Les services financiers, plus touchÃ©s par des fraudes en ligne

Internet

PostÃ© par : JerryG
PubliÃ©e le : 24/6/2015 15:00:00

Les dÃ©cideurs IT de dix pays mettent en Ã©vidence les pertes financiÃ¨res et les prÃ©occupations rÃ©glementaires liÃ©es Ã aux logiciels malveillants, au phishing, aux vols dâ□□identifiants et aux piratages de profils dâ□□employÃ©s.
Les organismes de services financiers de la zone EMEA sont de plus en plus exposÃ©s et prÃ©occupÃ©s par lâ□□augmentation des menaces de fraude en ligne, selon une enquÃªte commandÃ©e par F5 Networks.

Les dÃ©cideurs informatiques rÃ©vÃ¨lent quâ□□ils doivent constamment faire face Ã des attaques significatives ciblant les finances et la rÃ©putation de leur entreprise dues Ã des programmes malveillants, des campagnes de phishing, des attaques visant Ã sâ□□accaparer des identifiants utilisateurs ou dÃ©tourner leurs sessions. Cela a pour consÃ©quence de gÃ©nÃ©rer un besoin croissant pour des solutions multi-couches de protection et de dÃ©tection des fraudes en ligne et sur mobiles.

L'enquÃªte a rÃ©vÃ©lÃ© que 48 % des organisations ont, au cours des deux derniÃ¨res annÃ©es, dÃ©jÃ subi des pertes financiÃ¨res allant de 70 000 â□¬ Ã 700 000 â□¬ et ayant pour origine des fraudes en ligne. 9 % de ces actes de malveillance ont permis de dÃ©rober des sommes supÃ©rieures Ã 700 000 â□¬ et 3 % supÃ©rieures Ã 1 000 000 â□¬.

73 % ont citÃ© les atteintes Ã la rÃ©putation comme Ã©tant la principale prÃ©occupation liÃ©e Ã ces attaques, alors que 72 % craignent la perte de revenus et le fardeau de devoir effectuer des audits de sÃ©curitÃ© complets. Parmi les autres impacts nÃ©gatifs majeurs figurent la perte de la confiance et la fidÃ©litÃ© des clients (64 %) et les amendes potentielles par les organismes de rÃ©glementation (62 %).

Â« Que ce soit des attaques de type phishing, Man-in-the-middle, Man-In-The-Browser ou d'autres activitÃ©s basÃ©es Trojan comme des injections Web, des dÃ©tournements de formulaire en ligne, des modifications de pages ou des modifications de transactions, les dangers de la fraude en ligne sont inÃ©vitables et vaste pour les entreprises quel que soit leur secteur Â», dÃ©clare Gad Elkin, Directeur EMEA de la sÃ©curitÃ© de F5.

Â« Plus que jamais, il est essentiel de comprendre la nature des menaces et de mettre en Å□uvre des solutions qui Ã©liminent les attaques avant qu'elles ne puissent vraiment nuire. Ceux qui feront cela correctement seront rÃ©compensÃ©s par la fidÃ©litÃ© de leurs clients et en retireront les bÃ©nÃ©fices. Â»

Plus de 35% des rÃ©pondants ont affirmÃ© avoir subi des pertes liÃ©es Ã des fraudes ayant pour origine une large variÃ©tÃ© d'attaques en ligne. Les programmes malveillants ont Ã©tÃ© le principal coupable (75 %), suivie par le phishing (53 %), le piratage dâ□□identifiants (53 %) et le piratage de session (35 %).

Lorsque les stratÃ©gies de dÃ©fense ont Ã©tÃ© abordÃ©es, 37% des entreprises interrogÃ©es ont dÃ©clarÃ© qu'elles prÃ©fÃ©raient la dÃ©fense Ã fraude en ligne faisant appel Ã des solutions hybrides combinant des prestations et sur site ou en ligne. Le chiffre est plus Ã©levÃ© (59 % des rÃ©pondants) pour les organisations de plus de 5.000 employÃ©s.

55 % des rÃ©pondants affirment avoir adoptÃ© des solutions de prÃ©vention contre la fraude multi-couches. Les solutions embarquÃ©es sur les terminaux sont les plus populaires (62 %), suivie par l'analyse de navigation de page pour identifier les schÃ©mas de navigation suspects (59 %), et

lâ□□analyse des liens de relations entre les utilisateurs, les comptes et les terminaux pour dÃ©tecter les activitÃ©s criminelle et/ou les abus (59 Â»%). Les solutions fournissant une analyse comportementale de l'utilisateur et de comparaison pour des canaux spÃ©cifiques figurent Ã©galement en bonne place (55 %).

Ce contexte explique les raisons pour lesquelles il y a une demande croissante pour des solutions en ligne bÃ©nÃ©ficiant de capacitÃ©s de protection contre la fraude sans nÃ©cessitÃ© dâ□□installer quoi que ce soit sur le poste. Ceux-ci permettent aux organisations dâ□□Ã©quiper en temps rÃ©el tous les types de postes contre toutes les variÃ©tÃ©s de menaces en ligne sans que l'utilisateur ait Ã faire quoi que ce soit, Ã©cartant tout danger dans des situations telles que des injections de code HTML ou de script malveillants.

Cela inclut les menaces les plus rÃ©centes telles comme le malware Dyre, qui dispose d'un large Ã©ventail de capacitÃ©s qui en font l'un des chevaux de Troie bancaires les plus dangereux actuellement. Â« Les fraudeurs continuent d'Ã©voluer et d'exploiter le maillon le plus faible : l'utilisateur final Â», conclut Gad Elkin.

Â« Les organisations sont avancÃ©es dans leur approche visant Ã protÃ©ger les centres de donnÃ©es, mettre en Å□uvre l'authentification multi-facteurs et la protection des applications via des contrÃ´les cÃ´tÃ© serveur. NÃ©anmoins, beaucoup ont Ã©chouÃ© Ã sÃ©curiser efficacement les terminaux sur lesquels les utilisateurs interagissent directement avec les applications web. Â»