

Accès aux données: les informaticiens sont-ils les derniers privilégiés?

Les données de production font en général l'objet de contrôles stricts et rigoureux. On en oublierait parfois que les informaticiens sont au cœur de l'information et qu'ils disposent d'accès privilégiés à un large panel de données. Olivier Montaguti, Laurent Perret

Les accès à la liste des clients ou aux salaires de l'entreprise sont évidemment strictement contrôlés. Les disques durs des ordinateurs sont cryptés et il est peu probable qu'un voleur puisse récupérer quelques données que ce soit. En revanche, certains informaticiens disposent d'accès privilégiés ou de droits souvent interdits aux autres utilisateurs leur procurant des fonctionnalités sans restriction parfois dangereuses selon l'utilisation qui en est faite. Ceci est souvent le résultat, entre autres, d'une séparation des rôles et des responsabilités inefficace et d'une gestion des droits d'accès lacunaire.

Qui sont ces informaticiens?

Les premières populations d'informaticiens auxquelles on pense sont les ingénieurs systèmes et réseaux. Par définition, ils ont accès aux données des différents environnements de l'entreprise et leurs droits d'administration leur permettraient d'effacer jusqu'aux traces de leurs activités.

En revanche, il est d'autres populations auxquelles on pense moins: les personnes intervenant tout au long du cycle de développement des logiciels. De la phase d'analyse à celle des tests, il leur est, en effet, indispensable de disposer de données fidèles à celles en production et respectant au mieux les règles de gestion et contraintes d'exploitation. La tentation est alors grande d'utiliser les données de production pour permettre les évaluations, le développement et le test. Ce qui n'est pas en soi une mauvaise pratique, peut avoir pour effet direct de réduire à néant les mesures, règles et contrôles de sécurité appliqués en production.

Les risques

Il va sans dire que la population des informaticiens doit être intégrée dans toute démarche de gestion du risque car elle est une source potentielle de faille du système de sécurité d'une entreprise. Les risques ne sont pas moindres que pour les utilisateurs ordinaires.

Par maladresse ou par malveillance, de nombreux dommages peuvent être occasionnés:

- des données peuvent être irrémédiablement altérées ou perdues,
- des données ou des traitements peuvent être durablement indisponibles, entraînant l'arrêt d'une production ou d'un service.,
- des informations confidentielles ou erronées pouvant profiter à des sociétés concurrentes ou nuire à l'image de l'entreprise peuvent être divulguées.

Quelques risques d'une longue liste pouvant avoir un impact direct sur l'image, l'activité, voire la rentabilité de l'entreprise. Nombre d'exemples avérés aujourd'hui mettent en exergue les réels facteurs de risque renforçant la nécessité de sécuriser l'information et ce à tous les niveaux de l'entreprise.

Quelles mesures adopter

Le risque zéro n'existe pas, mais les données issues des environnements de production doivent être considérées avec le même niveau d'exigence de sécurité, lorsqu'elles sont utilisées à d'autres fins, tels le développement ou le test.

D'une façon générale, il faudra donc veiller à ce que les restrictions imposées aux utilisateurs restent appliquées aux informaticiens. On limitera également au plus petit nombre les dérogations, que ce soit en termes d'éléments de sécurité physique (imprimantes, lecteur/graveur de CD/DVD, ports USB...) ou de limitation de communication (ressources Internet, e-mail, Bluetooth, messagerie instantanée...).

Dans le cadre des activités d'un département, les données sensibles peuvent se retrouver sur différents types de support, parfois de façon transitoire. Sans appliquer à l'identique les règles et contrôles de sécurité et d'accès, des mesures alternatives, voire compensatoires peuvent être considérées et adaptées au dommage potentiel. Toutefois, quelles que soient les mesures prises, il reste capital de ne pas perdre de vue l'objectif initial nécessitant la mise à

disposition des données à des fins de production ou de test.

Parmi les mesures envisageables, on peut citer:

- rendre anonyme les données,
- exclure de la copie les éléments les plus critiques,
- créer de toutes pièces un ensemble de données pour les informations les plus critiques,
- dissocier la gestion des droits d'accès et les processus d'authentification,
- maîtriser les droits d'accès et contrôler l'utilisation des accès étendus,
- activer les traces d'audit (log),
- faire signer une charte de confidentialité,
- séparer le réseau de communication interne du réseau ayant accès à l'extérieur,
- rendre impossible l'utilisation de moyens de stockage externes...

Autant de mesures dont la liste n'est pas exhaustive et qui doivent être accompagnées d'une sensibilisation et d'une information régulière auprès des employés et des personnes travaillant pour l'entreprise (sous-traitants, prestataires de service, stagiaires). Une compréhension de l'importance de ce sujet ainsi qu'une implication de tous les acteurs de la société contribue à renforcer grandement la sécurité de ses données. <



Olivier Montaguti,
Senior Consultant
chez Itecor.



Laurent Perret,
Senior Manager
chez Itecor.