Chiffrer les champs de données et traiter la ségrégation des rôles

Mike Howse, le directeur des ventes de Protegrity, pose les questions que devraient se poser toutes les entreprises sur la sécurité de leurs données : »

Où sont les données ? Combien sont-elles ? Combien ont besoin d'être sécurisées ? Qui doit disposer d'un accès ? Et quand doivent-elles être effacées ? » La simple énoncée de ce question éveille l'attention. En effet, quelles sont les entreprises qui ont véritablement pris conscience des données qui doivent être protégées, comme les brevets, les documents stratégiques, des informations des RH ? Et qui contrôle l'accès aux données et peut être soupçonné en cas de fuites ? Bruno Rasle, auteur de '*Halte au spam*' et consultant chez Corina, rappelle que « *les entreprises ont généralement concentré leurs efforts sur la protection périphérique des systèmes, mais elles ont besoin de compléter cette approche par la protection des données*. » Comment ? En cryptant les données. « *C'est logique, mais personne ne le fait, personne ne chiffre*« . Et la réponse va au-delà du simple chiffrement, car elle se pose aussi sur la **ségrégation des rôles** : « *Il n'est pas normal qu'un administrateur de base de données ait accès à toute l'information, ce qui d'ailleurs n'est pas toujours confortable pour l'administrateur*. » L'exemple d'Oracle 10g est symptomatique de cette question. L'administrateur est tout puissant. Il peut même effacer ses propres traces ! **La France, un problème à part** « *C'est le même problème dans tous les pays*« , nous confie Sonia Camara de la Fuente, responsable Business Development de Protegrity. 3*Mis nous rencontrons des différences culturelles. En Espagne et en Italie notre démarrage est fort. En France, il y a toujours des différences de comportement sur la sécurité*« . « *Par exemple, il n'y a pas en France de culture ni de sensibilisation sur la sécurité des bases de données, et tout le monde se renvoie la responsabilité ! Et c'est la même chose chez les éditeurs. Et il y a beaucoup d'idées reçues, comme que les bases de données sont protégées et qu'elles sont éloignées des périmètres à risques. Pourtant,* ***60 % du risque sur les bases de données est interne***. » Les lois sont à peu près les mêmes dans toutes l'Europe, mais c'est leur application et les conséquences qui diffèrent. Ainsi, en Espagne, en permettant à la CNIL locale d'émettre des amendes, des affaires de sécurité des bases de données ont fait surface, sensibilisant les entreprises et les administrations, et le financement de la structure a pu ainsi être financée et disposer de plus de moyens. Autre exemple en Californie : si un vol d'informations personnelles a eu lieu, les entreprises ont l'obligation légale d'informer personnellement toutes les victimes? sauf si la base dérobée est cryptée. D'où la médiatisation de ces incidents, qui a sensibilisé les propriétaires de bases de données a adopter de nouvelles stratégies de protection, et en particulier le chiffrement. L'opacité du système français est loin de permettre une telle sensibilisation ! **Chiffrer les données, mais intelligemment** Le chiffrage des données n'est pas chose nouvelle. En revanche, le principal problème associé à cette approche reste la performance. La réponse apporté par Protegrity est pourtant simple : « *il ne faut pas chiffrer toute l'information, mais uniquement celle qui doit être confidentielle*. » « *Pour arriver à une sécurisation pertinente des données, il faut passer par plusieurs étapes de maturité. D'abord chiffrer une première fois l'information vraiment confidentielle. Ensuite traiter la ségrégation des rôles et séparer si c'est nécessaire l'administration des systèmes de l'administration du chiffrement. Enfin prouver à un tiers, assurer la traçabilité du chiffrement*. » Le traitement de la ségrégation des rôles a trouvé un écho important dans le sud de l'Europe où 80 % des acquéreurs de la solution étaient particulièrement sensibilisés à cette problématique. Ainsi

qu'à celle de l'outsourcing des bases de plus en plus présent. « *Les DRH ou les directeurs financiers devraient à ce propos se poser la question du traitement de leurs informations chez leurs partenaires et en outsourcing !* » **Le futur de la cryptographie ?** « *Nous devront prendre en compte le potentiel du hardware et gérer les problèmes de transparence. Mais le principal challenge de l'industrie c'est que la sécurité devient embarquée. Mais faut-il tout protéger ? Cela dépend de l'infrastructure. Nous devrons en revanche protéger les informations sur le desktop*. » « *Nous travaillons à établir un tunnel crypté entre l'utilisateur et la base de donnée pour sécuriser le transfert. Ce sera probablement une question de prix et de stratégie, sur des médias comme la carte de crédit ou le dossier médical. Nous devrons préserver l'intégrité des données et protéger les données structurées et non structurées*. » « *Dans quelques temps, il ne sera pas naturel de trouver de l'information qui ne soit pas cryptée*« , conclue Bruno Rasle. **Une solution adaptée signé Protegrity**

Avec Defiance DPS (*Data Protection System*), Protegrity, importé en France par Cortina, apporte une solution originale, adaptée et reconnue, qui offre le chiffrement des champs sensibles et non plus de la base entière (une technologie qui apporte plus de performance) et dans le même temps traite la ségrégation des rôles. Ce dernier point est important dans une stratégie de protection des données. « *La personne qui définit les règles de sécurité est indépendante de celle qui gère la base*. » Solution logicielle – « *C'est plus simple et économique à gérer et à 'scaler' qu'une appliance par serveur ou base de données* » ? la solution dispose d'une console centrale à ne configurer qu'une fois, et pour toutes les bases de données. L'administrateur du chiffrement défini quels champs sont à crypter, et avec quelle clé pour chaque champ. « *Peu importe les bases de données et les configurations hardware où elles sont implantées. Notre solution est agnostique en termes de plate-forme. Nous protégeons l'info de sa création à sa destruction. Même lorsqu'il faut convertir l'info pour la stocker ou sur un serveur Web*« . La solution est composée d'un 'bundle' de départ, avec la console d'administration, un Data Protector pour le serveur et un Data Protector pour le serveur de développement, l'ensemble proposé à 18.000 euros. A compléter ensuite par un Data Protector sur chaque CPU ou famille de base de données. DPS s'installe sur le serveur sans modifier l'environnement applicatif. Ainsi ce n'est pas la communication qui est chiffrée, elle reste transparente. Au niveau du client, l'administration centrale peut définir des profiles d'utilisateurs, s'adapter à l'annuaire LDAP de l'entreprise, et même définir des profils additionnels pour les partenaires, pour l'outsourcing plus particulièrement, avec des accès limités à l'information et flexibles dans le temps. Avant la fin de l'année, Protegrity proposera aussi une protection au niveau du fichier, qui sera intégrée dans l'infrastructure.