La gÃ©nÃ©ration Y peut soucieuse de la sÃ©curitÃ©
SÃ©curitÃ©
PostÃ© par : JerryG
PubliÃ©e le : 21/6/2012 14:00:00

Fortinet, lâ□□un des leaders de la sÃ©curitÃ© rÃ©seau haute performance â□□ a menÃ© une Ã©tude mondiale qui rÃ©vÃ¨le lâ□□ampleur des dÃ©fis posÃ©s aux systÃ¨mes informatiques des entreprises par la premiÃ¨re gÃ©nÃ©ration dâ□□utilisateurs du Bring Your Own Device (BYOD ou Â« Apportez votre appareil personnel Â» en franÃ§ais); les personnes qui utilisent leurs propres appareils au sein de leur entreprise.

Lâ□□Ã©tude dÃ©crit que les salariÃ©s Gen-Y qui utilisent leurs propres appareils se soucient peu des problÃ¨mes sÃ©curitaires, rÃ©vÃ©lant le fait inquiÃ©tant que plus dâ□□un tiers des salariÃ©s questionnÃ©s serait prÃªt Ã transgresser la politique de sÃ©curitÃ© de lâ□□entreprise qui leur interdit dâ□□utiliser leurs appareils personnels au travail ou Ã de fins professionnelles. Dans lâ□□ensemble, les rÃ©sultats mettent en Ã©vidence lâ□□urgence pour les entreprises dâ□□Ã©laborer des stratÃ©gies de sÃ©curitÃ© pour sÃ©curiser et gÃ©rer lâ□□activitÃ© BYOD.

Lâ□□Ã©tude, menÃ©e dans 15 pays au cours des mois de Mai/Juin 2012, a interrogÃ© plus de 3 800 salariÃ©s actifs Ã¢gÃ©s de 20 Ã 29 ans pour connaitre leurs points de vue sur le BYOD, son impact sur leur environnement de travail et leur approche en matiÃ¨re de sÃ©curitÃ© informatique dâ□□entreprise et personnelle.

La Forte DÃ©pendance Envers les Communications Personnelles Rend le BYOD Incontournable

Pour les personnes interrogÃ©es au cours de cette Ã©tude, qui reprÃ©sentent les dÃ©cisionnaires et gestionnaires de demain, le BYOD est confirmÃ© comme une activitÃ© courante. PrÃ¨s des trois quarts (74%) de lâ□□ensemble des sondÃ©s se livrent dÃ©jÃ rÃ©guliÃ¨rement Ã cette pratique contre 64% des FranÃ§ais. Plus important encore, 55% des personnes interrogÃ©es et 69% des FranÃ§ais, considÃ¨rent lâ□□utilisation de leurs appareils au travail comme un â□□droitâ□□ plutÃ´t quâ□□un â□□privilÃ¨ge.â□□

Du point de vue de lâ□□utilisateur, le principal facteur de la pratique du BYOD est que les individus peuvent Ã tout moment accÃ©der Ã leurs applications prÃ©fÃ©rÃ©es, notamment les rÃ©seaux sociaux et les communications privÃ©es. La dÃ©pendance Ã lâ□□Ã©gard des communications personnelles est frappante avec 35% des sondÃ©s admettant quâ□□ils ne pourraient pas passer plus dâ□□une journÃ©e sans avoir accÃ¨s aux rÃ©seaux sociaux et 47% seraient incapables de passer une journÃ©e sans SMS. La dÃ©pendance semble moins importante en France Ã ce jour

puisque les rÃ©sultats cÃ´tÃ© FranÃ§ais sont respectivement de 19% pour les rÃ©seaux sociaux et de 38% pour les SMS.

