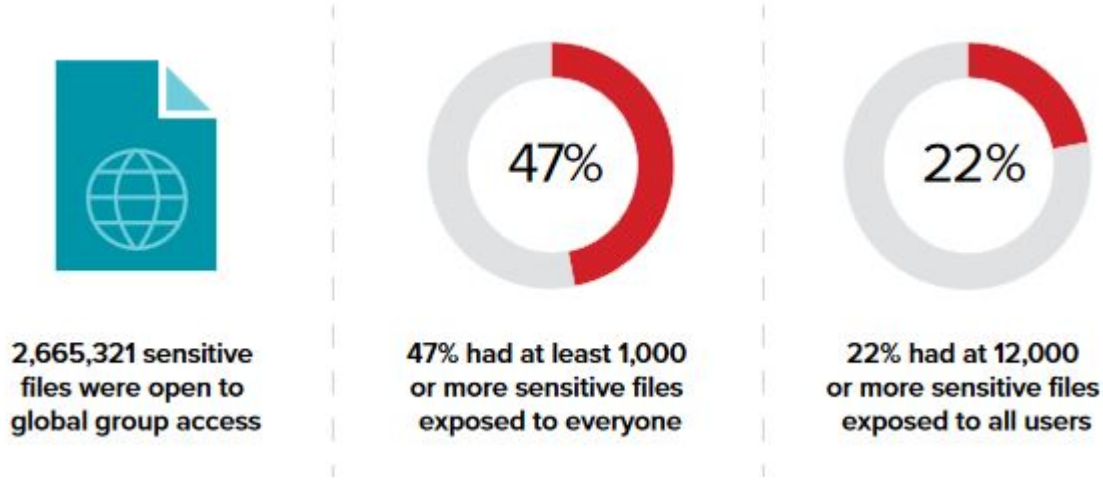
# Une entreprise sur deux laisse plus de 1000 fichiers sensibles en libre accès

47 % des organisations laissent au moins 1 000 fichiers sensibles accessibles à tous leurs employés. Et dans 22 % des entreprises, ce sont même plus de 12 000 fichiers renfermant des informations relatives à la régulation, à la propriété intellectuelle, ayant une valeur concurrencielle ou normalement réservées à certains employés qui sont en libre accès. Ce sont quelques unes des conclusions, pas si surprenantes en réalité, d'un audit mené par Varonis, un spécialiste de la protection de données, auprès de 80 organisations. Soit 3,79 Po de données, 2,8 milliards de fichiers et 236 millions de dossiers passés au crible. Sur ce total, 48 millions de dossiers étaient ouverts à tous au sein de l'organisation, explique Varonis. La démonstration concrète de la difficulté des administrateurs à gérer les droits d'accès aux dossiers et fichiers sensibles dans les systèmes Windows.




Une faiblesse qui, d'ailleurs, n'a pas échappé aux employés eux-mêmes. En août 2016, une étude du Ponemon Institute, commandée par le même Varonis, montrait que 62 % d'entre eux avaient conscience de pouvoir accéder à des données qu'ils n'étaient probablement pas censés voir. Ces lacunes sont d'ailleurs bien connues des professionnels de la sécurité. Une étude de Forrester Research montre que 60 % d'entre eux reconnaissent que leur organisation ne parvient pas à restreindre correctement les accès aux données en interne. Et deux tiers de ces spécialistes ajoutent que leur entreprise échoue à classer correctement l'information non structurée, là où réside une large part de la propriété intellectuelle et des plans stratégiques des organisations. Or, de récentes affaires ont montré que des employés sur le départ, mécontents ou simplement attirés par l'appât du gain, constituent une réelle menace pour la sécurité des entreprises.

## Bien gérer les dossiers pour le GDPR

Dans le détail, Varonis pointe également les erreurs dans la gestion des permissions d'accès aux dossiers partagés. 10 % d'entre eux sont ainsi associés à des permissions uniques, soit des autorisations ponctuelles fournies pour des cas particuliers. Or, pour Varonis, cette méthode se révèle trop complexe à analyser. « *Plus complexe est la structure du système de fichiers, plus il existe de*

*risques qu'un utilisateur se voit accorder un accès non prévu. Les permissions uniques accroissent la complexité quand une entreprise tente de se conformer à des régulations qui requièrent un suivi précis des accès aux données sensibles, comme c'est le cas du futur GDPR* », écrit Varonis. A ce problème touchant, un dossier sur 10, s'ajoutent quelques erreurs (dossiers protégés, bloquant l'héritage de droits, SID non résolue…), affectant quelques pourcents supplémentaires des dossiers audités. Notons que cette question de l'héritage des droits lors d'un changement de dossiers est tout sauf théorique ; elle était même au centre de l'affaire dite LuxLeaks, concernant des données dérobées à PwC Luxembourg.

Au-delà de la gestion des droits associés aux dossiers, se pose aussi la question de la maintenance des accès des utilisateurs. Varonis affirme avoir découvert, au cours de ses audits dans 80 organisations réparties dans le monde, près de 450 000 comptes d'utilisateurs périmés, mais conservant leurs droits d'accès associés. Une cible classique pour les hackers. A elle seule, une organisation du monde de l'éducation en comptait 231 000 ! Mais, même chez le meilleur élève du panel, 3 % des comptes étaient périmés. Varonis ajoute que plus de 500 000 comptes d'utilisateurs audités n'étaient pas associés à des règles d'expiration du mot de passe, ce qui facilite les attaques par force brute et le maintien de hackers dans des systèmes qu'ils seraient parvenus à compromettre.

**A lire aussi :**

Par crainte d'être licencié, un devops pirate son employeur

Quand un DSI laisse des backdoors pour pirater son ancien employeur

**Crédit photo : Maksim Kabakou / Shutterstock**