

Quid du chiffrement de données contre la menace interne?

Les faits divers et les statistiques des cabinets d'étude le confirment: les entreprises doivent protéger leurs données sensibles des indiscretions de leurs informaticiens. Peuvent-elles le faire avec les solutions de chiffrement de données proposées par le marché? Jean-Marc Bost

Les affaires LGT, HSBC et CS ont fait beaucoup de bruit dans un passé récent. A chaque fois, des informaticiens travaillant à l'intérieur de la banque ont été impliqués dans le vol et la revente de données à des gouvernements luttant contre l'évasion fiscale. Or, la menace interne ne concerne pas que les banques. Récemment, plusieurs entreprises ont déploré le même type d'expérience, au premier rang desquelles T-Mobile et Dupont de Nemour.

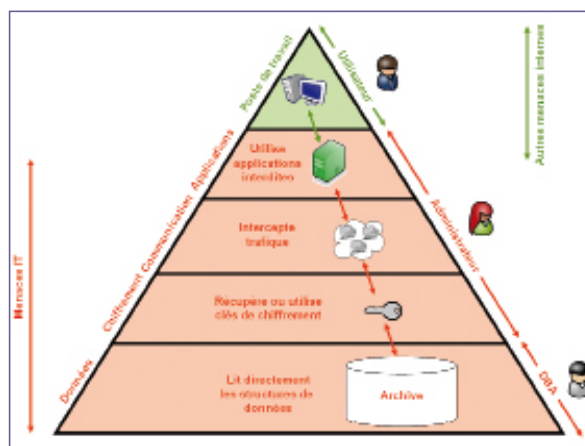
La menace interne concerne toutes les entreprises

Comme l'illustre le Data Loss Barometer du cabinet KPMG, la menace interne se précise: «La combinaison de la pression économique et de la tentation provoquée par les offres d'organisations criminelles ont conduit certains employés à envisager le vol comme une option possible», estime KPMG pour expliquer que 10% des vols de données en entreprise sont le fait de salariés. A force de dématérialiser, les entreprises sont de plus en plus dépendantes de leur informatique et de leurs informaticiens. Que ceux-ci soient malhonnêtes, ou maladroits, elles sont à leur merci.

Techniquement, il est aujourd'hui possible de protéger la confidentialité des données en les chiffrant. Cependant, les solutions du marché ont été conçues dans un autre but. Leur cible est plutôt la conformité aux nouvelles normes de protection contre les vols d'identités sur internet, type PCI/DSS. Sont-elles alors efficaces contre la menace interne?

Quid des solutions de chiffrement des bases de données?

Les systèmes de bases de données sont en première ligne de cette nouvelle offre avec, comme argument principal, la maîtrise du modèle de données et, par voie de conséquence, le faible impact des mécanismes de chiffrement sur le système d'information existant. On reproche parfois à ces systèmes la dépendance qu'ils engendrent vis-à-vis d'une technologie propriétaire et de leur



Pyramide des menaces internes

fournisseur mais qu'en est-il exactement de leur efficacité face à la menace interne?

En principe, un DBA (Data Base Administrator) peut toujours in fine déchiffrer toutes les données et un administrateur système peut installer les applications qu'il veut, à commencer par les outils d'interrogation de la base de données. La réponse des éditeurs est la restriction des privilèges, notamment en permettant aux DBA de contrôler les droits d'autres DBA. Toutefois, même si l'entreprise est décidée à instaurer la rigueur organisationnelle nécessaire à ce type de solution, au final, c'est l'IT qui contrôle l'IT. Dans ces conditions, peut-on dire que l'entreprise contrôle son personnel IT?

Le chiffrement par les applications est-il plus efficace?

L'alternative au chiffrement par la base de données est le chiffrement applicatif dans lequel ce sont les applications qui chiffrent les données avant de les stocker, et qui les déchiffrant après les avoir récupérées. Contrairement au cas précédent, les applications ne maîtrisent pas le modèle de données. En attendant la standardisation d'algorithmes capables de préserver le format des données, le chiffrement applicatif peut donc avoir un impact plus important sur le système d'information. En revanche, il est indépendant du stockage et facilite ainsi les opérations d'exportation et de migration ainsi que l'intro-

duction de nouvelles technologies de stockage.

Concernant la menace interne, le chiffrement applicatif est réputé mieux couvrir la «surface d'attaque» offerte à un voleur du fait que les données sont chiffrées dès qu'elles sortent de l'application. Dans la pratique, il faut néanmoins pondérer cet avantage. Les DBA doivent avoir accès à un minimum de données pour faire leur travail. Quant à l'administrateur système, il reste une menace car il a accès aux modules de chiffrement et il peut

installer ses propres applications de déchiffrement. Bien sûr, il existe des solutions complémentaires pour surveiller les applications mais elles sont exigeantes et restent sous le contrôle de l'administrateur. C'est encore l'IT qui contrôle l'IT.

La solution idéale?

On le voit bien, ces solutions sont imparfaites. On peut dire schématiquement que les solutions apportées par les bases de données ont un impact moindre sur le système d'information alors que les solutions applicatives réduisent plus sûrement les surfaces d'attaques. Aucune des deux solutions cependant ne peut prétendre, seule, couvrir l'intégralité de la menace interne. Il faudrait offrir aux départements sécurité une vue davantage métier qui leur permette de garder le contrôle sur l'IT. Tout l'enjeu est là: offrir une défense en profondeur, qui minimise les impacts sur le système d'information, et qui reste sous le contrôle exclusif de la sécurité, et non des informaticiens. <



Jean-Marc Bost
dirige la division
sécurité chez ELCA
Informatique SA
à Genève