Verizon, les donnÃ©es des cartes de paiement toujours trÃ¨s menacÃ©es
Internet
PostÃ© par : JPilo
PubliÃ©e le : 29/9/2011 13:00:00

Un rapport de Verizon montre quâ□□un trÃ¨s grand nombre dâ□□entreprises Ã©prouvent des difficultÃ©s Ã se conformer aux normes de sÃ©curitÃ© de lâ□□industrie des cartes de paiement, exposant ainsi les informations confidentielles des consommateurs Ã de trÃ¨s forts risques.

La seconde Ã©dition du rapport **Verizon Payment Card Industry Compliance Report** rÃ©vÃ¨le en effet que la plupart des entreprises qui acceptent des cartes de paiement (crÃ©dit et/ou dÃ©bit) ont le plus grand mal Ã atteindre et Ã conserver la certification de la norme Payment Card Industry Data Security Standard (PCI DSS), augmentant leurs risques de perte dâ□□informations client confidentielles et de fraudes Ã la carte de crÃ©dit.

Les lourdes pÃ©nalitÃ©s quâ□□elles encourent, notamment des amendes et une hausse des frais de traitement transactionnel par les enseignes Ã©mettrices des cartes, semblent sans effet, tout comme les pressions exercÃ©es par leurs partenaires et clients, qui exigent quâ□□elles dÃ©montrent leur conformitÃ© permanente.

En plus de faire lâ□□Ã©tat des lieux de la conformitÃ© aux normes PCI DSS, le rapport examine le degrÃ© de conformitÃ© des entreprises Ã chacune des 12 exigences PCI et Ã©met des recommandations pour les aider Ã sâ□□y soumettre durablement.

Â« *Nous espÃ©rions que davantage dâ□□entreprises se conforment Ã la norme PCI, car câ□□est ainsi quâ□□elles renforceront leur sÃ©curitÃ© et que le nombre de failles de sÃ©curitÃ© diminuera* Â», explique **Wade Baker**, directeur de la gestion du risque chez Verizon. Â« *Nous souhaitons que ce rapport les aide Ã mieux cibler leurs efforts et Ã appliquer nos recommandations pour accÃ©lÃ©rer leur mise en conformitÃ© PCI. Notre ambition est de parvenir Ã un environnement de transactions par carte plus sÃ©curisÃ© pour les consommateurs comme pour les entreprises.* Â»

REMARQUE : des ressources supplÃ©mentaires illustrant ce rapport, parmi lesquelles un podcast audio et des tableaux et graphiques haute rÃ©solution, sont Ã©galement disponibles.

Conclusions du rapport PCI sur les Ã©valuations PCI et les compromissions de donnÃ©es constatÃ©es

Le rapport sâappuie sur lâanalyse de la centaine dâÃ©valuations PCI DSS effectuÃ©es par lâÃ©quipe des PCI Qualified Security Assessors de Verizon en 2010, ainsi que sur les donnÃ©es recueillies par les experts du groupe Investigative Response de Verizon au cours de leurs enquÃªtes sur les infractions constatÃ©es sur les donnÃ©es de cartes de paiement. LâÃ©quipe Verizon Risk Intelligence a par ailleurs recoupÃ© ces Ã©valuations avec celles des Ã©tudes de cas de compromissions de donnÃ©es bancaires de son rapport 2011 Verizon Data Breach Investigations Report.

Les Ã©valuations portent sur des donnÃ©es dâentreprises basÃ©es aux Etats-Unis, en Europe et en Asie, offrant ainsi le premier panorama mondial de la norme PCI.

Principales analyses

Voici les principales conclusions du rapport 2011 Verizon Payment Card Industry Compliance Report :

â¢ Le degrÃ© de conformitÃ© ne sâest ni aggravÃ© ni amÃ©liorÃ© ; il reste Â« dÃ©cevant Â». Seules 21 % des organisations Ã©taient totalement conformes au cours du premier audit. Parmi les motifs de cette non-conformitÃ© PCI gÃ©nÃ©ralisÃ©e, le rapport note lâexcÃ¨s de confiance, la baisse de vigilance et la nÃ©cessitÃ© de se concentrer sur dâautres problÃ©matiques de conformitÃ© et de sÃ©curitÃ©.

