Data Leak Monitoring (DLM)

Les règles du Data Leak Monitoring (DLM)

PERSPECTIVE

Comment maîtriser la fuite de données, cette nouvelle plaie de la société de l'information ?
Ce livre blanc apporte une réponse à cette question cruciale qui hante les nuits des dirigeants, des DSI et des RSSI.

Architect of an Open World™

Table des matières

Introduction

La maîtrise de l'information se retrouve dans notre société de la connaissance au cœur de tous les enjeux. Une entreprise se doit légalement, vis-à-vis de ses clients et salariés, mais aussi pour assurer sa survie, de protéger son savoir-faire et les données à caractère personnel qui transitent sur son réseau.

Pourtant, la fuite d'informations sensibles, qu'elle soit accidentelle ou intentionnelle, est un phénomène bien réel. Selon une étude du Ponemon Institute, éditée en 2011, 70% des entreprises françaises auraient subi une perte de données sensibles en 2010. Les récentes affaires qui ont défrayé la chronique comme RSA, Sony… en sont des exemples médiatisés, mais de nombreuses entreprises en subissent régulièrement « en silence » les méfaits.

Très prochainement, ces « pertes d'informations silencieuses » ne pourront plus l'être. En effet, l'ordonnance du 24 août 2011 applicable à ce jour en France, venue transposer le Paquet Télécom, est, selon Maître Olivier Iteanu, suffisamment floue pour ne pas concerner uniquement les opérateurs. Cette ordonnance serait, pour lui, « une révolution culturelle qui va constituer une onde de choc dans la société française où l'omerta est de règle en cas de vulnérabilité du système ». Selon lui, outre les hébergeurs, de nombreux autres acteurs de la société de l'information devraient être concernés par l'obligation de notification, car « détenteurs de données à caractère personnel hébergées sur les réseaux numériques publics ». Cette ordonnance vient compléter l'article 34 de la Loi Informatique et Libertés, stipulant d'ores et déjà l'obligation de sécurité du responsable du traitement, qui doit prendre « toutes précautions utiles » contre les atteintes aux données, sous peine de sanctions pénales.

Enfin, la révision prochaine de la Directive européenne 95/46/CE de 1995, concernant la protection des données à caractère personnel, devrait lever toute ambiguïté, en dessinant dès 2012 les grandes lignes d'une future obligation de notification des failles de sécurité à tous ces états membres.

Malgré ces enjeux, bon nombre d'entreprises n'ont pas, à ce jour, mis en œuvre une réelle politique globale de protection de l'information. Elles sont d'ailleurs souvent incapables de cartographier les données de l'entreprise, de les classifier et d'y associer les mesures de sécurité adéquates en fonction de leur sensibilité. En la matière, les technologies de DLP offrent des perspectives séduisantes. Aujourd'hui, les offres se multiplient sur ce marché, mais peu de projets aboutissent véritablement.

Souvent effrayées par l'ampleur de la tâche, et ne sachant trop par où commencer, beaucoup d'entreprises se perdent en chemin. Pourtant, la démarche, si elle est faite dans les règles de l'art, étape par étape, n'est pas mission impossible et chaque entreprise récoltera au final les fruits de sa patience. On oublie trop souvent que la sécurité est un levier à la compétitivité des entreprises, pas uniquement un coût.

De plus, il ne faut pas perdre de vue que la technologie est certes une réponse, mais l'adhésion des utilisateurs est tout aussi importante. C'est pourquoi la technologie se doit d'être non intrusive dans le travail des collaborateurs. Elle doit s'inscrire comme un outil de sensibilisation et de prise de conscience de la valeur de l'information et non comme un vecteur supplémentaire de contrôle des salariés. L'objectif de ce livre blanc est d'accompagner les entreprises pas à pas dans cette démarche, en définissant les principales étapes, points de vigilance… à prendre en compte avant, pendant et après la mise en œuvre d'un projet DLM.

