SÃ©curitÃ© : Un frein important Ã lâ□□adoption du Cloud.
SÃ©curitÃ©
PostÃ© par : JPilo
PubliÃ©e le : 3/11/2017 13:30:00

Les entreprises de la zone EMEA se tournent de plus en plus vers Office 365 de Microsoft, mÃªme si compte tenu de toutes les cyber attaques rÃ©centes, les inquiÃ©tudes concernant la sÃ©curitÃ© restent lâ□□un des freins les plus importants Ã lâ□□adoption du Cloud.

Telle est une des principales conclusions dâ□□une enquÃªte internationale conduite auprÃ¨s de plus de 1.100 organisations par Barracuda Networks, Inc. (NYSE: CUDA), un leader des solutions de sÃ©curitÃ© et de protection de donnÃ©es basÃ©es sur le cloud.

Lâ□□enquÃªte, intitulÃ©e â□□Office 365 Adoption Survey: Drivers, Risks, and Opportunitiesâ□□ avait pour but de mesurer les tendances autour de lâ□□adoption et de lâ□□utilisation de Microsoft Office 365, y compris les facteurs contribuant Ã la dÃ©cision pour ou contre la migration vers cette plate-forme.

Lâ□□Ã©tude a Ã©galement permis de rassembler des informations sur lâ□□utilisation par les entreprises de solutions tierces de sÃ©curitÃ© et de protection de donnÃ©es avec Office 365, et leur engagement vis Ã vis de revendeurs Ã valeur ajoutÃ©e (VARs) et de fournisseurs de services managÃ©s.

Commentant ces rÃ©sultats, Chris Ross, SVP International chez Barracuda Networks, a dÃ©clarÃ© : â□□Lâ□□adoption dâ□□Office 365 continuant dâ□□augmenter dâ□□une annÃ©e sur lâ□□autre en Europe, il est naturel dâ□□assumer que les inquiÃ©tudes concernant les cyber menaces vont persister.Â

Mais il est encourageant de constater que les entreprises sâ□□Ã©veillent Ã lâ□□importance dâ□□une approche de protection multi-couches, ce qui suggÃ¨re une meilleure comprÃ©hension de leurs obligations lors de lâ□□adoption du Cloud.â□□

â□□Un domaine oÃ¹ lâ□□Europe a encore du chemin Ã faire pour atteindre les niveaux constatÃ©s aux Etats Unis est lâ□□adoption de solutions tierces pour ajouter une couche supplÃ©mentaire de sÃ©curitÃ© contre les attaques de spear phishing, dâ□□usurpation dâ□□identitÃ© et de â□□social engineeringâ□□,â□□ a-t-il ajoutÃ©.

â□□Seules 14 pour cent des organisations de la zone EMEA ont dÃ©jÃ quelque chose en place, Ã comparer Ã 36 pour cent aux Etats Unis. Nous pensons que cette situation devrait Ã©voluer au cours de lâ□□annÃ©e qui vient, et nous incitons les entreprises europÃ©ennes Ã y prÃªter attention.Â

Nous constatons que les cyber criminels changent de cibles, passant du top management Ã des employÃ©s plus bas dans la hiÃ©rarchie, et de grandes entreprises Ã des organisations plus petites disposant de moins de ressources.â□□

Principales conclusions dans la zone EMEA :

â□□ PrÃ¨s des deux tiers (62%) des entreprises de la zone EMEA utilisent dÃ©sormais Office 365, en augmentation de 50 pour cent par rapport Ã une enquÃªte similaire rÃ©alisÃ©e par Barracuda en 2016.

â□□ Parmi celles qui nâ□□utilisent pas aujourdâ□□hui Office 365, un peu moins de 40% indiquent quâ□□elles prÃ©voient de migrer dans lâ□□avenir â□□ une proportion moindre quâ□□aux Etats Unis, oÃ¹ prÃ¨s de 49% dÃ©clarent prÃ©voir cette migration.

