Les cyberattaques coÃ»tent 2,4 millions dâ□□euros Ã chaque PME franÃ§aise en 2009
Info
PostÃ© par : JulieM
PubliÃ©e le : 24/2/2010 0:00:00

Selon la nouvelle Ã©tude Symantec Â« **2010 State of Enterprise Security** Â», la sÃ©curitÃ© est la **premiÃ¨re prÃ©occupation des services informatiques**, Symantec Corp. publie aujourdâ□□hui les rÃ©sultats de son Ã©tude mondiale 2010 State of Enterprise Security (Ã©tat de la sÃ©curitÃ© dans les entreprises).

Cette Ã©tude, rÃ©vÃ¨le que **42 %** des entreprises du monde entier placent la sÃ©curitÃ© au coeur de leurs prÃ©occupations. Ce n'est pas une surprise, lorsque l'on sait que **75 %** des grandes entreprises ont Ã©tÃ© victimes de cyber attaques au cours des 12 derniers mois. Ces attaques leur coÃ»tent en moyenne 2 millions de dollars par an.

Selon cette Ã©tude, les entreprises en France nâ□□ont pas fait partie de Â« **lâ□□exception culturelle** Â» habituelle en termes de cyber attaques par rapport Ã la moyenne mondiale ; **73%** des entreprises dans lâ□□Hexagone ont Ã©tÃ© victimes de ce type dâ□□attaques en 2009. Enfin, les grandes entreprises ont signalÃ© qu'il Ã©tait de plus en plus difficile d'assurer leur sÃ©curitÃ© en raison du manque d'effectifs, de nouvelles initiatives informatiques qui exacerbent les problÃ¨mes de sÃ©curitÃ© et de la compliance.

Cette Ã©tude repose sur un sondage rÃ©alisÃ© dans 27 pays, dont la France, en janvier 2010 auprÃ¨s de 2 100 CIO, responsables de la sÃ©curitÃ© et directeurs informatiques.

Â« *La protection de l'information est aujourd'hui plus difficile quâ□□auparavant.* Â», explique **Francis deSouza**, viceprÃ©sident du groupe Enterprise Security de Symantec. Â« *La mise en place d'un modÃ¨le de sÃ©curitÃ© permet de protÃ©ger l'infrastructure et les donnÃ©es, d'appliquer les rÃ¨gles informatiques et de gÃ©rer les systÃ¨mes plus efficacement. Les entreprises pourront assurer ainsi leur compÃ©titivitÃ© dans le monde dÃ©pendant de l'information d'aujourd'hui.* Â»

Points forts de l'Ã©tude :

Â· La sÃ©curitÃ© informatique est l'une des grandes prÃ©occupations des entreprises du

monde entier : 84% des personnes interrogÃ©es la considÃ¨re comme impÃ©rative/trÃ¨s importante. 42 % des entreprises placent la cybersÃ©curitÃ© au coeur de leurs prÃ©occupations, devant les catastrophes naturelles, le terrorisme et la criminalitÃ© ordinaire. En consÃ©quence, les services informatiques accordent une attention particuliÃ¨re Ã la sÃ©curitÃ© de l'entreprise. En France, les entreprises affectent 100 personnes en moyenne Ã la sÃ©curitÃ© et Ã la compliance, et indiquent que Â« la prÃ©vention de pertes des donnÃ©es Â» (ou DLP) a Ã©tÃ© le problÃ©matique informatique le plus impactÃ© en raison dâ□□un manque dâ□□effectifs dÃ©diÃ©s.. La quasi-totalitÃ© des entreprises consultÃ©es en France (95 %) prÃ©voyait pour 2010 des changements en matiÃ¨re de sÃ©curitÃ©.

Â· Les entreprises franÃ§aises sont frÃ©quemment victimes d'attaques. Au cours des 12 derniers mois, 73 % ont Ã©tÃ© victimes de cyber attaques, 40 % les ayant considÃ©rÃ©es comme assez/trÃ¨s nuisibles. Pire, 29 %

des entreprises dans le monde entier ont signalÃ© une hausse de la frÃ©quence des attaques au cours des 12 derniers mois.

