

Evènement DLP "Prévention et Gestion de la fuite d'information" ou Data Leak Prevention

---000---

Dans le cadre des "Lundi de l'IE" du cercle d'Intelligence Economique du MEDEF Ile-de-France, le lundi 14 novembre 18h00-20h00 à Paris, Christophe d'Arcy, co-fondateur de la société MIRCA a traité ce sujet qui fait suite au lundi de l'IE du mois d'octobre, sur les plans de continuité d'activité (PCA), traités par Bruno Hamon, également co-fondateur de cette société d'audit, conseil et formation en sécurité du patrimoine informationnel..

Le prochain Lundi de l'IE est prévu le 16 janvier sur le thème complémentaire des Advanced Persistent Threats (APT) par Nicolas Ruff, du centre de recherche EADS.

Christophe d'Arcy commence par présenter Dropbox. Ce service permet de stocker et de synchroniser des fichiers en ligne ou de les partager avec d'autres ordinateurs, en déposant dans un dossier "*Dropbox*" des fichiers qui seront automatiquement synchronisés sur des serveurs sécurisés et sur les ordinateurs qui ont le client DropBox installé. Quelques failles dans le logiciel ont pu permettre aux employés de Dropbox d'avoir directement accès aux données de leurs 25 millions de clients dans le monde. Nous voici ainsi plongés dans la réalité de la fuite d'informations sensibles, vers l'extérieur de l'entreprise. Autre exemple, SONY a du faire face à un piratage de données nominatives sur son PS3 Playstation Network et a été contraint d'expliquer quels étaient les ravages subis par ses clients.

A la question posée par Christophe aux environ 70 participants de l'évènement, "qui parmi vous a eu connaissance d'une fuite d'information dans son organisation ?", personne n'a levé la main. Comme les enquêtes indiquent que 67% des entreprises ont déclaré avoir subi des détournements de données, Christophe en déduit que les participants à cet évènement ont une chance incroyable de faire partie du tiers des entreprises qui n'ont pas été encore confrontées à ce problème 😊

Par contre il est avéré, entre autres nombreux exemples, que l'UMP, Turbomeca, Renault, l'Education Nationale (avec les sujets du Bac), le ministère des Finances et de l'Industrie pour n'en citer que quelques uns, ont reconnu avoir été victimes de fuites d'information.

A la question "chez qui a été mise en place une solution DLP ?", personne n'a levé la main. Le coût d'un enregistrement détourné, avec ses conséquences parfois difficilement cernables en perte de confiance, altération de l'image de marques, compromissions, campagnes de communication rendues nécessaires, est estimé à 150 euros. Les 150 millions d'enregistrements égarés par Sony par exemple, pourraient coûter 15 milliards d'euro à cette entreprise.

Christophe donne quelques chiffres significatifs :

- Un message sur 400 comporte des données confidentielles ;
- Un fichier sur 50 est partagé à tort ;
- Un portable sur 10 est volé ;
- Une clé USB sur deux contient des informations confidentielles, clés USB qui sont souvent prêtées ;

- Et enfin, aux USA, une identité numérique est volée toutes les quatre secondes.

Ajouté à cela, 59% des employés qui quittent une entreprise emmènent avec eux des données sensibles. D'autant plus que s'ils en sont les auteurs, ils considèrent qu'elles leur appartiennent. Les entreprises, bien souvent, ne font pas grand-chose pour les en empêcher.

Mais il n'est pas exact de penser que la malveillance soit la seule cause de fuite de données sensibles. Elle n'intervient en fait que dans un tiers des cas. La négligence et les problèmes techniques se partagent à part égale les deux autres tiers.

