

Vol de données sensibles: peut-on s'en prémunir?

Pour l'entreprise, la perte ou le vol d'informations confidentielles, qu'elles soient de nature commerciale, financière, médicale ou issues d'un département R&D, représentent un préjudice parfois critique. Peut-on assurer la confidentialité de ces données sensibles? Jacques Medina

Il faut commencer par faire une distinction claire entre la perte et le vol. La perte est le résultat d'une erreur humaine, souvent involontaire, contre laquelle la mise en place de mesures techniques de protection, par exemple le cryptage des données, va s'avérer efficace.

Le cas du vol de données est tout à fait différent. L'entreprise se voit confrontée à une entité interne ou externe, éventuellement composée de plusieurs maillons, dont le but est de s'approprier par tous les moyens des données ciblées. «Par tous les moyens»: c'est ce qui complique la lutte contre le vol de données. Cela signifie que les simples mesures techniques applicables contre la perte ne seront plus suffisantes.

L'ensemble des affaires récentes de vol de données a un dénominateur commun: à un moment donné, certaines personnes ont eu accès à des données sensibles dans le cadre direct ou indirect de leur travail. Elles ont ensuite accaparé ces données pour des raisons diverses, allant du mécontentement contre les conditions de travail au pseudo combat éthique contre l'ordre établi, en passant par l'appât du gain et le refus de toute forme de contrainte.

Comment se protéger?

Les protections d'ordre technique sont toujours possibles. Par exemple, ne plus permettre un accès direct aux données par un individu, mais exiger l'approbation préalable d'autres personnes afin de mieux contrôler ces accès - ce contrôle peut être complété par l'enregistrement de l'utilisation faite de ces données. Crypter les données en n'autorisant leur décryptage que par les personnes autorisées. Répartir les données sur différents supports pour compliquer la tâche au voleur potentiel.

Mais que faire face aux multiples moyens que peut employer une personne malintentionnée pour extraire les données de l'entreprise, comme leur téléchargement vers un site externe, la copie sur une unité de stockage amovible, les impressions, la copie d'écran (via son GSM par exemple) ou même des techniques plus rudimentaires comme la mémoire



Face aux multiples moyens que peut employer une personne malintentionnée pour extraire les données de l'entreprise, la vigilance s'impose.

Source: © Hans-Joachim Roy

sation ou la transcription manuscrite de ces informations?

Dans ces cas, la surveillance de la personne devient nécessaire afin de détecter les changements de comportement suspects. Et nous entrons là dans un domaine très sensible qui porte sur des aspects humains, légaux mais aussi techniques auxquels l'entreprise n'est pas forcément préparée. Aujourd'hui, certains mandats de sécurité consistent à étudier le comportement d'une personne au travers des différentes informations qu'elle publie dans des forums, pour déterminer la probabilité qu'elle représente un risque. Nous sommes loin des technologies anti spam ou pare-feu!

Rester pragmatique

Pour déterminer si une entreprise doit se préparer à faire face à ce type de menace, il faut répondre à deux questions: «le jeu en vaut-il la chandelle?» et «à qui profite le crime?». Ainsi, le vol d'un fichier client d'une PME locale semble peu attractif car il sera difficilement exploitable et présente des risques légaux certains. Par contre, l'obtention de données R&D pharmaceutiques est beaucoup plus intéressante. Certains résultats de recherche sont codifiés et enregistrés avant d'avoir fait l'objet d'un dépôt de brevet. Leur vol à ce stade peut représenter un gain de plusieurs millions de francs. L'actualité récente montre que même des États sont prêts à se compromettre dans le vol de données. Ils disposent en outre de res-

sources financières, techniques et logistiques quasiment illimitées.

Les entreprises sont-elles protégées face au vol de données? Malheureusement, peu d'entre elles ont pris la mesure du risque. Souvent, elles ont mis en place des solutions de traçabilité qui permettent (parfois) de reconstituer le scénario de l'incident, mais elles sont incapables de prévenir le vol.

Que faire alors? Les démarches à entreprendre sont multiples mais doivent avant tout rester pragmatiques. Il est illusoire d'espérer la solution miracle qui va répondre à 100% à la problématique du vol de données.

D'un point de vue technique, outre les solutions de sécurité traditionnelles, les technologies suivantes peuvent être évaluées:

- Prévention de la fuite d'informations (DLP) sur les stations de travail
- Contrôle des accès privilégiés des administrateurs
- Audit et monitoring des bases de données sur les serveurs
- Toute solution permettant de garantir la sécurité physique des données, qu'elles soient stockées (serveurs, stations de travail, supports mobiles), ou en transit.

En parallèle, certaines procédures s'imposent:

- Procéder à la classification des données, encore trop souvent lacunaire
- S'assurer de la déontologie des collaborateurs (sensibilisation, règlements, sanctions)
- Détecter et étudier les comportements anormaux ou les changements d'attitude au sein du personnel d'encadrement

Et s'inspirer de Sophocle qui disait dans *Philoctète*: «Plus faibles sont les risques, meilleure est l'entreprise.» <



Jacques Medina,
Security Architect,
Navixia SA