Â· Toutes les entreprises (100 %) ont subi des pertes en ligne en 2009. Les trois premiÃ¨res formes de perte Ã©taient le vol de propriÃ©tÃ© intellectuelle, le vol de coordonnÃ©es des cartes de crÃ©dit de clients ou

d'autres donnÃ©es financiÃ¨res, ainsi que le vol d'informations permettant d'identifier les clients. Dans 92 % des cas, ces pertes se sont traduites par un prÃ©judice financier. Les trois premiers prÃ©judices Ã©taient la perte de productivitÃ©, le manque Ã gagner et la perte de confiance des clients. Les grandes entreprises dÃ©pense plus de 2 million de dollars pour se protÃ©ger contrer les cyber attaques.

La sÃ©curitÃ© de l'entreprise est de plus en plus difficile Ã assurer pour un certain nombre de raisons : la premiÃ¨re est le manque d'effectifs, les secteurs les plus touchÃ©s Ã©tant la sÃ©curitÃ© des rÃ©seaux (44 %), la sÃ©curitÃ© des terminaux (44 %) et la sÃ©curitÃ© de la messagerie (39 %) ; la deuxiÃ¨me rÃ©side dans le fait que les entreprises lancent de nouvelles initiatives qui rendent la sÃ©curitÃ© plus difficile Ã assurer. Les initiatives considÃ©rÃ©es par les services informatiques comme les plus problÃ©matiques du point de vue de la sÃ©curitÃ© sont les infrastructures en tant que services, les plates-formes en tant que services, la virtualisation des serveurs, la virtualisation des terminaux et les logiciels en tant que services (SaaS) ; enfin, la compliance constitue Ã©galement un enjeu considÃ©rable. Une entreprise type examine 19 normes ou cadres normatifs informatiques distincts et en applique actuellement huit.

Ces normes sont les suivantes : ISO, HIPAA, Sarbanes-Oxley, CIS, PCI et ITIL.

Â« La Banque Commerciale dâ□□Abu Dhabi est lâ□□exemple mÃªme de lâ□□entreprise qui a mis en place une stratÃ©gie de sÃ©curitÃ© efficace en mettant lâ□□accent sur le traitement proactif des problÃ¨mes, Â» ajoute Francis deSouza. Â« Pour un coÃ»t annuel fixe, lâ□□entreprise dispose dâ□□une sÃ©rie de solutions, de produits et de services lui fournissant une protection 24 heures sur 24, la surveillance et la gestion des menaces. Cette approche est bien plus rentable et productive que la sÃ©curisation dâ□□un rÃ©seau aprÃ¨s incident. Â»

Recommandations

Â· Les entreprises doivent renforcer la sÃ©curitÃ© de leur infrastructure en sÃ©curisant les terminaux, en protÃ©geant la messagerie et les accÃ¨s Internet, et en implÃ©mentant la sauvegarde et la restauration des donnÃ©es. Afin de dÃ©tecter et de gÃ©rer rapidement les menaces, les entreprises ont Ã©galement besoin de visibilitÃ©, dâ□□informations et de solutions de sÃ©curitÃ©.

Â· Les administrateurs de parc informatique doivent protÃ©ger les donnÃ©es proactivement en adoptant une approche centrÃ©e sur l'information, afin de protÃ©ger Ã la fois les donnÃ©es et les interactions. Une approche orientÃ©e contenu de la protection de l'information est dÃ©cisive pour savoir oÃ¹ se trouvent les informations sensibles, qui y a accÃ¨s et comment elles entrent dans l'entreprise ou en sortent.

Â· Les entreprises doivent mettre en place des rÃ¨gles informatiques, les appliquer, et automatiser leurs processus de compliance. En attribuant la prioritÃ© aux risques et en dÃ©finissant des rÃ¨gles couvrant l'ensemble des sites, les clients peuvent appliquer celles-ci par une automatisation et des flux de travail intÃ©grÃ©s. Ils peuvent ainsi non seulement identifier les menaces, mais remÃ©dier aux incidents lorsqu'ils se produisent, voire les anticiper.

Â· Les entreprises doivent gÃ©rer leurs systÃ¨mes en mettant en oeuvre des environnements d'exploitation sÃ©curisÃ©s, en distribuant et en appliquant les correctifs selon leur niveau, en automatisant les processus pour rationnaliser le rendement, et en assurant le suivi et le reporting de l'Ã©tat du systÃ¨me.

Cliquer pour **Tweeter: @Symantec** Selon une Ã©tude de Symantec, les cyber attaques coÃ»tent $2 millions par an aux grandes entreprises.