Violations de donnÃ©es : Plus "si", mais "quand" se produisent-elles!
SÃ©curitÃ©
PostÃ© par : JulieM
PubliÃ©e le : 12/7/2016 14:30:00

Si les cas de violations de donnÃ©es Ã grande Ã©chelle alimentant rÃ©guliÃ¨rement l'actualitÃ© (Ashley Madison, Target, Sony, etc.) ont pu dÃ©montrer quelque chose, c'est qu'il ne s'agit plus pour les entreprises de savoir si elles seront attaquÃ©es mais plutÃ´t quand cela se produira.

Â
Les entreprises doivent savoir comment rÃ©agir et quelles actions mettre en place rapidement pour limiter la propagation des dÃ©gÃ¢ts causÃ©s par une fuite des donnÃ©es. Si chaque individu peut Ãªtre touchÃ© par ces attaques (cadres, dirigeants, consommateurs, employÃ©s et partenaires), seules les entreprises qui mettent en place des dispositifs de sÃ©curitÃ© en interne, pour minimiser l'impact des violations, seront en meilleure posture pour se dÃ©fendre face aux coÃ»ts et aux dÃ©gÃ¢ts causÃ©s.

Il est clair que, ces derniers temps, le comportement des entreprises a Ã©voluÃ© : au lieu de sâappuyer uniquement sur des mesures prÃ©ventives dans leur pÃ©rimÃ¨tre dâactions, elles s'assurent dÃ©sormais de disposer d'un contrÃ´le des dommages et d'une rÃ©sistance lorsque ces attaques se produisent. Ce n'est alors plus considÃ©rÃ© comme un signe de faiblesse lorsqu'un responsable sÃ©curitÃ© dÃ©clare Â« Je sais que nous ferons l'objet de cyberattaques mais je ne sais pas quel procÃ©dÃ© sera utilisÃ©. Â»

En revanche, ce qui pourrait nuire aux sociÃ©tÃ©s serait lâexposition dÃ©munie aux cyberattaques lorsque ces derniÃ¨res sont mal Ã©quipÃ©es en matiÃ¨re de sÃ©curitÃ© pour minimiser ces intrusions dans leur systÃ¨me. Ce nouveau comportement est en train de transformer la faÃ§on dont les entreprises considÃ¨rent la sÃ©curitÃ© informatique.

La rÃ©alitÃ©, c'est qu'il est pratiquement impossible de prÃ©dire et d'arrÃªter chaque attaque sur le web. Dans le monde digital d'aujourd'hui, les utilisateurs ont besoin d'accÃ©der Ã une diversitÃ© de systÃ¨mes, dâapplications et de donnÃ©es critiques dans le cadre de leur fonction. Non seulement ces ressources existent derriÃ¨re le pare-feu de l'entreprise, mais le recours systÃ©matique Ã l'application SaaS se traduit souvent par un accÃ¨s aux donnÃ©es en dehors du rÃ©seau de l'entreprise.

Ajoutons Ã cela la diversification croissante du mode d'accÃ¨s des utilisateurs Ã ces ressources, liÃ©e Ã l'adoption de l'informatique mobile, et vous obtenez un environnement extrÃªmement complexe. Les frontiÃ¨res du rÃ©seau traditionnel sont en train de s'estomper. Par consÃ©quent, sâabriter derriÃ¨re le mur de protection du rÃ©seau informatique de lâentreprise ne constitue plus une sÃ©curitÃ© suffisante.

L'un des signes les plus encourageants de ce changement d'attitude, c'est que beaucoup dâentreprises ont compris lâimportance de la visibilitÃ© et du contrÃ´le des accÃ¨s pour leurs applications, dans le cloud comme sur le web, et ce quel que soit le dispositif utilisÃ© pour y accÃ©der. C'est prÃ©cisÃ©ment ce qu'apportent la gouvernance des identitÃ©s et la gestion des accÃ¨s.

Placer une solution efficace de gestion des identitÃ©s au cÅur de leur stratÃ©gie de sÃ©curitÃ© permet aux entreprises de rÃ©agir rapidement Ã une intrusion, de mieux comprendre qui est

exposÃ© et ce qui est menacÃ©, et fondamentalement d'empÃªcher la propagation d'une attaque. Par consÃ©quent, mÃªme si nous faisions tout ce que nous pouvions pour nous protÃ©ger dâ□□une intrusion, lâ□□entreprise est capable de prendre des mesures efficaces pour augmenter sa rÃ©sistance et rÃ©duire l'impact nÃ©gatif d'une violation.

AprÃ¨s tout, ce n'est pas simplement lâ□□acte de violation des donnÃ©es, mais plutÃ´t la gravitÃ© de leur perte qui entraÃ®ne un impact sur l'activitÃ© de l'entreprise, nuit Ã sa marque, et au final affecte son chiffre d'affaires. Nous confirme Juliette Rizkallah, chief marketing officer, SailPoint.