SÃ©curitÃ© des donnÃ©es : 5 dispositions Ã prendre pour les entreprises
SÃ©curitÃ©
PostÃ© par : JulieM
PubliÃ©e le : 16/12/2011 13:30:00

Julien Champagne, Directeur des ventes SafeNet France, Espagne et Portugal, tire les enseignements dâ□□une annÃ©e difficile sur le point de vue de la sÃ©curitÃ© des donnÃ©es, et l **â□□impact dâ□□un Ã©ventuel changement du cadre lÃ©gislatif** .

Cette annÃ©e 2011 aura Ã©tÃ© marquÃ©e par un grand nombre de failles de sÃ©curitÃ©, et ce phÃ©nomÃ¨ne indique clairement la nÃ©cessitÃ© d'une rÃ©glementation et dâ□□un contrÃ´le plus stricts sur le marchÃ© de la sÃ©curitÃ© des donnÃ©es. Ces failles ont Ã©rodÃ© la confiance des consommateurs en la capacitÃ© des entreprises Ã protÃ©ger leur donnÃ©es personnelles : dans le futur les dÃ©cideurs vont devoir prendre la protection des donnÃ©es beaucoup plus au sÃ©rieux, afin que le grand public ne perde pas confiance en lâ□□Ã©conomie numÃ©rique.

Dâ□□autant que le grand public pourrait bientÃ´t dÃ©couvrir que le nombre de failles de sÃ©curitÃ© est beaucoup plus important que lâ□□on imagine, puisque les organisations publiques et privÃ©es pourraient bientÃ´t Ãªtre frappÃ©es dâ□□une obligation lÃ©gislative de reporter aux autoritÃ©s compÃ©tentes les failles de sÃ©curitÃ©, et les pertes de donnÃ©es quâ□□elles provoquent.

En effet, la commission europÃ©enne prÃ©voit de rendre obligatoire le rapport des failles de sÃ©curitÃ© comme lâ□□a dÃ©clarÃ© Vivian Reeding, Vice PrÃ©sidente de la Commission EuropÃ©enne, en juillet dernier : Â« Les entreprises devraient renforcer leurs prÃ©cautions contre le vol d'identitÃ© et mieux protÃ©ger les donnÃ©es personnelles des consommateurs. Elles devraient immÃ©diatement notifier les violations de sÃ©curitÃ© des donnÃ©es et de confidentialitÃ©. J'ai l'intention d'introduire la condition obligatoire de notifier les violations de sÃ©curitÃ© des donnÃ©es pour tous les secteurs. Â». La Commission EuropÃ©enne prÃ©voirait Ã©galement dâ□□appliquer des sanctions financiÃ¨res, sous forme dâ□□amendes pouvant aller jusquâ□□Ã 5 % du chiffre dâ□□affaires pour les sociÃ©tÃ©s ayant perdu des donnÃ©es privÃ©es.

Les entreprises ne devraient pas attendre un changement du cadre lÃ©gislatif pour agir, et vraiment travailler Ã limiter les consÃ©quences dâ□□une brÃ¨che de sÃ©curitÃ©, en faisant en sorte par exemple, que les donnÃ©es perdues ou volÃ©es aient Ã©tÃ© chiffrÃ©es au prÃ©alable, et les clÃ©s de chiffrement utilisÃ©es tenues Ã l'Ã©cart des cybercriminels.

Cependant, le talon dâ□□Achille reste lâ□□humain, les emails, les piÃ¨ce-jointes ouvertes, car nous faisons confiance Ã la personne qui nous lâ□□envoie, ou parce que le contenu nous parait authentique. Câ□□est pourquoi une approche dÃ©fensive multicouche devient critique, et permet de contrer les attaques qui exploitent les failles humaines et la crÃ©dulitÃ© des utilisateurs en

protÃ©geant la donnÃ©e elle-mÃªme.