Quand un détournement de données est révélé, s'agit-il de fuite, de perte ou de vol ? La fuite peut être empêchée par un contrôle strict de l'information de l'organisation, la perte peut être compensée par des sauvegardes, quant au vol, il pose un problème juridique intéressant puisqu'il n'y a pas en général soustraction frauduleuse de la chose d'autrui, caractéristique d'un vol, puisque l'information volée se trouve toujours chez autrui, bien qu'elle soit maintenant également à l'extérieur. Il est certain que l'engouement pour les réseaux sociaux, et le Web 2.0, ne peuvent que faciliter la fuite d'information. Une sensibilisation des utilisateurs est indispensable pour leur faire prendre conscience qu'il ne faut pas tout révéler, par exemple sous Facebook, Twitter...

On peut s'appuyer sur des technologies qui protègent l'information, comme l'IAM (Identity and Access management), la DRM (Gestion des droits numériques) et le chiffrement.

Arrivé à ce stade, on peut commencer à définir ce qu'est la DLP.

La définition qu'en donne Christophe d'Arcy est "La DLP est un ensemble de mesures organisationnelles et techniques visant à identifier, surveiller et protéger l'information, qu'elle soit stockée, en mouvement ou en cours d'utilisation. L'impression, la copie sur clés USB sont aussi à prendre en compte.

Pour prévenir ces fuites, il est indispensable d'abord d'identifier quelles sont les données à surveiller, non seulement celles qui sont stockées mais aussi celles qui sont en mouvement ou en cours d'utilisation.

Les facteurs de risques proviennent d'abord de la sensibilité des données. Un enregistrement (nom, prénom, adresse) est déjà une donnée sensible. Le sont bien entendu aussi les coordonnées bancaires, les listes de prix et de clients, les données stratégiques lors de fusions/acquisitions, les savoir-faire, les dossiers bancaires ou médicaux.

Les risques viennent ensuite de la vulnérabilité des systèmes, surtout ceux dont les gestionnaires et les utilisateurs n'ont pas conscience qu'ils ne sont pas suffisamment protégés, ou qu'il peuvent être les cibles des pirates. Les données d'une entreprise, qui prend beaucoup de précaution avec la sécurité de l'Information, mais qui sont confiées à un prestataire pour une campagne marketing peuvent faire l'objet de fuites si le prestataire ne prend pas les mêmes précautions que son client. Christophe cite l'exemple de Turbomeca, Groupe Safran.

N'oublions pas bien entendu, parmi les risques, le facteur humain qui est aujourd'hui la plus grande faille d'un système d'information mais qui peut être réduit par des campagnes de sensibilisation et de formation.

Quels sont les impacts d'une fuite d'information ?

En général ils sont loin d'être négligeables, que ce soit par les pertes financières, les pertes de confiance des clients, des partenaires, des salariés, sans oublier le déni d'image et dans certains cas, la sécurité des personnes. Quand les hacktivistes écolos ont révélés les coordonnées et les activités de certains employés de Shell, la vie de ceux-ci a pu être mise en danger.

Il faut prendre conscience de la nécessité de placer des protections autour de son information, et ne pas penser que ses données n'intéresseront pas les pirates. C'est le début d'une sagesse salutaire.

Quelles sont les principales difficultés liées à la DLP ?

D'abord, contrairement à ce qu'on peut croire, 80% des violations de l'information survenant sur une organisation viennent de l'intérieur, collaborateurs, prestataires, stagiaires... Les personnes ont toujours des raisons qui leur semblent bonnes de détourner l'information, surtout quand elles quittent l'entreprise, surtout que "les autres le font" alors pourquoi pas soi. Alors on s'envoie des fichiers depuis l'organisation vers sa messagerie personnelle gmail ou Yahoo ; on copie ses fichiers sur clé USB ou sur Laptop, et bien sûr en clair, pour l'utiliser depuis son domicile, ne serait-ce que parce qu'utiliser les VPN, prend trop de temps.

