Verizon : Etat des lieux de la cybercriminalitÃ© par secteur
Info
PostÃ© par : JPilo
PubliÃ©e le : 25/10/2012 11:00:00

Outre les menaces qui pÃ¨sent sur les acteurs des secteurs de la vente au dÃ©tail, de lâ□□hÃ´tellerie, de la finance et de la santÃ©, Verizon consacre tout un dossier au vol de propriÃ©tÃ© intellectuelle.

Verizon publie le 24 octobre 2012 une sÃ©rie dâ□□Ã©tats des lieux de la cybercriminalitÃ©, secteur par secteur, sur la base de ses rapports Â« **Verizon 2012 and 2011 Data Breach Investigations Reports** Â».

Les acteurs de la vente au dÃ©tail, de lâ□□hÃ´tellerie, de la finance et de la santÃ© y trouveront lâ□□essentiel pour comprendre les rouages des compromissions de donnÃ©es dont ils sont la cible et mieux sâ□□en prÃ©munir.

Verizon consacre Ã©galement tout un volet au vol dâ□□Ã©lÃ©ments de propriÃ©tÃ© intellectuelle, contre lequel il est de plus en plus difficile de se protÃ©ger dans bon nombre de secteurs.

Â« *Pour pouvoir prÃ©venir les compromissions de donnÃ©es, il est indispensable de comprendre en quoi elles consistent* Â», explique Wade Baker, responsable de lâ□□Ã©quipe RISK de Verizon. Â« *Câ□□est ce que tente dâ□□expliciter cette Ã©tude ciblÃ©e qui, nous lâ□□espÃ©rons, rÃ©pondra aux questions soulevÃ©es par des entreprises du monde entier qui souhaitent protÃ©ger non seulement leurs donnÃ©es mais aussi leur image de marque*. Â»

Principales analyses par secteur dâ□□activitÃ©. Voici les nouvelles constatations publiÃ©es :

Finance et assurances

â□¢ Le secteur des services financiers est confrontÃ© Ã des dÃ©fis de protection de

lâ□□information bien spÃ©cifiques. Cible de choix, il attise la convoitise des cybercriminels les plus audacieux et tenaces.

â□¢ GÃ©nÃ©ralement motivÃ©s par lâ□□appÃ¢t du gain , les attaquants procÃ¨dent de maniÃ¨re directe (accÃ¨s Ã des comptes et applications internes) ou indirecte (fraude en aval), exploitant principalement les DAB, applications Web et salariÃ©s.

â□¢ Plusieurs mesures dâ□□amÃ©lioration de la sÃ©curitÃ© sont envisageables , notamment le renforcement de la protection des DAB et de la gestion des droits dâ□□accÃ¨s, le dÃ©veloppement dâ□□applications sÃ©curisÃ©es et la formation et sensibilisation des salariÃ©s Ã ces problÃ©matiques.

SantÃ©

â□¢ Les petites et moyennes structures (de 1 Ã 100 salariÃ©s), pour lâ□□essentiel des Ã©tablissements de soins externes comme les cabinets mÃ©dicaux et dentaires, sont les premiÃ¨res victimes de la cybercriminalitÃ© dans le secteur de la santÃ©.

â□¢ Les attaques sont gÃ©nÃ©ralement le fait de bandes criminelles organisÃ©es dont lâ□□objectif est de dÃ©rober des donnÃ©es personnelles et bancaires aux petites entitÃ©s, moins risquÃ©es, pour accomplir diverses fraudes financiÃ¨res.

â□¢ Les assaillants procÃ¨dent le plus souvent par piratage de terminaux point de vente et exploitation de programmes malveillants. Equipements mÃ©dicaux et dossiers mÃ©dicaux Ã©lectroniques figurent Ã©galement parmi leurs cibles privilÃ©giÃ©es.

â□¢ La plupart des infractions pourraient Ãªtre Ã©vitÃ©es au moyen de mesures relativement simples Ã mettre en place, telles que la modification des mots de passe administrateur sur tous les terminaux point de vente, lâ□□installation dâ□□un pare-feu, lâ□□interdiction de naviguer sur le Web via les terminaux point de vente et la mise en conformitÃ© de ces terminaux Ã la norme PCI DSS (Payment Card Industry Data Security Standard).

Vente au dÃ©tail

â□¢ Le secteur de la vente demeure victime de nombreuses compromissions de donnÃ©es, perpÃ©trÃ©es pour la plupart par des bandes du crime organisÃ©, qui pÃ©nÃ¨trent dans le systÃ¨me des terminaux point de vente traitant les transactions commerciales quotidiennes dans lâ□□ambition de rÃ©aliser des profits. Pour ce faire, ils utilisent les codes dâ□□accÃ¨s par dÃ©faut, peu sÃ©curisÃ©s ou faciles Ã deviner et des services dâ□□accÃ¨s Ã distance de tiers.

