

### S curit  : Un frein important   l'adoption du Cloud.

#### S curit 

Post  par : JPilo

Publi 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, m me si compte tenu de toutes les cyber attaques r centes, les inqui tudes concernant la s curit  restent l'un des freins les plus importants   l'adoption du Cloud.

Telle est une des principales conclusions d'une enqu te internationale conduite aupr s de plus de 1.100 organisations par Barracuda Networks, Inc. (NYSE: CUDA), un leader des solutions de s curit  et de protection de donn es bas es sur le cloud.



L'enqu te, intitul e   Office 365 Adoption Survey: Drivers, Risks, and Opportunities   avait pour but de mesurer les tendances autour de l'adoption et de l'utilisation de Microsoft Office 365, y compris les facteurs contribuant   la d cision pour ou contre la migration vers cette plate-forme.

L' tude a  galement permis de rassembler des informations sur l'utilisation par les entreprises de solutions tierces de s curit  et de protection de donn es avec Office 365, et leur engagement vis   vis de revendeurs   valeur ajout e (VARs) et de fournisseurs de services manag s.

Commentant ces r sultats, Chris Ross, SVP International chez Barracuda Networks, a d clar  :   L'adoption d'Office 365 continuant d'augmenter d'une ann e sur l'autre en Europe, il est naturel d'assumer que les inqui tudes concernant les cyber menaces vont persister.  

Mais il est encourageant de constater que les entreprises s veillent   l'importance d'une approche de protection multi-couches, ce qui sugg re une meilleure compr hension de leurs obligations lors de l'adoption du Cloud.

Un domaine o  l'Europe a encore du chemin   faire pour atteindre les niveaux constat s aux Etats Unis est l'adoption de solutions tierces pour ajouter une couche suppl mentaire de s curit  contre les attaques de spear phishing, d'usurpation d'identit  et de social engineering, a-t-il ajout .

Seules 14 pour cent des organisations de la zone EMEA ont d j  quelque chose en place,   comparer   36 pour cent aux Etats Unis. Nous pensons que cette situation devrait  voluer au cours de l'ann e qui vient, et nous incitons les entreprises europ ennes   y pr ter attention.

Nous constatons que les cyber criminels changent de cibles, passant du top management   des employ s plus bas dans la hi rarchie, et de grandes entreprises   des organisations plus petites disposant de moins de ressources.

### Principales conclusions dans la zone EMEA :

Pr s des deux tiers (62%) des entreprises de la zone EMEA utilisent d sormais Office 365, en augmentation de 50 pour cent par rapport   une enqu te similaire r alis e par Barracuda en 2016.

Parmi celles qui n'utilisent pas aujourd'hui Office 365, un peu moins de 40% indiquent qu'elles pr voient de migrer dans l'avenir   une proportion moindre qu'aux Etats Unis, o  pr s de 49% d clarent pr voir cette migration.

La plus grande inqui tude visant la s curit  pour plus de 90% des entreprises europ ennes concerne les ransomwares. Pr s la moiti  d'entre elles (48%) avouent avoir d j   t  frapp e par une infection de ce type, m me si seulement 3% d'entre elles ont finalement pay  la ran on.

Pour les entreprises ayant d j   t  frapp es, l'email a  t  de loin le principal vecteur d'attaque pour les cyber-criminels, pr s des trois quarts (70%) des attaques par ransomware arrivant via email. Les trafic Web (18%) et le trafic r seau (12%) n'ont repr sent  qu'un nombre relativement faible d'infections.

La raison la plus couramment invoqu e pour ne pas migrer vers Office 365 a chang  depuis l' tude de l'ann e derni re, les entreprises europ ennes rejoignant les am ricaines en pla ant en t te les inqui tudes concernant la s curit  (32%). Mais   la diff rence des Etats Unis, les entreprises europ ennes citent toujours une politique n o Cloud  comme une raison significative de ne pas migrer (28%).

Malgr  ces inqui tudes, plus de 85 pour cent des entreprises europ ennes interrog es ont indiqu  ne pas utiliser la fonction Advanced Threat Protection (ATP) de Microsoft Office 365   s'appuyant plut t sur des solutions tierces pour accro tre la protection de leurs environnements Office 365.

Plus de deux cinqui mes d'entre elles (43%) utilisent des solutions tierces de s curit , d'archivage ou de sauvegarde, ce chiffre  tant encore plus important (68%) parmi celles qui pr voient de migrer.

A c t  de cela, 41% des organisations interrog es ont d clar  redouter des attaques de phishing, de spear phishing, d'usurpation d'identit  ou de social engineering.

Toutefois, seules 14% des organisations europ ennes ont indiqu  disposer d'une solution tierce pour adresser ces menaces.

Ces r sultats confirment la prise de conscience croissante des besoins de s curit  que nous constatons chez nos clients, et la n cessit  d'adopter une approche multi-couches pour progresser, a ajout  Sanjay Ramnath, Vice President of Security Products and Business Strategy chez Barracuda.

Nos clients et nos partenaires indirects qui d ploient Barracuda Sentinel et Barracuda Essentials for Office 365 peuvent migrer certains de leurs processus de gestion strat giques dans le Cloud, tout en  tant certains d' tre prot g s contre les ransomwares, les attaques de spear phishing et d'autres menaces avanc es.

Barracuda Essentials for Office 365 est une solution multi-couches de s curit  email, de sauvegarde et d'archivage en mode Cloud qui aide   prot ger les organisations contre les attaques avanc es via email et les pertes de donn es, tout en minimisant les interruptions d'exploitation.

Barracuda Sentinel combine trois puissantes composantes comprenant une technologie d'intelligence artificielle, un outil de visualisation des usurpations de noms de domaine utilisant l'authentification DMARC, et une formation contre les techniques de fraude, dans une m me solution qui prot ge contre les attaques personnalis es d'aujourd'hui.

La solution s'int gre directement avec l'API Office 365 pour un d ploiement facile, sans composant mat riel ni logiciel  g rer.

**[Plus sur l'enqu te.](#)**