



# Garder les données sécurisées, même pendant les travaux

**PREJUDICES** Lors de tests ou de développements, les fichiers clients ou personnels sont vulnérables. Leur sécurisation ne relève pas des seules équipes informatiques.

**C**omment une entreprise peut-elle sécuriser au maximum ses bases de données personnelles? L'assurance, qui possède de nombreux fichiers clients, est au cœur de cette problématique, à un moment où les cas de disparition de données bancaires, fiscales ou de santé font l'actualité. Une enquête menée par le cabinet britannique Freeform Dynamics, spécialisé dans l'impact du développement des technologies sur les affaires, souligne le manque de vigilance en matière de confidentialité des données.

Ainsi, plus de 70% des entreprises utilisent des informations issues des bases de production pendant le développement de logi-

ciels, sachant par exemple que les services financiers conservent plus de 80% des informations importantes sous forme électronique. Or, contrairement aux domaines opérationnels de l'activité, désormais dotés de moyens de contrôle, la protection des informations repose dans ce cas presque exclusivement sur les épaules de l'équipe informatique.

## Données personnelles et anonymat

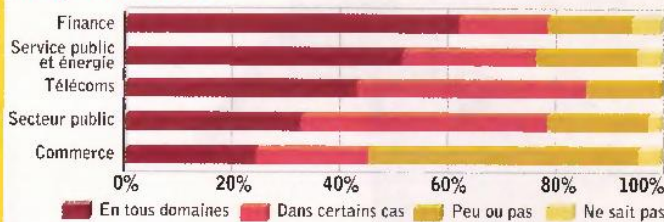
« La racine du problème est là, insiste Jon Collins, de Freeform Dynamics. Les personnes impliquées dans le développement et le test de logiciels ne sont pas toujours employées par l'entreprise.

L'activité est souvent répartie sur plusieurs sites et l'environnement informatique utilisé pour les tests n'est pas toujours distinct de celui des systèmes de production. » De plus, aussi curieux que cela paraisse, les responsables des risques et de la sécurité ne sont bien souvent pas informés de l'utilisation de données personnelles.

Dès lors, comment sécuriser ces différentes opérations? Tout d'abord, en investissant dans des outils qui masquent les identités et évitent la dépendance à l'égard de processus manuels d'anonymisation, susceptibles de générer des erreurs. Une personne peut toutefois être chargée de s'assurer que ce nettoyage ou maquillage des données est efficace.

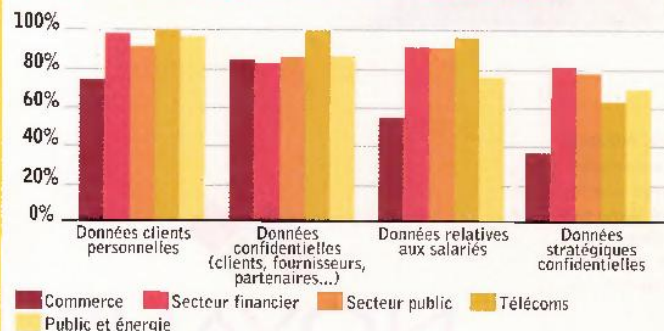
## LE SECTEUR FINANCIER PROTÈGE MAL SES DONNÉES CLIENTS

Jusqu'à quel point confiez-vous le développement et la phase de tests des logiciels à des tiers?



Durant la phase de test des applications sur site, les sous-traitants ont accès aux données réelles des entreprises. Celles de la finance sont très exposées.

Quels types d'informations gardez-vous sous format électronique?



Le stockage informatique des données clients est nécessaire pour les sociétés financières, qui doivent être réactives. Mais elles s'exposent ainsi à la malveillance des pirates ou de collaborateurs qui peuvent revendre les fichiers.

## Masques, boîtes noires et mots de passe

Ensuite, il est nécessaire de s'intéresser autant aux équipes internes qu'externes, en étant vigilant à toute forme de turn-over. À partir du moment où ces données font l'objet de revente, des « mafias » peuvent aussi facilement infiltrer les centres d'appels, d'autant plus que l'intérim constitue un vivier pour le recrutement des équipes.

Enfin, il faut tracer les connexions, et gérer scrupuleusement les autorisations d'accès, afin de prévenir ou de sanctionner des comportements délictueux. « Attention aux mots de passe qui se multiplient ou qui ne sont pas désactivés après le départ des administrateurs », met en garde Jean-Noël de Galzain, PDG de Wallix. Cette société a mis au point un système qui permet, sur le principe d'une boîte noire, d'enregistrer en continu toutes les connexions afin de détecter anomalies, fraudes et erreurs de pilotage des systèmes, ce que prévoit d'ailleurs la réglementation. ●

MADELEINE VATEL