Communiqué de Presse

Contact Presse:

Annabelle Sou
Fortinet
+ 33 (0)4 89 87 05 76
asou@fortinet.com

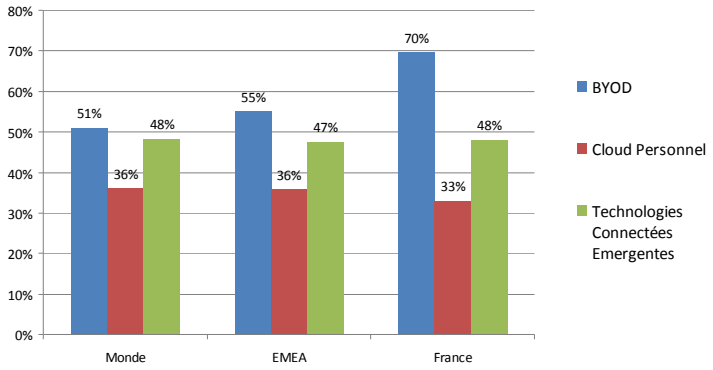
L'Etude Mondiale Fortinet Montre la Forte Détermination de la Génération Y à Transgresser les Politiques BYOD/Bring-Your-Own-Cloud de l'Entreprise, Alors que les Technologies Emergentes Arrivent sur Le lieu de Travail

Jusqu'à 51% (et 70% en France) des salariés âgés de 21 à 32 ans seraient prêts à transgresser les politiques de l'entreprise limitant l'utilisation des appareils, des services de stockage cloud et des technologies 'wearable' personnels à des fins professionnelles

Sophia Antipolis, 21 Octobre 2013 - Fortinet® (NASDAQ: FTNT) - l'un des leaders de la sécurité réseau haute performance – publie aujourd'hui une étude mondiale qui révèle la tendance grandissante de la Génération Y active à être prête à transgresser les politiques de l'entreprise régissant l'utilisation de leurs propres appareils, comptes de stockage cloud personnels et nouvelles technologies telles que les montres intelligentes, les Google Glass et les voitures connectées. Menée dans 20 pays en Octobre 2013 auprès de 3200 salariés âgés de 21 à 32 ans, les résultats de cette enquête indépendante montrent une augmentation de 42% - contre 94% en France - dans la volonté d'enfreindre les règles d'usage par rapport à l'enquête Fortinet similaire menée l'an dernier[1]. Cette nouvelle étude décrit également dans quelle mesure la Génération Y a été victime de cybercriminalité sur ses propres appareils, évalue ses 'connaissances sur les menaces Internet' et l'étendue des pratiques de stockage des actifs de l'entreprise sur des comptes cloud personnels.

1 L'étude de la Sécurité Internet 2012 de Fortinet a interrogé 3872 salariés de 20 à 29 ans dans 15 pays et a posé exactement la même question.

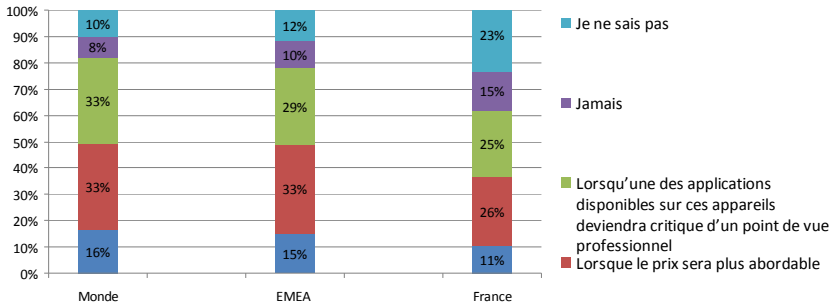
Forte Tendance à la Transgression



Alors que l'échantillon global est plutôt bienveillant à l'égard des dispositions prises par leurs employeurs en matière de politiques BYOD, avec au total, 45% des personnes interrogées confirmant qu'elles les 'avantagent' (34% en France), 51% déclarent qu'elles seraient prêtes à transgresser les politiques mises en place interdisant l'utilisation d'appareils personnels au travail ou à des fins professionnelles. En France, cette tendance est encore plus forte puisqu'elle atteint 70%. Cette tendance alarmante à ignorer les mesures visant à protéger aussi bien l'employeur que les salariés s'applique à d'autres domaines de l'utilisation personnelle de l'informatique. 36% des personnes interrogées utilisant leurs propres comptes de stockage cloud personnels (par exemple DropBox) à des fins professionnelles déclarent qu'elles seraient prêtes à enfreindre les règles leur interdisant d'utiliser ces services. En France, elles représentent 33%. Concernant les technologies émergentes telles que les Google Glass et les montres intelligentes, presque la moitié (48% dans le monde et en France) des personnes interrogées seraient prêtes à transgresser les politiques visant à limiter l'utilisation de ces appareils au travail.