â□□ La plus grande inquiÃ©tude visant la sÃ©curitÃ© pour plus de 90% des entreprises europÃ©ennes concerne les ransomwares. PrÃ¨s la moitiÃ© dâ□□entre elles (48%) avouent avoir dÃ©jÃ Ã©tÃ© frappÃ©e par une infection de ce type, mÃªme si seulement 3% dâ□□entre elles ont finalement payÃ© la ranÃ§on.

â□□ Pour les entreprises ayant dÃ©jÃ Ã©tÃ© frappÃ©es, lâ□□email a Ã©tÃ© de loin le principal vecteur dâ□□attaque pour les cyber-criminels, prÃ¨s des trois quarts (70%) des attaques par ransomware arrivant via email. Les trafic Web (18%) et le trafic rÃ©seau (12%) nâ□□ont reprÃ©sentÃ© quâ□□un nombre relativement faible dâ□□infections.

â□□ La raison la plus couramment invoquÃ©e pour ne pas migrer vers Office 365 a changÃ© depuis lâ□□Ã©tude de lâ□□annÃ©e derniÃ¨re, les entreprises europÃ©ennes rejoignant les amÃ©ricaines en plaÃ§ant en tÃªte les inquiÃ©tudes concernant la sÃ©curitÃ© (32%). Mais Ã la diffÃ©rence des Etats Unis, les entreprises europÃ©ennes citent toujours une politique â□□no Cloudâ□□ comme une raison significative de ne pas migrer (28%).

â□□ MalgrÃ© ces inquiÃ©tudes, plus de 85 pour cent des entreprises europÃ©ennes interrogÃ©es ont indiquÃ© ne pas utiliser la fonction Advanced Threat Protection (ATP) de Microsoft Office 365 â□□ sâ□□appuyant plutÃ´t sur des solutions tierces pour accroÃ®tre la protection de leurs environnements Office 365.Â

Plus de deux cinquiÃ¨mes dâ□□entre elles (43%) utilisent des solutions tierces de sÃ©curitÃ©, dâ□□archivage ou de sauvegarde, ce chiffre Ã©tant encore plus important (68%) parmi celles qui prÃ©voient de migrer.

â□□ A cÃ´tÃ© de cela, 41% des organisations interrogÃ©es ont dÃ©clarÃ© redouter des attaques de phishing, de spear phishing, dâ□□usurpation dâ□□identitÃ© ou de â□□social engineeringâ□□.

Toutefois, seules 14% des organisations europÃ©ennes ont indiquÃ© disposer dâ□□une solution tierce pour adresser ces menaces.

â□□Ces rÃ©sultats confirment la prise de conscience croissante des besoins de sÃ©curitÃ© que nous constatons chez nos clients, et la nÃ©cessitÃ© dâ□□adopter une approche multi-couches pour progresser,â□□ a ajoutÃ© Sanjay Ramnath, Vice President of Security Products and Business Strategy chez Barracuda.Â

â□□Nos clients et nos partenaires indirects qui dÃ©ploient Barracuda Sentinel et Barracuda Essentials for Office 365 peuvent migrer certains de leurs processus de gestion stratÃ©giques dans le Cloud, tout en Ã©tant certains dâ□□Ãªtre protÃ©gÃ©s contre les ransomwares, les attaques de spear phishing et dâ□□autres menaces avancÃ©es.â□□

Barracuda Essentials for Office 365 est une solution multi-couches de sÃ©curitÃ© email, de sauvegarde et dâ□□archivage en mode Cloud qui aide Ã protÃ©ger les organisations contre les attaques avancÃ©es via email et les pertes de donnÃ©es, tout en minimisant les interruptions dâ□□exploitation.

Barracuda Sentinel combine trois puissantes composantes comprenant une technologie dâ□□intelligence artificielle, un outil de visualisation des usurpations de noms de domaine utilisant lâ□□authentification DMARC, et une formation contre les techniques de fraude, dans une mÃªme solution qui protÃ¨ge contre les attaques personnalisÃ©es dâ□□aujourdâ□□hui.Â

La solution sâ□□intÃ¨gre directement avec lâ□□API Office 365 pour un dÃ©ploiement facile, sans composant matÃ©riel ni logiciel Ã gÃ©rer.

Plus sur lâ□□enquÃªte.