DLM : définition et objectifs

Le DLM (Data Leak Monitoring) est conçu comme un outil de surveillance, permettant de signaler les fuites de données, sans pour autant bloquer la sortie du document. Les entreprises savent aujourd'hui qu'elles ont des fuites de données, mais elles sont généralement incapables de les quantifier et d'en identifier clairement les causes. Le DLM se distingue ainsi des outils classiques de DLP, qui bloquent les documents avant leur sortie, réduisant ainsi l'efficacité de l'entreprise avec un nombre importants de « faux » positifs. Il se veut ainsi un outil de sensibilisation, permettant d'informer les employés du caractère sensible des documents qu'ils manient, et surtout de mettre en œuvre la politique de sécurité définie par l'entreprise.

Pour ce faire, l'outil de DLM va s'appuyer sur une analyse du réseau. La plupart du temps, il est placé en sortie du réseau local, donc en entrée d'Internet, afin de détecter les documents qui sortent vers l'extérieur. Au préalable, une phase d'identification des documents sensibles est nécessaire. L'équipe en charge du projet détermine un certain nombre de mots clés, d'expressions, d'interlocuteurs, ou encore de situations, en fonction desquelles des règles de détection vont être établies. Ces règles vont être appliquées par l'outil DLM qui va scruter le réseau et identifier les documents conformes à ces règles.

Les documents sont identifiés par rapport aux différents protocoles présents au catalogue. Il est ainsi important d'avoir des protocoles très larges (chat, messageries personnelle, professionnelle…) afin d'élargir au maximum la surveillance.
La technologie de DLM fonctionne sur la profondeur de la recherche ; elle va apposer une signature ou une empreinte sur le document, tout ou partie, qui sera ensuite détectée par l'appliance.

La mise en œuvre et les règles du DLM

Définition des besoins et objectifs de l'entreprise en termes de données sensibles

Avant de se lancer dans un projet, l'entreprise doit au préalable définir ses besoins et objectifs en matière de prévention de la fuite d'information. Veut-elle s'inscrire dans un processus de surveillance et de blocage ou juste de prévention et de signalement de la fuite de données?

Cartographie des données et identification des documents sensibles

Il s'agit ici d'identifier, dans un premier temps, toutes les données de l'entreprise, qu'elles soient stockées ou en cours d'utilisation, et de définir les risques et impacts en cas de perte ou de fuite de telle ou telle information. Cette étape va permettre de déterminer les documents les plus sensibles, à protéger en priorité.

Commencer par un périmètre restreint et l'étendre au fur et à mesure

Toutefois, pour être facilement opérationnelle, la phase évoquée précédemment doit être bien délimitée. En effet, afin de réduire la taille des projets et d'obtenir un résultat plus rapide, il faut commencer par un périmètre restreint, celui des données les plus critiques, puis l'étendre petit à petit au reste de l'entreprise. On pourra ainsi aisément démontrer la pertinence du projet à la Direction Générale.
Nous conseillons de démarrer par un projet pilote auprès d'un département ou d'un service, puis d'identifier ses enjeux en termes de documents sensibles. Le plus simple est de déterminer les documents confidentiels. Des mots clés seront ainsi identifiés et les règles de sensibilité des documents pourront être affinées au fur et à mesure, afin de réduire au strict minimum le nombre de documents sensibles.

Commencer par un projet pilote sur un seul service permet, en outre, de réduire les craintes des autres services grâce au bouche à oreille entre les différentes entités. L'extension progressive de l'outil dans l'entreprise s'en trouve ainsi largement facilitée et acceptée.

Tous les acteurs ont un rôle à jouer

Les échanges entre les différents acteurs (MOA, métiers, DSI, RSSI) sont primordiaux lors de l'identification des données sensibles. Ce sont les métiers qui détermineront les documents sensibles et définiront les règles à appliquer. Le RSSI émet, quant à lui, des avis et la DSI créera les règles informatiques et mettra en œuvre les outils. Ce sont les métiers qui utiliseront l'outil. Il doit donc être facile à utiliser pour les non-informaticiens. Les collaborateurs doivent être des partenaires du projet et non des adversaires.