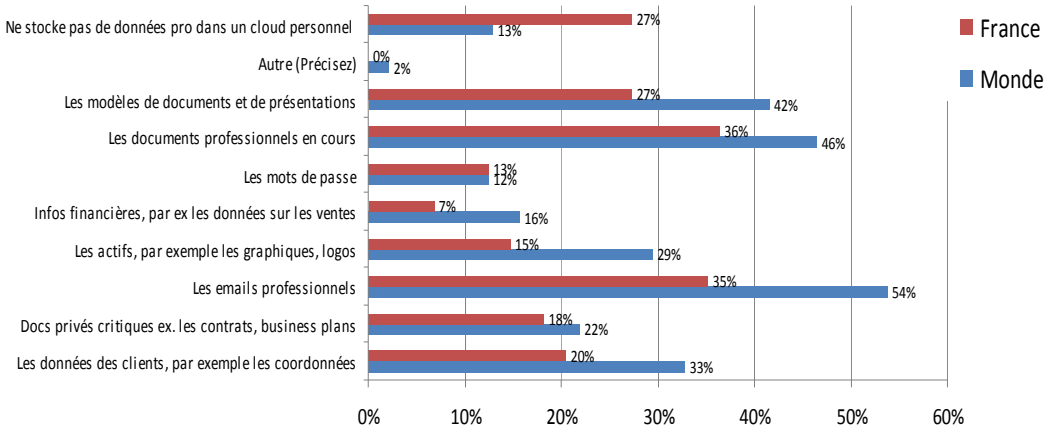
La Technologie 'Wearable' Prête à Entrer sur le Lieu de Travail

Interrogées sur le temps nécessaire à la propagation des technologies 'wearable' (technologies qui se portent sur soi), telles que les montres intelligentes et les Google Glass, sur le lieu de travail ou à des fins professionnelles, 16% des sondés déclarent 'immédiatement' et 33% lorsque leurs prix baisseront. En France, ces pourcentages sont respectivement de 11% et 26%. Seulement 8% de l'échantillon et 15% en France, ne pense pas que ces technologies vont se répandre.

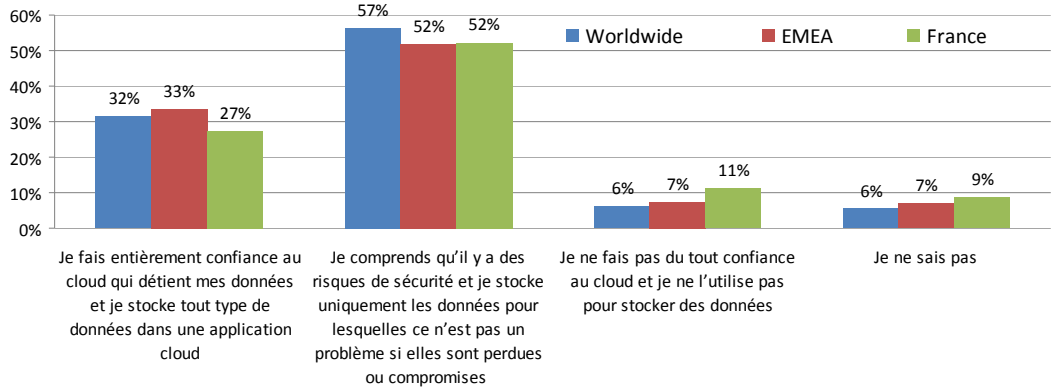


L'Utilisation Généralisée des Comptes Cloud Personnels pour les Données Sensibles de l'Entreprise

89% de l'échantillon global possède au moins un compte de service de stockage cloud personnel contre 82% en France. A noter que DropBox est utilisé par 38% de l'échantillon total et 28% en France. 70% des titulaires de comptes personnels ont utilisé leurs comptes à des fins professionnelles. En France, ils représentent 58%. Au niveau mondial, 12% de ces titulaires admettent stocker les mots de passe professionnels à l'aide de ces comptes (13% en France), 16% des informations financières (7% en France), 22% des documents privés sensibles comme les contrats/business plans (18% en France), tandis qu'un tiers (33%) stockent des données clients (20% en France).

