Protection des donnÃ©es dans les dÃ©lais impartis : Aie!
SÃ©curitÃ©
PostÃ© par : JulieM
PubliÃ©e le : 30/5/2017 13:00:00

Varonis Systems, Inc., lâ□□un des principaux Ã©diteurs de solutions logicielles de protection des donnÃ©es contre les menaces internes et les cyberattaques, publie les rÃ©sultats dâ□□une Ã©tude indÃ©pendantei visant Ã Ã©valuer les comportements vis-Ã -vis du rÃ¨glement gÃ©nÃ©ral europÃ©en sur la protection des donnÃ©es (GDPR) qui entrera en vigueur dans un an.

MenÃ©e auprÃ¨s de 500 dÃ©cideurs informatiques au Royaume-Uni, en Allemagne, en France et en AmÃ©rique du Nord, cette Ã©tude rÃ©vÃ¨le que 75 % des entreprises auront des difficultÃ©s Ã se prÃ©parer en vue de cette Ã©chÃ©ance. 42 % indiquent quâ□□il ne sâ□□agit pas dâ□□une prioritÃ© pour elles en dÃ©pit des risques de sanctions financiÃ¨res qui pourraient leur coÃ»ter jusquâ□□Ã 4 % de leur chiffre dâ□□affaires mondial ou 20 millions dâ□□euros (selon le montant le plus Ã©levÃ© des deux).

74% des entreprises franÃ§aises interrogÃ©es expliquent quâ□□elles devront faire face Ã de sÃ©rieux dÃ©fis pour Ãªtre en conformitÃ© avec le GDPR. 58 % dÃ©clarent avoir dÃ©jÃ procÃ©dÃ© Ã une Ã©valuation de lâ□□impact sur les donnÃ©es, ou Ã un audit interne pour dÃ©terminer qui a accÃ¨s aux informations dâ□□identification personnelle dÃ©tenues par leur entreprise.

Mais 42 % des entreprises franÃ§aises disposent de moins dâ□□un an pour effectuer cette Ã©valuation et remÃ©dier Ã des accÃ¨s trop permissifs.

De plus, les rÃ©sultats des entreprises ayant rÃ©alisÃ© une Ã©valuation montrent que les normes en matiÃ¨re de rÃ©glementation des donnÃ©es font cruellement dÃ©faut dans la mesure oÃ¹ plus des deux tiers (69 %) des entreprises ont identifiÃ© au moins un cas dâ□□accÃ¨s trop permissif aux informations dâ□□identification personnelle.

Cela fait Ã©cho aux niveaux tout aussi alarmants dâ□□accÃ¨s trop permissifs aux donnÃ©es relevÃ©s dans le rapport 2017 de Varonis sur les risques liÃ©s aux donnÃ©es qui indique que, dans prÃ¨s de la moitiÃ© des entreprises, au moins 1 000 fichiers sensibles contenant des informations dâ□□identification personnelle sont accessibles Ã nâ□□importe quel employÃ©.

InterrogÃ©s sur les secteurs les plus susceptibles dâ□□Ãªtre sanctionnÃ©s, si une entreprise venait Ã Ãªtre victime dâ□□une violation de donnÃ©es, les dÃ©cideurs informatiques franÃ§ais citent les secteurs de lâ□□informatique, des technologies et des tÃ©lÃ©communications (19 %), devant le secteur financier (18 %).

Lorsque la question porte sur le pays, 58 % (contre 68 % des Britanniques) sont dâ□□accord ou entiÃ¨rement dâ□□accord pour dire quâ□□une entreprise du Royaume-Uni sera sanctionnÃ©e pour lâ□□exemple en cas dâ□□infraction dâ□□une disposition quelconque du rÃ¨glement GDPR de lâ□□UE du fait du Brexit.

Les difficultÃ©s de nombreuses entreprises Ã se prÃ©parer au GDPR figurent parmi les principaux constats de lâ□□Ã©tude :

55 % avouent avoir des difficultÃ©s Ã appliquer lâ□□article 17 du rÃ¨glement, le Â« droit Ã

lâ□□oubli Â», selon lequel elles doivent Ãªtre capables de localiser et de cibler des donnÃ©es spÃ©cifiques afin dâ□□automatiser leur suppression Ã la demande du consommateur.

52 % peinent Ã localiser les informations dâ□□identification personnelle sur leur rÃ©seau, Ã dÃ©terminer qui y a accÃ¨s et y accÃ¨de, et Ã savoir Ã quel moment ces donnÃ©es peuvent et doivent Ãªtre supprimÃ©es conformÃ©ment Ã lâ□□article 30, Â« Registre des activitÃ©s de traitement Â».

50 % ont des problÃ¨mes avec lâ□□article 32, Â« SÃ©curitÃ© du traitement Â», en vertu duquel elles doivent mettre en Å□uvre des privilÃ¨ges dâ□□accÃ¨s Â« a minima Â», instaurer un systÃ¨me de responsabilitÃ©, avec des dÃ©tenteurs dÃ©signÃ©s des donnÃ©es, et produire des rapports attestant que les politiques et processus adÃ©quats sont actifs et efficaces.

Â« La conclusion la plus inquiÃ©tante est quâ□□une entreprise sur quatre ignore oÃ¹ rÃ©sident ses donnÃ©es sensibles Â», commente Christophe Badot, Directeur GÃ©nÃ©ral France de Varonis. Â« Pour ces entreprises, le rÃ©veil risque dâ□□Ãªtre brutal dans un an.

Ã□ dÃ©faut dâ□□une parfaite visibilitÃ© sur lâ□□emplacement de leurs donnÃ©es sensibles, et sur les personnes qui y ont accÃ¨s et y accÃ¨dent, leurs chances de se conformer au rÃ¨glement sont minces, ce qui les place en tÃªte de liste des entreprises qui sâ□□exposeront Ã des sanctions. Â»

Â« Les entreprises du secteur public sont manifestement celles qui ont le plus de mal Ã se conformer au rÃ¨glement : elles sont beaucoup plus susceptibles de manquer de budget (26 % des entreprises du secteur public disposent dâ□□un budget distinct prÃ©vu Ã cet effet, contre 41 % dans le secteur privÃ©) Â», poursuit Christophe Badot.

Â« Nous avons reÃ§u un nombre considÃ©rable dâ□□appels dâ□□organismes du secteur public craignant de ne pas disposer des fonds ni des compÃ©tences nÃ©cessaires pour assurer leur mise en conformitÃ© dans les dÃ©lais impartis.

Ã□ moins dâ□□un changement avant lâ□□Ã©chÃ©ance fixÃ©e au mois de mai de lâ□□annÃ©e prochaine, la CNIL pourrait trÃ¨s bien infliger des sanctions financiÃ¨res Ã des organismes publics dÃ©jÃ Ã court dâ□□argent et affaiblis par une avalanche de cyberattaques, telles que le rÃ©cent ranÃ§ongiciel WannaCry. Â»

[1] Conclusions dâ□□une Ã©tude indÃ©pendante commandÃ©e par Varonis et rÃ©alisÃ©e par VansonBourne. Lâ□□Ã©tude porte sur un panel de 500 dÃ©cideurs informatiques issus dâ□□entreprises comptant plus de 1 000 employÃ©s (100 personnes interrogÃ©es au Royaume-Uni, en France et en Allemagne, et 200 en AmÃ©rique du Nord). Elle a Ã©tÃ© menÃ©e entre le 17 avril et le 9 mai 2017.