Respect des obligations CNIL

Le projet doit s'inscrire dans le respect des obligations de la CNIL, concernant la surveillance de données électroniques. Le dispositif devra faire l'objet d'une information des salariés, d'un avis du comité d'établissement, et d'une déclaration à la CNIL. Il devra figurer dans la charte informatique ou règlement intérieur, et devra, bien évidemment, être ajusté au but poursuivi. Afin de s'assurer que le projet n'enfreint aucune loi ni exigence, le service juridique doit être intégré dans la boucle.

Choix technologique et mise en œuvre de l'outil de DLM

Une fois l'identification des données sensibles et l'attribution de mots clés effectués, l'outil de DLM se chargera de classifier automatiquement les données, puis d'assurer une traçabilité des actions et documents envoyés. Ensuite, les métiers affineront au fur et à mesure les règles de sécurité. Il s'agit ainsi de s'inscrire dans un cercle vertueux : affiner, détecter, prévenir avec pour finalité un renforcement permanent de la politique de sécurité.

L'humain au cœur de la politique de sécurité

Les utilisateurs se trouvent au cœur de la politique de protection de l'information, car eux seuls sont capables de déterminer les documents sensibles à surveiller. C'est aussi l'humain qui commet souvent l'erreur, d'ailleurs l'alerte va être sur lui. Il est fondamental de rassurer les salariés quant à la technologie et à son aspect non-intrusif. Contrairement aux outils de DLP associés à la notion de surveillance et de contrôle, l'outil de DLM est perçu comme un outil d'aide pour les collaborateurs afin d'éviter les erreurs involontaires.

Education et sensibilisation des utilisateurs

En parallèle de ce type de projet, une phase d'éducation et de prévention des salariés doit donc être mise en place. Il est essentiel de placer l'utilisateur au cœur de la politique de sécurité et de protection du patrimoine numérique, afin qu'il ait conscience de l'information qu'il manipule et qu'il s'en sente responsable. Il devrait d'ailleurs, à terme, y avoir de moins en moins de fuites de données grâce à la prise de conscience des salariés.

Processus de maintien et d'amélioration continue

Il faut agir de façon progressive, affiner sans cesse les règles et éduquer les utilisateurs. Le DLM doit être utilisé comme un outil de formation et de prévention et non comme un outil de répression. L'objectif est de trouver le juste équilibre entre protection de la fuite d'information et productivité de l'entreprise dans le respect des libertés des salariés. Enfin, il ne faut pas oublier que le DLM doit s'inscrire dans un processus global de protection de l'information.

Un utilisateur témoigne !

Comment réduire la fuite de données en quelques mois ?

Suite à une analyse de risques, une grande entreprise a décidé d'améliorer la confidentialité de ses informations sensibles et de déployer une solution de détection de fuite de données. Avant de mettre en œuvre cette solution à grande échelle, elle a d'abord souhaité la tester sur un périmètre restreint. Le centre de R&D a ainsi été choisi pour réaliser un projet pilote, comme en témoigne ce RSSI.

Quelles sont les raisons qui vous ont poussé à mettre en œuvre votre solution ?

Dans le cadre de notre processus global de gestion des risques, nous avons conduit une analyse de risque, dont les résultats nous ont démontrés que nous devions améliorer la confidentialité de nos informations les plus sensibles. Dans cet objectif de gestion des risques, un certain nombre de projets ont été identifiés ; la DLP en faisait partie et a fait l'objet d'une étude de faisabilité prioritaire.

Quels étaient vos objectifs ?

Nous avons d'abord souhaité valider l'adéquation de la solution et la méthodologie projet sur un site, afin de préparer la généralisation et le déploiement à l'échelle de l'entreprise. L'identification des données à protéger et leur implémentation dans la solution nous semblait une tâche assez ardue et nécessitait un test grandeur nature sur un périmètre ciblé.
Le 1er site que nous avons retenu a été sélectionné parce qu'il héberge exclusivement un métier sensible (R&D) et parce que son organisation métier et IT nous a semblé pouvoir accueillir un tel projet.

Avez-vous eu un sponsor en interne qui a soutenu votre projet ?

Le projet a été initié au niveau des risques, mais a pu bénéficier d'une très forte impulsion donnée par le directeur du site qui accueillait le projet pilote. Son site a pu servir de démonstrateur pour la solution, mais a aussi été montré en exemple pour les autres entités du Groupe.