Mais nous devons Ã©galement ne pas oublier que lâ□□infrastructure elle-mÃªme doit Ãªtre protÃ©gÃ©e. La principale leÃ§on Ã retenir suite Ã lâ□□avalanche de failles de sÃ©curitÃ© est la nÃ©cessitÃ© de dÃ©ployer le chiffrement et de sÃ©curiser les clÃ©s de chiffrement elles-mÃªmes pour attÃ©nuer les dommages gÃ©nÃ©rÃ©s par ce type dâ□□attaque.

Voici les 5 dispositions que SafeNet recommande aux entreprises de prendre avant mÃªme le changement du cadre lÃ©gislatif:

1/Chiffrer et tokeniser les donnÃ©es critiques qui bougentâ□¦ et qui ne bougent pas non plus !

Le chiffrement est le meilleur moyen de sÃ©curiser les donnÃ©es. Que ce soit dans un datacenter ou sur un appareil mobile. Il protÃ¨ge les donnÃ©es en mouvement et celles qui ne le sont pas. En effet, les dommages causÃ©s par les failles rÃ©centes auraient Ã©tÃ© moindres si les entreprises avaient observÃ© cette Ã©tape. A lâ□□inverse des technologies DLP, le chiffrement est plus simple Ã mettre en place par les Ã©quipes IT puisquâ□□il ne repose pas sur le long processus de classification de donnÃ©es, qui repousse souvent les projets.

2/ AmÃ©liorer le contrÃ´le des donnÃ©es grÃ¢ce Ã lâ□□authentification forte

Fournir aux travailleurs en tÃ©lÃ©travail ou aux collaborateurs externes une authentification forte permet de sâ□□assurer que seules les personnes, les ressources et les applications autorisÃ©es accÃ¨dent aux informations.

3/ PrivilÃ©gier une approche unifiÃ©e

Les appareils mobiles prÃ©sentent un risque majeur, puisquâ□□ils peuvent Ãªtre facilement perdus ou volÃ©s. La mise en Å□uvre unifiÃ©e des programmes dâ□□authentification, des politiques de sÃ©curitÃ© et dâ□□un contrÃ´le des informations dâ□□identification pour les terminaux appartenant aux salariÃ©s permet de limiter les effets nÃ©gatifs de la Â« consumerisation Â» de lâ□□IT.

4/ SÃ©curiser lâ□□infrastructure elle-mÃªme

Prendre des mesures concrÃ¨tes pour sÃ©curiser lâ□□infrastructure elle-mÃªme en utilisant des modules de sÃ©curitÃ© matÃ©riels, Â« Hardware Security ModulesÂ», qui garantissent la protection des clÃ©s de chiffrement numÃ©riques. Ainsi, mÃªme si le hacker pÃ©nÃ©trait le rÃ©seau, il ne pourrait toujours pas accÃ©der aux clÃ©s !

5/ Envisager le chiffrement comme un service IT

Chiffrer ses donnÃ©es peut se rÃ©vÃ©ler dÃ©routant et compliquÃ© Ã envisager, mais de nombreuses entreprises, en raison de la modernisation des datacenters, commencent Ã centraliser le chiffrement et Ã fournir Â« le chiffrement comme service IT Â». Un service IT de chiffrement centralisÃ© permet aux Ã©quipes de gÃ©rer lâ□□ensemble de lâ□□aspect Â« protection des donnÃ©es Â». Ainsi, on Ã©vite que diffÃ©rents services ou filiales dâ□□une mÃªme entreprise ne crÃ©ent et ne gÃ¨rent leur propre chiffrement. Cela permet de gÃ©rer et dâ□□auditer plus facilement la sÃ©curitÃ© de lâ□□entreprise. Autre avantage supplÃ©mentaire : la gestion centralisÃ©e des clÃ©s. Lâ□□un des plus grands inconvÃ©nients lorsque chaque service ou filiale dâ□□une entreprise applique le chiffrement des donnÃ©es de son cÃ´tÃ© est la prolifÃ©ration des clÃ©s de sÃ©curitÃ©. En les centralisant, on assure une gestion plus efficace de ces clÃ©s.