



Communiqué de Presse - Embargo jusqu'au 27 Juin 2011

Contact Presse:

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

Une Etude Européenne sur la Sécurité IT Révèle Comment les Entreprises Font Face Aux Tendances Emergentes

Parmi les principales conclusions: les réseaux sans-fil sont identifiés comme étant la plus grande vulnérabilité; une position draconienne est adoptée à l'encontre de l'utilisation d'appareils mobiles personnels; 93% des entreprises pratiquent une consolidation de la sécurité

Sophia Antipolis, 27 Juin 2011 — Fortinet® (NASDAQ: FTNT) - l'un des principaux acteurs du marché de la sécurité réseau et le leader mondial des systèmes unifiés de sécurité UTM (Unified Threat Management) – dévoile aujourd'hui les résultats d'une enquête européenne de grande envergure sur les stratégies de sécurité informatique de plus de 300 moyennes à très grandes entreprises. L'enquête, commanditée par Fortinet, a interrogé des décideurs informatiques d'entreprises situées en France, en Allemagne, en Italie, en Espagne, au Benelux et au Royaume-Uni, au sujet de leurs approches en matière de stratégie de sécurité face à l'évolution constante de l'utilisation de l'IT dans les entreprises.

Une Couverture Plus Etendue à Moindre Coût: Les Pré-requis de la Stratégie de Sécurité de Demain

Une couverture plus complète incluant davantage d'actifs de l'entreprise au-delà du périmètre du cœur du réseau, comme les terminaux mobiles, process, etc., et une meilleure rentabilité ont été classées comme les deux principales améliorations nécessaires pour parfaire la stratégie de sécurité de demain. Parmi les plus importants facteurs poussant

à un changement stratégique de sécurité, on trouve les 'traditionnelles' préoccupations de lutte contre la sophistication croissante des menaces et des attaques (25% l'ont nommé comme étant le levier le plus important) et de respect des règles de conformité (16%). Cependant, les décideurs informatiques se sentent tout autant contraints de s'adapter à un ensemble de tendances IT dont le cloud computing

	Europe	France
Le principal facteur pour changer de stratégie		
Sophistication des attaques et des menaces	25%	20%
Règles de conformité	16%	14%
Mobilité	16%	18%
Consumérisation de l'IT	9%	8%
Virtualisation	13%	16%
Cloud computing	19%	24%

(19%), la mobilité (16%) et la virtualisation (13%), tous trois nommés par les sondés comme principaux facteurs d'influence pour réévaluer leur stratégie de sécurité informatique.

De Nombreuses Stratégies A Bout de Course

Un sixième des entreprises interrogées (16% des entreprises européennes ; contre 24% des entreprises françaises) n'ont soit aucune stratégie de sécurité IT, ou ne l'ont pas réexaminé depuis plus de trois ans. Seulement 60% des entreprises ont effectué une réévaluation complète de leur stratégie de sécurité informatique au cours des 12 derniers mois.

“Compte tenu de l'adoption rapide du cloud et de l'augmentation des tablettes PC et smartphones en entreprise, il est essentiel pour les organisations de revoir régulièrement leur stratégie de sécurité IT et, en ce sens, celles qui ne l'ont pas fait depuis un an et plus, s'exposent à des risques plus importants” déclare Patrice Perche, Vice-Président Senior des Ventes Internationales et du Support chez Fortinet. *“Par exemple, face à la tendance grandissante de consomérisation de l'IT, dans laquelle les utilisateurs ont plus de pouvoir dans le choix des pratiques informatiques et des technologies qu'ils préfèrent utiliser au sein de l'organisation, il n'est pas surprenant de constater que 60% des sondés sont préoccupés par la capacité de leur organisation à sécuriser les données de l'entreprise dans ce nouvel environnement dynamique, influence par les utilisateurs.”*

La Plupart des Stratégies de Sécurité Protège les Mobiles, Mais Pas les Appareils Personnels

88% de l'ensemble de l'échantillon ont indiqué que leur stratégie de sécurité IT inclut une stratégie de sécurité mobile dédiée contre 82% des sondés français. Cependant, 66% des entreprises autorisent seulement l'utilisation du parc

	Europe	France
Chaque utilisateur est tenu responsable de la sécurité de son appareil mobile	21%	26%
L'utilisation du parc d'appareils mobiles de l'entreprise est uniquement autorisée avec une politique de sécurité en place	40%	38%
Chaque utilisateur est tenu responsable et l'utilisation du parc d'appareils mobile de l'entreprise est uniquement autorisée	26%	18%
Aucune stratégie de sécurité mobile en place	11%	16%

d'appareils mobiles de l'entreprise pour lesquels une politique de sécurité peut être directement appliquée. 21% des entreprises indiquent que les utilisateurs d'appareils mobiles personnels sont tenus responsables de la sécurité de l'appareil en question.

Réseaux Sans Fil: La Plus Grande Vulnérabilité

Interrogés sur quelles parties de leur infrastructure IT étaient vulnérables d'un point de vue sécurité, les réseaux sans fil ont été l'élément le plus identifié (cité par 57% de l'échantillon) par les sondés. Non seulement mis en évidence par la plupart des entreprises, les réseaux sans fil sont également classés en tête des vulnérabilités, devant l'infrastructure de cœur du réseau (classé 2^{ème}) et les bases de données (3^{ème}).

Pour la France, ce classement est un peu différent puisque le stockage des données est classé en tête des vulnérabilités devant les réseaux sans fil (2^{ème}) et l'infrastructure de cœur du réseau (3^{ème}).