Avez-vous eu recours à un intégrateur pour vous aider dans votre démarche ?

Plus qu'un intégrateur, il nous a fallu un expert DLP capable de comprendre les enjeux métiers – et donc identifier les informations les plus sensibles –, de mettre en œuvre la solution et d'accompagner la montée en charge et la mise au point dans la durée.

Comment avez-vous débuté votre projet de DLP ?

Nous avons choisi une solution qui offre la possibilité dans un premier temps de passer par une phase durant laquelle les utilisateurs sont informés et sensibilisés. Le projet a été lancé par des workshops avec les responsables de processus métiers ; les échanges avec notre expert ont permis d'identifier les enjeux clés de leur business, leurs modes de fonctionnement et les informations les plus sensibles. En parallèle, la charte d'usage du SI a été mise à jour afin de tenir compte de la législation. Dans notre cas, la collaboration avec le service juridique local a été très importante car chaque pays dispose de sa propre législation Informatique & Libertés et la charte doit être très précise.

Dans ce type de projet, la phase de classification des données est considérée comme la plus difficile. Avez-vous rencontré des difficultés ? Si oui, comment les avez-vous surmontées ?

Comme souvent, nos interlocuteurs métiers considèrent leurs propres besoins et informations comme les plus sensibles de l'entreprise. Or un travail de sélection doit être réalisé en gardant en tête que ces informations et leurs usages devront être concrètement implémentés dans la solution. Par conséquent, une position avec beaucoup de recul et un devoir de conseil est nécessaire à ce stade afin de les accompagner dans cette sélection.

Avez-vous eu des difficultés pour identifier les documents sensibles ?

Une démarche homogène vis-à-vis de chaque métier permet d'identifier les documents sensibles avec le même niveau d'analyse. Par ailleurs, la fonction « discover » de certaines solutions de DLP permettent de rechercher les documents sensibles sur le SI ; mais dans tous les cas, il faut pouvoir les désigner en amont et ne pas attendre de l'outil qu'il le fasse seul.

L'adhésion des métiers et des utilisateurs est incontournable dans de tels projets. Comment êtes-vous parvenu à l'obtenir ?

Dans ce type de problématique, la solution technique remplit un certain nombre d'objectifs, mais l'utilisateur et le management restent les maillons essentiels contribuant à la sécurité.
Par conséquent, comme dans tous les projets visant à améliorer la sécurité de l'information, il est indispensable de les associer à la démarche et d'expliquer les objectifs et les enjeux du projet : lors du kick off, tous les responsables métiers étaient présents ; lors des workshops, nous avons accompagné leur réflexion et expliquer les impacts des choix de données sensibles ; à la mise en œuvre, l'implémentation progressive des fonctions permet de bien appréhender le nouveau dispositif et de mettre en place une démarche de résolution des incidents efficace.
Par ailleurs, l'implication des managers est très importante : ils seront engagés dans la remédiation (lors d'incidents relatifs à la fuite d'informations) et sont donc des relais opérationnels et terrains très importants ; une action de formation / sensibilisation peut être spécifiquement conçue pour eux.

Avez-vous rencontré des difficultés lors du déploiement de la solution choisie ? Comment les avez-vous surmontées ?

Techniquement, la solution ne présentait pas de graves lacunes. Toutefois, certaines spécificités de notre environnement technique ont nécessité un support important de la part de l'éditeur et des équipes intégration. La relation entre notre entreprise et lui est donc primordiale pour ne pas perdre de temps, avoir accès au support du meilleur niveau possible, et même proposer des évolutions sur la roadmap du produit.
Si la solution est utilisée en « stand alone », la mise en œuvre de la solution nécessite des études d'architecture dans le domaine des réseaux (dimensionnement et surveillance des flux). Par ailleurs, dans le cadre d'une intégration dans une architecture de sécurité globale, la mise en œuvre de ces solutions nécessite aussi des études d'architecture relativement poussées dans les domaines systèmes (postes et serveurs), services d'infrastructure (annuaire, messagerie…), gestion des habilitations, hébergement centralisé (datacenters redondants…).

