Les PME mal Ã©quipÃ©es pour dÃ©tecter les intrusions en temps rÃ©el
SÃ©curitÃ©
PostÃ© par : JerryG
PubliÃ©e le : 18/7/2013 15:00:00

Au moment oÃ¹ les atteintes Ã la sÃ©curitÃ© deviennent une certitude, il est extrÃªmement utile de disposer dâ□□un Â« plan de secours Â», affirme Varonis.

Une rÃ©cente enquÃªte rÃ©alisÃ©e par la sociÃ©tÃ© Varonis, spÃ©cialiste de la protection des donnÃ©es, rÃ©vÃ¨le que plus de 40 % des responsables informatique ne bÃ©nÃ©ficient que de capacitÃ©s trÃ¨s faibles, voire nulles de dÃ©tection automatisÃ©e des atteintes Ã la sÃ©curitÃ© des donnÃ©es, quâ□□il sâ□□agisse dâ□□alertes en temps rÃ©el ou de rapports quotidiens/hebdomadaires. Les rÃ©sultats montrent quâ□□une proportion de 24 % soit prÃ¨s dâ□□un quart des rÃ©pondants ne possÃ¨dent pas de technologies automatisÃ©es en place pour dÃ©tecter les atteintes en surveillant les modifications des privilÃ¨ges utilisateurs, les accÃ¨s suspects aux donnÃ©es, les modifications dâ□□accÃ¨s aux fichiers ou une activitÃ© email inhabituelle. 19 % disposent dâ□□une capacitÃ© automatisÃ©e basique permettant la dÃ©tection de certains de ces Ã©vÃ©nements. Et uniquement 6 % des participants sont en mesure de surveiller tous ces Ã©vÃ©nements en temps rÃ©el.

Lâ□□enquÃªte, rÃ©alisÃ©e auprÃ¨s de 248 professionnels de la sÃ©curitÃ©, lors des confÃ©rences Infosecurity de Londres et dâ□□Orlando, visait Ã mieux comprendre comment les entreprises sont capables de dÃ©tecter des atteintes en cours.

Â« *Les rÃ©sultats de cette enquÃªte sont particuliÃ¨rement alarmants dans la mesure oÃ¹ aucun systÃ¨me de protection nâ□□est parfait, une intrusion par des hackers, des utilisateurs non autorisÃ©s ou des utilisateurs autorisÃ©s abusant de leur accÃ¨s, est inÃ©vitable* Â», indique **David Gibson**, vice-prÃ©sident de **Varonis**. Â« *Et comme les atteintes Ã la sÃ©curitÃ© sont une certitude, il est fortement conseillÃ© de disposer dâ□□un plan ou dâ□□une stratÃ©gie de secours visant Ã limiter les consÃ©quences dâ□□une intrusion.* Â»

En haut de la liste des mesures de limitation des risques figurent les techniques de dÃ©tection et de surveillance des Ã©vÃ©nements systÃ¨me inhabituels. Les contrÃ´les de dÃ©tection qui pistent et analysent les activitÃ©s utilisateurs, fichiers et systÃ¨me Ã la recherche dâ□□anomalies constituent un niveau primordial de dÃ©fense. Ils sont aussi importants que les contrÃ´les de prÃ©vention que sont lâ□□authentification, les listes de contrÃ´le dâ□□accÃ¨s et les pare-feux.

Une fois les dÃ©fenses de lâ□□entreprise traversÃ©es, les pirates cherchent des contenus de haute valeur, tels que des informations personnelles, des donnÃ©es de propriÃ©tÃ©s intellectuelles, des numÃ©ros de carte de crÃ©dit et toutes autres donnÃ©es sensibles.

La capacitÃ© quâ□□a un dÃ©partement informatique de pister ces donnÃ©es est fondamentale pour pouvoir limiter les consÃ©quences dâ□□une intrusion. Malheureusement, les participants se sont rÃ©vÃ©lÃ©s assez mal prÃ©parÃ©s dans ce domaine. Seuls 29 % dâ□□entre eux ont la

capacitÃ© de dÃ©tecter si des fichiers contenant des donnÃ©es sensibles sont consultÃ©s ou crÃ©Ã©s. Avec lâ□□avÃ¨nement de services de Cloud comme Dropbox, qui sont utilisÃ©s de faÃ§on informelle par les employÃ©s, les entreprises ont un nouveau domaine Ã explorer Ã la recherche de contenus sensibles. Les rÃ©sultats montrent que les entreprises doivent Ã©galement amÃ©liorer leurs capacitÃ©s de surveillance dans le Cloud : seuls 22 % des entreprises sont en mesure de pouvoir pister des donnÃ©es envoyÃ©es vers le cloud.

De faÃ§on plus positive, les grandes entreprises ont montrÃ© quâ□□elles parvenaient mieux Ã identifier les Ã©vÃ©nements anormaux au niveau des fichiers ou du systÃ¨me. 36 % de celles-ci utilisent des techniques automatisÃ©es pour dÃ©tecter les modifications de contrÃ´le dâ□□accÃ¨s aux fichiers (contre 28 % sur lâ□□ensemble des rÃ©pondants). 37 % utilisent lâ□□automatisation pour dÃ©tecter les modifications de privilÃ¨ges, contre 30 % si lâ□□on prend lâ□□ensemble du panel.

Â« *Lâ□□audit et lâ□□analyse du systÃ¨me, de la sÃ©curitÃ©, des applications et des journaux de consultation des fichiers sont essentiels Ã de bonnes pratiques de maÃ®trise des intrusions Â»,* remarque **David Gibson**. *Â« Les rÃ©sultats de lâ□□enquÃªte ne sont guÃ¨re encourageants, particuliÃ¨rement en matiÃ¨re de dÃ©couverte dâ□□intrusions impliquant des donnÃ©es sensibles lisibles par lâ□□homme dans les systÃ¨mes de fichiers de lâ□□entreprise. Seuls 28 % des participants sont en effet capables de dÃ©tecter un accÃ¨s suspect aux donnÃ©es.* Â»

Il ne fait aucun doute que ces dÃ©fenses de premiÃ¨re ligne sont critiques dans la prÃ©vention des atteintes de sÃ©curitÃ©. Cependant, les cybercriminels disposent de bien dâ□□autres vecteurs dâ□□attaque qui, combinÃ©s avec les APT (menaces persistantes avancÃ©es), ne peuvent pas toujours Ãªtre empÃªchÃ©es. Les entreprises doivent Ãªtre capables de dÃ©tecter ce quâ□□elles ne peuvent empÃªcher.

Â« *En dâ□□autres termes, les entreprises doivent admettre que, dÃ¨s le moment oÃ¹ elles stockent des donnÃ©es sensibles, quelquâ□□un cherchera Ã y accÃ©der, et un hacker ou un utilisateur interne malintentionnÃ© y accÃ©dera Ã un moment ou Ã un autre. Câ□□est pourquoi les mÃ©thodes de dÃ©tection de secours sont vitales pour stopper les atteintes dÃ¨s quâ□□elles se produisent, et donc pour limiter les dommages* Â», conclut **David Gibson**.