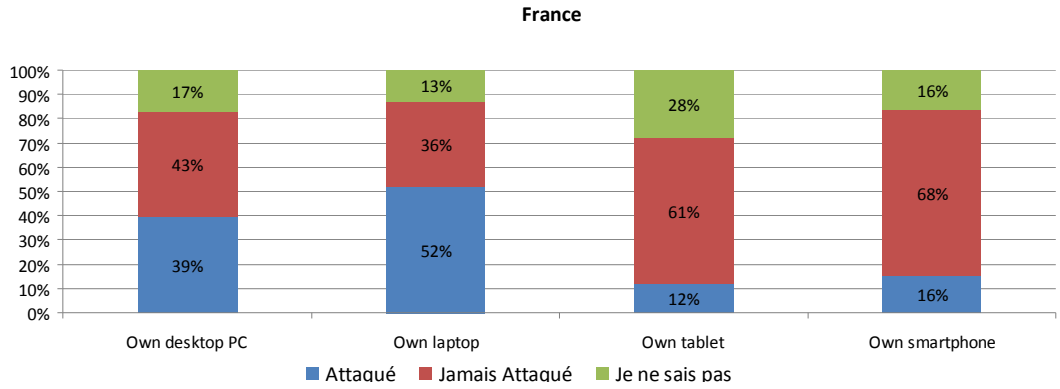


Presque un tiers (32%) des utilisateurs de stockage cloud de l'échantillon déclarent qu'ils font entièrement confiance au cloud qui détient leurs données personnelles, et seulement 6% déclarent y être hostiles par manque de confiance. En France, ils sont respectivement 27% et 11%.



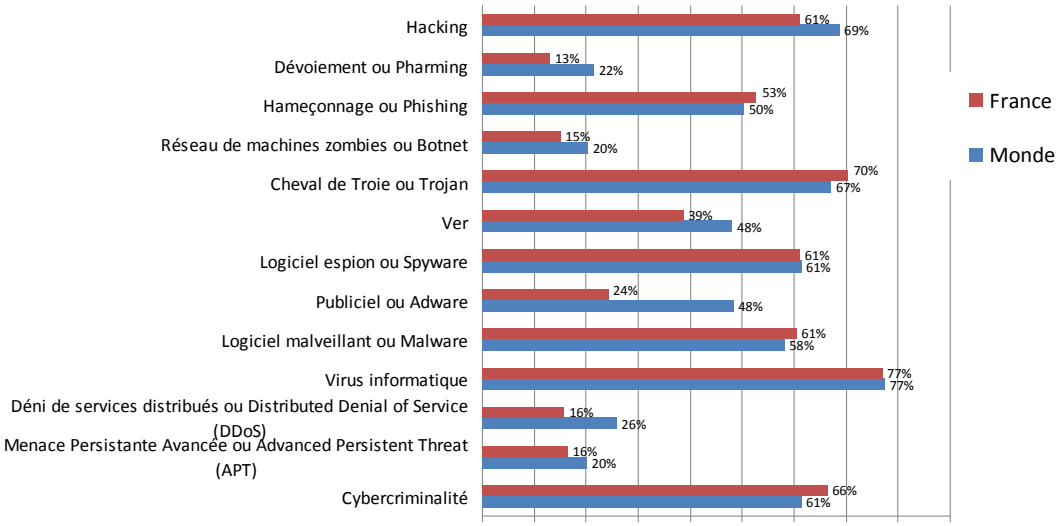
Connaissance des Menaces Requise alors que l'Etude Montre que les Attaques sont Réelles

Interrogées sur la compromission de leurs appareils et l'impact qui en a résulté, plus de 55% des sondés indiquent avoir été victimes d'une attaque sur leurs PC ou ordinateurs portables personnels (plus de 45% en France), et environ la moitié (en France, moins de la moitié) affirment que ces attaques ont affecté leur productivité et/ou ont engendré une perte de données personnelles et/ou d'entreprise. Alors que l'échantillon contient un plus grand nombre de détenteurs de smartphones personnels que d'ordinateurs portables et PC, les attaques ont été beaucoup moins fréquentes sur les smartphones (19% au monde et 16% en France), avec une proportion légèrement plus élevée à entrainer une perte des données et/ou une perte de productivité au travail que celle constatée sur les PC/ordinateurs portables. Le même pourcentage a été observé pour les tablettes (19% au monde et 12% en France), mais avec des conséquences plus importantes, puisque 61% (72% en France) de ces attaques ont eu des répercussions importantes.