â¢ Le dÃ©faut de conformitÃ© PCI accroÃ®t les risques de compromissions de donnÃ©es. Le rapport de cette annÃ©e a de nouveau dÃ©montrÃ© que les entreprises non conformes aux normes PCI sont plus exposÃ©es aux risques de vol de donnÃ©es bancaires, de vol dâidentifiants et de fraude.

â¢ Les entreprises peinent tout particuliÃ¨rement Ã satisfaire les exigences PCI les plus importantes. Elles reconnaissent avoir surtout des difficultÃ©s avec les exigences nÂ°3 (protÃ©ger les donnÃ©es stockÃ©es concernant les titulaires de cartes de paiement), nÂ°10 (surveiller et contrÃ´ler les accÃ¨s), nÂ°11 (tester rÃ©guliÃ¨rement les systÃ¨mes et procÃ©dures de sÃ©curitÃ©) et nÂ°12 (faire appliquer les rÃ¨gles de sÃ©curitÃ©), qui visent toutes Ã protÃ©ger les donnÃ©es des porteurs de cartes de paiement.

â¢ Lâabsence de prioritÃ© accordÃ©e aux efforts de mise en conformitÃ© rÃ©vÃ¨le une sous-estimation des risques sÃ©curitaires. Lâapproche par prioritÃ© (Prioritized Approach) lancÃ©e en 2009 visait Ã aider les entreprises Ã identifier et rÃ©duire les risques liÃ©s aux donnÃ©es de cartes de paiement et Ã faciliter la mise en place des procÃ©dures annuelles imposÃ©es par la norme PCI. Le rapport indique toutefois que de nombreuses entreprises se sont contentÃ©es de suivre les recommandations de la norme PCI DSS, sans adosser de stratÃ©gie de gestion des risques Ã leur dÃ©marche de mise en conformitÃ©. Par consÃ©quent, beaucoup ignorent les menaces sÃ©curitaires prÃ©sentant les plus grands risques et impacts nÃ©gatifs.

â¢ La norme PCI protÃ¨ge contre les attaques les plus courantes. Les logiciels malveillants et le piratage constituent les deux types dâattaques les plus frÃ©quents sur les donnÃ©es des titulaires de cartes de paiement. De nombreuses dispositions de la norme PCI se recoupent pour prÃ©venir ces attaques.

Recommandations pour se mettre en conformitÃ©

A lâissue de ses recherches approfondies, Verizon prÃ©conise les recommandations suivantes

aux entreprises qui Ã©prouvent des difficultÃ©s Ã se conformer Ã la norme PCI :

â¢ GÃ©rer la mise en conformitÃ© au quotidien, en continu. Lâ□□adhÃ©sion Ã la norme PCI requiert en effet une attention de tous les instants. Cela passe par lâ□□examen quotidien des journaux dâ□□activitÃ©, la surveillance hebdomadaire de lâ□□intÃ©gritÃ© des fichiers, lâ□□analyse trimestrielle des vulnÃ©rabilitÃ©s et des tests de pÃ©nÃ©tration annuels. Verizon recommande que ces activitÃ©s soient confiÃ©es Ã un responsable PCI en interne, qui veille Ã la mise en conformitÃ© quotidienne de lâ□□entreprise.

â¢ Ne pas sâ□□auto-Ã©valuer, ou alors avec la plus grande prÃ©caution . Les commerÃ§ants de niveaux 1 et 2 (ceux qui traitent les plus gros volumes de transactions par carte) sont autorisÃ©s Ã auto-Ã©valuer leur degrÃ© de conformitÃ© Ã la norme PCI. Toutefois, au vu des nombreux conflits dâ□□intÃ©rÃªt potentiels, Verizon leur recommande vivement de confier Ã un tiers impartial lâ□□Ã©valuation ou la validation des rÃ©sultats dâ□□Ã©valuation.

â¢ Se prÃ©parer Ã satisfaire des exigences plus strictes. En octobre 2010, le PCI Security Standards Council annonÃ§ait la norme PCI DSS 2.0, une version plus stricte imposant la validation de la mÃ©thodologie de dÃ©finition du champ dâ□□application. Les entreprises, dont la plupart peinent dÃ©jÃ Ã se conformer Ã la norme actuelle, vont donc devoir se prÃ©parer rapidement Ã adhÃ©rer Ã cette nouvelle version.