Une Faible ConsidÃ©ration des Risques Professionnels AmÃ¨ne les SalariÃ©s Ã Transgresser la Politique de lâ□□Entreprise

La premiÃ¨re gÃ©nÃ©ration de salariÃ©s adeptes du BYOD comprend les risques posÃ©s par le BYOD Ã leur organisation. Effectivement, 42% de lâ□□Ã©chantillon (contre 36% des FranÃ§ais) estiment que la possibilitÃ© de perte des donnÃ©es et lâ□□exposition aux menaces informatiques malveillantes est le principal risque. Pourtant, ce qui est inquiÃ©tant pour les dÃ©partements informatiques, câ□□est que la prise de conscience de ce risque nâ□□empÃªche pas un grand nombre de salariÃ©s dâ□□Ãªtre prÃªt Ã contourner les politiques de lâ□□entreprise. En effet, plus dâ□□un tiers des sondÃ©s (36% et 30% des FranÃ§ais) ont admis quâ□□ils ont ou seraient prÃªts Ã transgresser la politique de lâ□□entreprise interdisant lâ□□utilisation des appareils personnels Ã des fins professionnelles. Parmi les 15 pays interrogÃ©s, le chiffre le plus Ã©levÃ© est celui de lâ□□Inde avec 66% des sondÃ©s.

Concernant les politiques interdisant lâ□□utilisation des applications non autorisÃ©es, le chiffre reste Ã peu prÃ¨s le mÃªme, avec 30% de lâ□□ensemble des personnes interrogÃ©es (contre 25% de FranÃ§ais) admettant quâ□□elles ont ou seraient prÃªtes Ã transgresser la politique. Pour les organisations, les risques liÃ©s aux applications non autorisÃ©es vont sâ□□accroitre. En effet, 69% des sondÃ©s (contre 59% de FranÃ§ais) ont confirmÃ© quâ□□ils sont intÃ©ressÃ©s par le Bring Your Own Application (Â« Apportez votre propre application Â» en franÃ§ais) - dÃ©crivant le fait que les utilisateurs pourront crÃ©er et utiliser leurs propres applications personnalisÃ©es au travail.

Lâ□□Ã©tude fait Ã©galement allusion Ã la rÃ©sistance Ã laquelle les organisations pourraient faire face si elles dÃ©cident de mettre en place une solution de sÃ©curitÃ© sur lâ□□appareil du salariÃ©. La majoritÃ© des sondÃ©s (66% et 69% des FranÃ§ais) se considÃ¨rent eux-mÃªmes â□□ et non lâ□□entreprise â□□ responsables de la sÃ©curitÃ© de leurs appareils personnels utilisÃ©s Ã des fins professionnelles. Câ□□est de trois Ã presque six fois plus que ceux qui estiment que la responsabilitÃ© incombe finalement Ã leurs employeurs (22% contre 12% des FranÃ§ais).

â□□*Lâ□□Ã©tude rÃ©vÃ¨le clairement lâ□□important dÃ©fi rencontrÃ© par les organisations pour concilier la sÃ©curitÃ© et le BYOD*,â□□ dÃ©clare **Yann Pradelle**, Vice-PrÃ©sident RÃ©gional Europe du Sud et Afrique chez Fortinet. â□□*Alors que les utilisateurs veulent et sâ□□attendent Ã utiliser leurs propres appareils pour le travail, la plupart pour un confort personnel, ils ne veulent pas confier la responsabilitÃ© de la sÃ©curitÃ© de leurs propres appareils Ã lâ□□organisation. Dans un tel environnement, les organisations doivent reprendre le contrÃ´le de leur infrastructure informatique par une forte sÃ©curisation Ã la fois de lâ□□accÃ¨s entrant et sortant du rÃ©seau de lâ□□entreprise et pas uniquement implÃ©menter une gestion des appareils mobiles ou â□□MDMâ□□. Les organisations ne peuvent pas compter sur une seule technologie pour rÃ©pondre aux dÃ©fis de sÃ©curitÃ© du BYOD. La stratÃ©gie de sÃ©curitÃ© rÃ©seau la plus efficace demande un contrÃ´le prÃ©cis sur les utilisateurs et les applications, et pas seulement sur les appareils*.â□□