certaines solutions de DLP préconisent de protéger les données «à la source». Il s'agit concrètement de déterminer une empreinte pour les données «retenues» en phase de découverte des données sensibles ou pour les données jugées sensibles dès leur création.

Cette empreinte permettra ensuite d'en suivre la circulation, même si le document est altéré ou si une partie seulement est copiée. Ce type de solutions est très ambitieux. Il est en effet très difficile de maintenir à jour un inventaire des données sensibles et de savoir où elles résident, celles-ci changeant en permanence de niveau de sensibilité, de localisation, de propriétaire. Des données sensibles nouvelles peuvent également être créées à tout moment.

Canaux empruntés

Une fois les données sensibles définies, d'autres types de dispositifs prévoient d'identifier les canaux à travers lesquels une fuite de données pourrait avoir lieu (interface réseau, mail, USB, imprimante…) et d'y appliquer une politique de sécurité personnalisée afin d'empêcher les données sensibles d'y transiter.

Mais les données sensibles peuvent transiter par beaucoup de canaux de diffusion. Tous les canaux du système d'information sont susceptibles d'être utilisés. Il s'agit donc de se focaliser sur les canaux qui sont le plus sujets à une fuite de données et de les sécuriser en priorité.

Démarrer sur un périmètre réduit

Devant la multitude de solutions possibles, leur manque de maturité et le manque de maîtrise par les responsables de la sécurité et les opérationnels, il est plus sage de définir un périmètre réduit sur lequel le dispositif va démarrer, et le faire évoluer par étapes jusqu'à arriver à une maîtrise complète des données.

Les étapes précédentes permettent de définir un périmètre précis en termes de données à protéger, de périphériques et de canaux. On peut également y ajouter une population, une entité ou un site géographique déterminé.

Dans la plupart des entreprises ayant déployé un dispositif de DLP, ce dernier ne s'applique qu'à un sous-ensemble de la société, non à l'intégralité.

Implication du management

Avoir l'appui du management pour ce type de projet n'est pas chose facile. On constate même souvent une réticence. Cette réticence est notamment due à :

- L'impact du projet sur le mode de travail et la performance des utilisateurs,
- La complexité du projet,
- Les coûts de démarrage et les coûts récurrents,
- Les compétences internes requises.

Obtenir des résultats rapides, probants et à moindre coût est donc la clé pour obtenir l'appui du management et même l'acceptation par tous les acteurs. D'où l'intérêt de démarrer le projet sur un périmètre réduit.

La classification des données n'est ni un prérequis ni un objectif

Il est très difficile de classifier toutes les données d'une entreprise et de maintenir à jour un inventaire. Contrairement aux idées reçues, et qui ont freiné beaucoup de projets DLP, cette classification des données n'est pas un prérequis à la mise en place d'un dispositif DLP. Comme il est possible de démarrer un dispositif DLP sur un périmètre réduit, l'intégration des données pourra se faire de manière progressive et itérative.

Le DLP ne résoudra pas tous les problèmes

Il est illusoire de penser que le DLP permettra d'assurer à lui seul une couverture totale contre les fuites de données.

Pour obtenir des résultats probants (couverture homogène, contrôle des fuites, adhésion des utilisateurs, appui du management…), il sera donc nécessaire d'organiser son dispositif DLP en s'appuyant sur les technologies et les processus organisationnels existants : analyse des risques, gestion des incidents de sécurité, alertes, contrôle d'accès, gestion des dérogations, chiffrement…

Gestion du changement

Mener à bien un projet de DLP va aussi nécessiter de mettre à contribution tous les utilisateurs du système d'information, chacun ayant un rôle à jouer dans le bon déploiement du dispositif : management, responsables métiers, managers, service juridique et bien sûr utilisateurs finaux.

Sensibilisation des utilisateurs

Il est toujours très difficile d'empêcher les utilisateurs légitimes malveillants de contourner la solution, même si celle-ci peut leur compliquer la tâche. Un dispositif de DLP vise donc en premier lieu la prévention contre les fuites dues à la négligence ou à l'inconscience des utilisateurs légitimes. D'où l'importance de la sensibilisation des utilisateurs.

La sensibilisation des utilisateurs ne saurait être considérée comme la étape passagère d'un projet DLP : elle ne commence et ne se termine pas avec le projet. La sensibilisation des utilisateurs est un processus organisationnel indépendant continu qui vise à faire prendre conscience aux utilisateurs de la nature sensible des données qu'ils manipulent et de l'existence d'un cadre règlementaire et d'obligations légales.

Pour favoriser l'adhésion des utilisateurs, il est important d'expliquer les bonnes pratiques et les modalités d'application des nouvelles règles introduites par le dispositif de DLP et de les impliquer dans la gestion de la politique de sécurité.

Règles d'Or

Respecter les règles suivantes peut vous aider à mieux réussir votre projet de DLP et à protéger vos données sensibles :

- Déterminer les réglementations auxquelles son entreprise est soumise,
- Identifier les risques liés à une éventuelle fuite de données,
- Impliquer toutes les parties prenantes,
- Déterminer la solution cible en fonction de ses besoins,
- Démarrer sur un périmètre réduit,
- Avoir l'appui du top management,
- Gérer le changement,
- Sensibiliser les utilisateurs,
- Définir des règles et des stratégies.

Pour aller plus loin

CEIS propose des prestations d'étude personnalisées :

- Etude technique et fonctionnelle détaillée,
- Comparatif des principales offres du marché par rapport à vos besoins,
- Préconisations dans le choix d'une solution technique de DLP,
- Maquettage des solutions,
- Guide pratique de déploiement progressif.

CEIS est également en mesure de vous accompagner dans la réalisation de votre projet DLP (classification des données, sensibilisation, conduite du changement…).

CEIS

LES NOTES STRATÉGIQUES

Déjà parus :

Nouvelles guerres de l'information : le cas de la Syrie. Novembre 2012

La sauvegarde de la BITD italienne : quel rôle pour les districts aérospatiaux ? Mai 2012

Enjeux caucasiens : quelles recompositions d'alliances ? Juin 2012

Puissance aérienne française et format de l'armée de l'air
Le cas de l'aviation de combat. Juin 2012

L'assistance militaire à des armées étrangères, l'avenir de l'action indirecte. Juillet 2012 – english version available

Le F35/JSF : ambition américaine, mirage européen. Juillet 2012

Ariane et l'avenir des lancements spatiaux européens. Août 2012

Compagnie Européenne d'Intelligence Stratégique (CEIS)

Société Anonyme au capital de 150 510 € - SIRET : 414 881 821 00022 - APE : 741 G

280 boulevard Saint Germain – 75007 Paris
Tél. : 01 45 55 00 20 – Fax : 01 45 55 00 60