Parmi l'une des conclusions inquiétantes de l'étude, 14% des personnes interrogées déclarent qu'elles ne seraient pas prêtes à avouer à leur employeur si l'un des appareils personnels qu'elles utilisent à des fins professionnelles était compromis. En France, ce pourcentage est de 18% .

L'enquête a examiné le 'degré de connaissances' des personnes interrogées sur les différents types de menaces de sécurité, et les résultats révèlent deux extrêmes opposés - l'ignorance et le savoir -, avec entre deux, une moyenne de 27% de degré de connaissance minimal (24% en France). Interrogées sur les menaces comme les APT, DDoS, Botnets et Pharming, jusqu'à 52% - contre 67% en France - se révèlent incultes sur ces types de menaces. Ce constat est l'occasion pour les départements informatiques de former les salariés sur les menaces et leur impact.



L'enquête indique également un lien direct entre l'usage du BYOD et la connaissance des menaces, montrant que plus les sondés ont l'habitude du BYOD, meilleure est leur compréhension des menaces. Cette conclusion est positive pour les entreprises qui envisagent si/quand elles doivent établir des politiques en association avec une formation sur les risques.

"*L'étude de cette année soulève les problèmes rencontrés par les entreprises qui tentent de mettre en place des politiques autour de l'utilisation du BYOD, des applications cloud et bientôt de l'adoption des nouvelles technologies connectées*," déclare Yann Pradelle, Vice Président de l'Europe du Sud et Afrique du Nord chez Fortinet. "*L'étude souligne également le défi majeur auquel sont confrontés les responsables informatiques quand il s'agit de savoir où se trouvent les données de l'entreprise et la façon dont elles sont accessibles. Il y a maintenant plus que jamais le besoin d'une intelligence sécuritaire à instaurer au niveau du réseau dans le but de permettre le contrôle des activités de l'utilisateur en fonction des appareils, des applications utilisées et de sa situation géographique.*"

"*Il est inquiétant de voir la transgression des politiques si élevée et en si forte hausse, ainsi que les nombreux sondés issus de la Génération Y ayant été victimes de cybercriminalité*," poursuit Yann Pradelle. "*Cependant, le côté positif est que 88% des personnes interrogées – et 82% en France - admettent qu'elles doivent comprendre les risques de sécurité posés par leurs propres appareils. La formation des salariés sur les menaces et son possible impact est un autre aspect clé pour assurer la sécurité informatique d'une entreprise.*"

Note aux rédactions
L'Etude de la Sécurité Internet 2013 de Fortinet a été un exercice de recherches entrepris entre le 7 et le 13 octobre 2013 au nom de Fortinet par Vision Critical, entreprise d'étude de marché indépendante. L'étude a impliqué 3200 individus disposant d'un Bac+4 au minimum, âgés de 21 à 32, salariés à temps plein, et détenteurs de leurs propres smartphones, tablettes ou ordinateurs portables.

*20 pays ont participé à cette étude: Brésil, Canada, Chili, Chine, Colombie, France, Allemagne, Hong Kong, Inde, Italie, Japon, Corée, Mexique, Pays-Bas, Pologne, Russie, Espagne, Taiwan, Royaume-Uni et Etats-Unis.

A propos de Fortinet (www.fortinet.fr)
Fortinet (code NASDAQ : FTNT) est un des principaux fournisseurs de solutions de sécurité réseau et un des leaders du marché des systèmes unifiés de sécurité **Unified Threat Management** ou UTM. Nos produits et services d'abonnements assurent une protection étendue, intégrée et efficace contre les menaces dynamiques, tout en simplifiant l'infrastructure de sécurité informatique. Parmi nos clients figurent des administrations, des fournisseurs d'accès et de nombreuses entreprises, dont la plupart font partie du classement 2012 du Fortune Global 100. FortiGate, le produit phare de Fortinet, intègre des processeurs ASIC pour une meilleure performance et plusieurs fonctions de sécurité conçues pour protéger les applications et les réseaux contre les menaces Internet. Au-delà de ses solutions UTM, Fortinet offre une large gamme de produits conçus pour protéger le périmètre étendu des entreprises – du terminal au périmètre et au cœur de réseau, en passant par les bases de données et applications. Fortinet, dont le siège social se trouve à Sunnyvale en Californie (États-Unis), dispose également de bureaux dans le monde entier.

###

FTNT-O