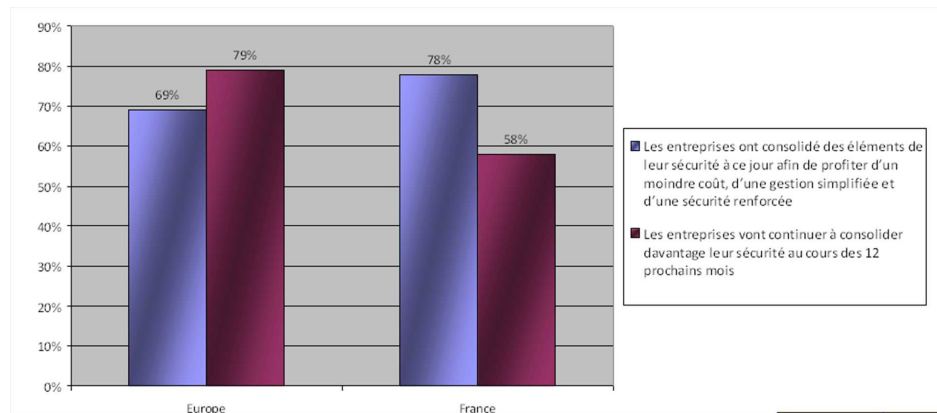
La Fin des Pare-feux Traditionnels

Avec l'identification et le contrôle des applications comme éléments sous-jacents des pare-feux de 'nouvelle génération' et de la mort des pare-feux traditionnels, aujourd'hui 50% de l'échantillon utilisent actuellement, ou prévoient de déployer, un pare-feu doté de fonctionnalités de contrôle d'applications. Les pare-feux applicatifs web et XML dédiés ont également été adoptés en nombre, avec 43% de l'échantillon global qui utilisent actuellement, ou envisagent d'utiliser, cette technologie pour sécuriser les applications web.

- Le Royaume-Uni montre le plus fort taux d'adoption de pare-feux de 'nouvelle génération' avec 60% de l'échantillon utilisant cette technologie
- L'Allemagne et l'Italie sont les pays dans lesquels les pare-feux applicatifs web /XML sont les plus adoptés, avec chacun 54% de leur échantillon

Consolidation de la Sécurité Réseau - Encore Un Travail en Cours?

69% des sondés européens ont consolidé des éléments de leur sécurité à ce jour afin de profiter d'un moindre coût, d'une gestion simplifiée et d'une sécurité renforcée contre 78% des sondés français. 79% de l'ensemble de l'échantillon déclarent qu'ils vont continuer à consolider davantage leur sécurité au cours des 12 prochains mois contre 58% des français.



24% des organisations interrogées prévoient d'entreprendre un projet de consolidation de sécurité réseau pour la première fois dans les 12 prochains mois. Seulement 7% de l'échantillon global n'ont pas l'intention d'entreprendre dans un avenir proche un quelconque projet de consolidation de sécurité réseau.

- L'Italie est le pays dans lequel il y a encore beaucoup à faire en matière d'adoption de la consolidation de sécurité réseau, avec 60% de l'échantillon global indiquant que ceci est toujours en projet (la moyenne européenne est de 55%),
- Au Benelux, 24% de l'échantillon ont le sentiment d'avoir atteint le niveau de consolidation de sécurité réseau recherché (moyenne européenne = 14%),

- Les organisations françaises de l'échantillon sont les plus susceptibles de débiter une consolidation de sécurité réseau (34%) pour la première fois. Au Benelux, le chiffre est seulement de 16%,
- Les italiens et les espagnols sont les plus opposés à toute suggestion de consolidation de sécurité réseau (10%); près de trois fois plus que les allemands et les britanniques (4% chacun).

“Les départements IT et les professionnels de sécurité informatique font face à des défis venant de toutes parts, alors qu'ils se battent pour maintenir une stratégie de sécurité cohérente qui protège à la fois les données et répond aux besoins changeants des utilisateurs et de l'entreprise au sens large,” ajoute Patrice Perche. *“Les organisations qui demandent une approche technologique commune au travers d'une gamme de solutions de sécurité bout-en-bout sont les mieux positionnées pour faire face à ces défis sans pour autant compliquer les process de gestion, compromettre les performances, ou encore ajouter des coûts supplémentaires inutiles.”*

###

Note aux rédactions

L'Etude européenne de Fortinet sur la Stratégie de Sécurité est un exercice de recherches entrepris en Mai-Juin 2011 au nom de Fortinet par Vision Critical, entreprise d'étude de marché indépendante. L'enquête a impliqué 305 décisionnaires IT en charge de la stratégie de sécurité informatique dans des entreprises de 250-999 employés (38% de l'échantillon), 1000-2999 employés (21% de l'échantillon) et plus de 3000 employés (41% de l'échantillon).

A propos de Fortinet (www.fortinet.com)

Fortinet (code NASDAQ : FTNT) est un des principaux fournisseurs de solutions de sécurité réseau et le leader du marché des systèmes unifiés de sécurité *UnifiedThreat 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 2009 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.

###

Copyright © 2011 Fortinet, Inc. Tous droits réservés. Les symboles ® et ™ indiquent respectivement les marques déposées et non enregistrées de Fortinet, Inc., et de ses filiales et partenaires. Les marques Fortinet incluent mais ne sont pas limitées : Fortinet, FortiGate, FortiGuard, FortiManager, FortiMail, FortiClient, FortiCare, FortiAnalyzer, FortiReporter, FortiOS, FortiASIC, FortiWiFi, FortiSwitch, FortiVoIP, FortiBIOS, FortiLog, FortiResponse, FortiCarrier, FortiScan, FortiDB and FortiWeb. L'ensemble des marques commerciales citées dans le présent communiqué sont la propriété de leurs détenteurs respectifs. Fortinet n'a pas vérifié de façon indépendante les déclarations ou les certificats ci-dessus attribués à des tiers et Fortinet n'a pas approuvé de telles déclarations.