Alors lancer un projet DLP, c'est aussi avouer qu'il faut se protéger contre soi-même. Mais son ampleur supposée, limite l'envie de s'y lancer, surtout quand les données sont abondantes et réparties un peu partout. Mais, et ce fut l'objet d'un débat animé durant l'évènement, il faut savoir que seulement 5% des données sont réellement sensibles. Il faut d'abord cartographier les données, établir les risques et leur impact, identifier les vulnérabilités et la probabilité de fuites, et sensibiliser le personnel sur les dangers que présente pour l'organisation, la fuite des données vers l'extérieur. Ensuite, on établit des règles pour la protection de l'information, en procédant par étapes itératives. Et chaque fois qu'un nouveau contexte arrive sur le système d'information, il faut aussi raisonner DLP.

Un point fondamental de réussite d'un projet DLP est l'implication de la Direction Générale, sinon le projet est soumis à l'échec. La standardisation (Bruno Hamon préside un nouveau groupe qui se crée actuellement à l'AFNOR sur la DLP, qui éditera un guide des bonnes pratiques avant d'en faire une norme) et les aspects juridiques de la protection des données individuelles devraient favoriser une prise de conscience de la Direction. Citons la loi informatique et liberté de 1978 et l'implication de la CNIL, la loi d'Estraigne Escoffier qui fait obligation pour les opérateurs télécoms en France, de déclarer les fuites de données nominatives et qui est actuellement discutée au Sénat. D'autres lois ciblent la sécurité des données médicales (HIPAA...), des données financières (Bale, Sox...).

La démarche d'un projet de DLP est "top down", avec une phase de conception durant laquelle on cadre les objectifs et on définit les règles et la politique de la DLP, une phase de mise en œuvre avec implémentation, la DLP devenant alors opérationnelle, et le suivi du projet. Christophe identifie 10 phases allant de la phase 1 : cadrage du projet à la phase 10 : amélioration continue.

Christophe termine par le volet Cloud Computing, ou informatique en nuage dont la sécurité est le principal souci. Dans un Lundi de l'IE, Jean-Marc Grémy, de Cabestan, avait traité le sujet. Et, précise Christophe, la sécurité du Cloud est avant tout un problème de DLP. Sans cela, le Cloud peut constituer un SPOH (Single Point Of Hacking). Il faut se protéger suffisamment en précisant tous les détails du contrat qui lit le client avec son prestataire de Cloud. Il faut penser aux clauses de réversibilité, d'effacement propre des données quand on quitte son prestataire. Et si on empile les opérateurs de Clouds, parfois à son insu quand ceux-ci sous-traitent une partie des services à d'autres opérateurs, il faut avoir conscience que cela rend quasi impossible la localisation des données. Le juridique n'a pas fini d'avoir du travail avec les événements fâcheux qui vont se produire dans un avenir qui peut être proche.

Bien entendu des freins à l'établissement de règles de DLP peuvent venir des utilisateurs qui se sentiront espionnés ou qui ressentiront les contrôles comme un manque de confiance de la direction, envers eux. C'est pour cela qu'une sensibilisation devra accompagner impérativement tout projet DLP. Un projet DLP doit être avant tout un projet de la Direction générale, plus qu'un projet purement technique.

La séance questions / réponses qui a suivi a été très animée, je n'ai pas pris de notes puisque j'étais occupé à passer le micro aux participants, ceci étant, et c'est valable pour tous nos événements, pour n'en rien manquer, il faut venir, et la participation aux "Lundi de l'IE" est gratuite, avec demande d'inscription obligatoire.

Nous nous sommes donné rendez-vous pour le prochain Lundi de l'IE consacré à la sécurité, sur les APT le lundi 16 janvier 2012, ou même avant au colloque "stratégies d'influence pour réussir à l'international" le 14 décembre de 17h30 à 20h, toujours au même endroit, 10 rue de Débarcadère, 75017 Paris.

*Gérard Peliks
Coordinateur de l'activité sécurité de l'Information
des "Lundi de l'IE" du MEDEF Ile de France
gerard.peliks@cassidian.com*