â□¢ Les plus vulnÃ©rables sont les franchisÃ©s et autres PME, qui manquent souvent des ressources et de lâ□□expertise nÃ©cessaires en interne pour assurer leur sÃ©curitÃ©. Ces sociÃ©tÃ©s ont recours Ã des prestataires externes dont les mesures de protection se rÃ©vÃ¨lent souvent inadÃ©quates ou Ã des solutions prÃªtes Ã lâ□□emploi qui ne satisfont pas toujours pleinement leurs besoins.

â□¢ Les employÃ©s sont frÃ©quemment impliquÃ©s dans les infractions, dÃ©libÃ©rÃ©ment ou Ã leur insu. Il nâ□□est pas rare quâ□□un salariÃ© clique sur une piÃ¨ce-jointe infectÃ©e ou visite un site Web frauduleux depuis un ordinateur de lâ□□entreprise, propageant alors le programme malveillant au systÃ¨me et laissant Ã lâ□□attaquant le champ libre pour accÃ©der aux autres terminaux du rÃ©seau.

HÃ´tellerie et restauration

â□¢ Ce secteur dÃ©tient le triste record du plus grand nombre de compromissions de

donnÃ©es depuis 2 ans.

â¢ Les terminaux point de vente, qui traitent quotidiennement les paiements, sont des cibles faciles pour les bandes du crime organisÃ©.

â¢ Ce secteur, plus que tout autre, doit instaurer des mesures prÃ©ventives.

Vol dâÃ©lÃ©ments de propriÃ©tÃ© intellectuelle

â¢ De maniÃ¨re gÃ©nÃ©rale, la dÃ©tection et lâidentification des vols de propriÃ©tÃ© intellectuelle est une tÃ¢che extrÃªmement ardue, qui nÃ©cessite des compÃ©tences dâexpert. Bon nombre de ces compromissions sont ainsi percÃ©es Ã jour une fois les dÃ©gÃ¢ts constatÃ©s. En limiter lâimpact nÃ©cessite un travail de longue haleine. Les vols dâÃ©lÃ©ments de propriÃ©tÃ© intellectuelle sont souvent le fruit dâune connivence entre salariÃ©s et individus externes. Parmi les salariÃ©s complices, 2/3 sont des employÃ©s permanents. Les intervenants extÃ©rieurs agissent souvent de maniÃ¨re directe, dans lâintention de nuire, mais aussi rÃ©guliÃ¨rement sur sollicitation et avec le concours dâutilisateurs internes.

â¢ La plupart des vols sont commis par des concurrents dÃ©terminÃ©s qui voient en cette mÃ©thode un moyen rapide dâacquÃ©rir un avantage stratÃ©gique, financier ou technologique, notamment. Les attaquants associent gÃ©nÃ©ralement plusieurs mÃ©thodes jusquâÃ trouver la combinaison gagnante, souvent complexe et graduelle.

â¢ Il nâexiste aucune solution universelle pour se protÃ©ger efficacement contre ce risque. La meilleure des dÃ©fenses consiste Ã faire preuve de bon sens, en sâappuyant sur des donnÃ©es factuelles.

Verizon 2012 Data Breach Investigations Report

Lâédition de mars 2012 marque la 5Ã¨me annÃ©e de publication du rapport. Avec plus de 855 enquÃªtes et 174 millions de compromissions constatÃ©es, câest la 2Ã¨me annÃ©e avec autant de donnÃ©es perdues depuis que les Ã©quipes Verizon RISK (Research Investigations Solutions Knowledge) ont commencÃ© Ã recueillir des informations en 2004. Cette annÃ©e, 5 partenaires ont contribuÃ© au rapport par lâapport de donnÃ©es Ã Verizon : les services secrets amÃ©ricains, la Dutch National High Tech Crime Unit des Pays-Bas, la police fÃ©dÃ©rale australienne, le service irlandais Reporting & Information Security Service et la e-Crime Unit de la police centrale londonienne.

Lâédition 2012 est la premiÃ¨re Ã avoir Ã©tÃ© traduite de lâanglais au franÃ§ais, Ã lâitalien, au japonais, Ã lâallemand, au portugais et Ã lâespagnol. Elle est Ã©galement disponible au format iBook.

Au travers de sa filiale Terremark, Verizon propose aux entreprises du monde entier de protÃ©ger leur bien le plus prÃ©cieux : leurs donnÃ©es. Pour ce faire, elle leur propose toute un portefeuille de services de sÃ©curitÃ©, sur site et en Cloud : solutions de gouvernance, de gestion des risques et de mise en conformitÃ© ; solutions de gestion des identitÃ©s et des accÃ¨s ; service dâenquÃªtes (Forensics) ; services de protection des donnÃ©es ; services de gestion des menaces et des vulnÃ©rabilitÃ©s.

Pour plus dâinformation sur les services de sÃ©curitÃ© de Verizon