Imation prÃ©dit l'avenir de la sÃ©curitÃ© mobile pour 2012
Internet
PostÃ© par : JulieM
PubliÃ©e le : 23/1/2012 11:00:00

L'essor du tÃ©lÃ©travail n'est pas sans consÃ©quence pour les entreprises : en dehors des dÃ©fis liÃ©s Ã l'organisation des ressources humaines et Ã la mise en place de solutions techniques adaptÃ©es, elles doivent faire face Ã **des risques accrus en matiÃ¨re de sÃ©curitÃ© informatique**, portÃ©s par l'augmentation des volumes de transfert de donnÃ©e. Ainsi, 2012 pourrait bien devenir l'annÃ©e de tous les dangers.

Â« *Nous pouvons affirmer avec certitude que les pertes de donnÃ©es ne vont pas disparaÃ®tre de si tÃ´t. En 2012, le recourt croissant Ã un personnel nomade et les risques grandissants liÃ©s aux points d'accÃ¨s vont exposer les entreprises Ã de nouveaux risques, particuliÃ¨rement si elles ne s'engagent pas fermement Ã mieux protÃ©ger leurs donnÃ©es. Les DSI doivent Ã©galement se souvenir que la conformitÃ© ne constitue qu'une exigence minimale, un stade qu'il est nÃ©cessaire de dÃ©passer s'ils souhaitent garantir la sÃ©curitÃ© de leurs donnÃ©es en 2012.* Â» commente **Lawrence Reusing**, directeur gÃ©nÃ©ral sÃ©curitÃ© mobile Imation.

Ã la lumiÃ¨re de ces Ã©volutions, Imation prÃ©sente ses prÃ©visions 2012 pour la sÃ©curitÃ© mobile :

1. Le nombre des atteintes Ã la sÃ©curitÃ© des donnÃ©es va continuer Ã croÃ®tre en 2012, suite Ã des erreurs humaines ou des attaques malveillantes. Dans un rapport pour 2012, le Ponemon Institute note que les risques au niveau des points d'accÃ¨s augmentent en raison de l'adoption du Cloud Computing et des supports amovibles, deux tendances figurant parmi les principales menaces identifiÃ©es pour 2012.

2. La conformitÃ© va continuer Ã imposer la protection des donnÃ©es, l'Union EuropÃ©enne envisage ainsi d'infliger aux entreprises une amende pouvant atteindre 5 % de leur chiffre d'affaires mondial pour sanctionner les atteintes Ã la sÃ©curitÃ© les plus graves. Les nouvelles rÃ©glementations vont aussi s'appliquer aux filiales europÃ©ennes des multinationales, pour garantir que ces derniÃ¨res ne puissent Ã©chapper aux sanctions. Ces rÃ©glementations ne vont pas entrer en vigueur cette annÃ©e, mais elles tÃ©moignent de la ferme intention de l'UE de lutter contre les entreprises qui prennent des mesures insuffisantes pour protÃ©ger les donnÃ©es.

3. Les services financiers vont observer une augmentation de la fraude, des attaques et des menaces Internet avec une sophistication croissante, les cybercriminels dissÃ©minant plus de programmes malveillants et de chevaux de Troie, comme dans le cas des attaques ZeuS en 2011.

L'essor des groupes de hacking organisÃ©s comme Anonymous qui visent les organismes financiers tels que Visa et PayPal renforce le risque pour les cibles potentielles.

4. Collaboration accrue et plus grande sensibilisation Ã la responsabilitÃ© commune en termes de sÃ©curitÃ© des donnÃ©es alors que les Ã tats, les entreprises et les individus acceptent dans leur ensemble leur responsabilitÃ© individuelle. Le constat que la sÃ©curitÃ© des donnÃ©es doit se faire dans le cadre d'une dÃ©marche collaborative et convergente va gagner du terrain.

5. Une stratÃ©gie plus proactive va s'imposer alors que les entreprises consacrent plus de ressources Ã la prÃ©vention pour anticiper les menaces. La sensibilisation et l'attention autour des stratÃ©gies de reprise d'activitÃ© vont se renforcer. La gravitÃ© des menaces modernes, les sanctions possibles des autoritÃ©s rÃ©glementaires et l'impact majeur des attaques sur les marques (cas de la Sony PlayStation 3 en 2011) expliquent ces tendances.

6. Les effets des programmes malveillants vont continuer Ã s'intensifier avec le tÃ©lÃ©travail car un nombre grandissant d'employÃ©s doivent faire sortir des donnÃ©es de l'entreprise. Le personnel nomade Ã©tant amenÃ© Ã croitre, un volume croissant de donnÃ©es va Ãªtre transmis en ligne ou transportÃ© physiquement, d'oÃ¹ une menace accrue de perte ou d'atteinte Ã la sÃ©curitÃ©. L'emploi de dispositifs cryptÃ©s Ã protection antivirus devrait se rÃ©pandre en rÃ©ponse aux menaces grandissantes que prÃ©sente cette Ã©volution des modes de travail.

7. L'utilisation du matÃ©riel personnel (BYOD, ou Bring Your Own Device) va se gÃ©nÃ©raliser sur le lieu de travail, engendrant de possibles problÃ¨mes de compatibilitÃ© pour le service informatique et renforÃ§ant le besoin d'outils de suivi et d'indicateurs d'utilisation. Des informations sur les types de dispositifs utilisÃ©s, ainsi que les modalitÃ©s d'accÃ¨s Ã certaines donnÃ©es, seront essentielles Ã des fins d'audit. La capacitÃ© de produire rapidement des rapports prÃ©cis et d'enregistrer des informations dÃ©taillÃ©es sur les donnÃ©es que les employÃ©s envoient ou reÃ§oivent va jouer un rÃ´le clÃ© pour effectuer cet audit et prouver la conformitÃ©.

8. La consumÃ©risation de l'informatique va se poursuivre dans l'entreprise. La formation du personnel sera cruciale pour lutter contre ces problÃ¨mes, et les entreprises devront investir davantage pour s'assurer que les employÃ©s reÃ§oivent des conseils pratiques sur leurs responsabilitÃ©s en matiÃ¨re de sÃ©curitÃ© des donnÃ©es. Elles devront Ã©galement veiller Ã maintenir Ã jour leurs politiques internes de sÃ©curitÃ© et Ã intÃ©grer Ã ces derniÃ¨res l'Ã©volution des technologies et des modes de travail.