Quelles sont les parties de votre projet qui ont été les plus faciles à réaliser ?

Toutes les phases d'un projet de cette nature nécessitent beaucoup d'attention, de pilotage et d'anticipation ; mais dans notre cas, le fait que le 1er site déployé ait été très bien organisé sur le plan métier et IT nous a grandement facilité la tâche, notamment pour l'intégration de la gestion des incidents dans les processus ITIL du site. Les processus DLP ont donc été adaptés à nos standards et à notre organisation.

Combien de temps a pris le déploiement de votre solution ?

La phase de déploiement aura pris 7 à 8 mois. Il a fallu environ 1 à 2 mois pour déterminer les spécifications de la solution, puis environ 2 mois pour la déployer sur les serveurs. La phase de tuning a été la plus longue puisqu'elle a duré 4 mois.

Après le déploiement, le suivi et le maintien en conditions opérationnelles sont souvent problématiques. Comment en assurez-vous la continuité ?

Cette phase est effectivement clé : pour sécuriser la mise en œuvre et l'adoption de la solution, la phase consiste à déployer progressivement les fonctions restrictives et de surveillance de la DLP. Elle permet également de valider son paramétrage fonctionnel en analysant les remontées d'incidents et en vérifiant que les « faux-positifs » ne sont pas trop nombreux et se réduisent dans la durée. Au fil du temps, c'est la réduction des risques que nous suivons grâce à l'administration de la DLP. Nous avons vu effectivement une réduction considérable des fuites de données, tant involontaires que volontaires.

Où en êtes-vous aujourd'hui dans l'avancée de votre projet ? Quel bilan faites-vous ?

Cette phase est effectivement clé : pour sécuriser La réussite de la phase pilote doit encore être validée lors d'un Comité de Pilotage, mais nous sommes d'ores et déjà en train de préparer la généralisation à l'ensemble de l'entreprise.

Avec le recul et l'expérience, quels sont, selon vous, les pièges à éviter ?

Au-delà des risques classiques associés à un projet d'intégration (pré-requis système, livraison des serveurs, des licences, ouverture des accès et des droits…), il est très important d'entamer une démarche progressive en démarrant avec un nombre limité de règles afin de faciliter l'adoption et valider l'efficacité d'une telle solution.

Quels conseils pouvez-vous donner aux entreprises en la matière ?

Bien valider et cadrer les attentes des parties prenantes, avoir la capacité de comprendre chaque métier de l'entreprise, savoir donner du sens aux informations qui remontent de la solution en matière de réduction des risques et sensibiliser l'ensemble des collaborateurs de l'entreprise.

visibull est une solution de Data Leak Monitoring (DLM). Cette appliance virtualisée, qui vient se brancher sur le réseau, procède en trois temps :

- La découverte et le référencement des documents sensibles à partir de critères propres à l'organisation (mots clés, destinataires…) ;
- Le contrôle des flux sortant du périmètre de surveillance, quel qu'en soit le protocole (mail, messagerie instantanée, réseaux sociaux…) ;
- L'alerte lorsqu'une communication litigieuse est repérée.

visibull n'empêche pas la sortie du document, mais, à la manière d'une caméra de surveillance, participe à l'éducation, à la prévention et à la traçabilité des éventuelles fuites.

Le déploiement de visibull nécessite de définir finement, en amont, les règles de référencement des fichiers sensibles (en fonction du contenu, de la date, des personnes…), d'établir l'organisation et les processus appropriés (destinataires des alertes, procédures de suivi et d'intervention…), et d'assurer auprès des collaborateurs une conduite pédagogique du changement, le tout dans le respect des règlementations nationales et internationales. Tout au long de cette démarche qui associe métiers et sécurité, Bull accompagne ses clients par du conseil et des services spécialisés pour un usage optimal de visibull.

Bull – Rue Jean Jaurès – 78340 Les Clayes-sous-Bois – France

Ce livre blanc est imprimé sur papier composé de 40 % de fibres éco-certifiées issues d'une gestion forestière durable et de 60 % de fibres recyclées, en application des règles environnementales (ISO 14001). IMPRIM'VERT®

W-DLMfr1