Commerçants: que faire pour atteindre la conformité PCI?

Guide rapide PCI-DSS

BlueTower - Le 15 mai 2014

Vous venez de recevoir une notification de votre banque acquéreur vous demandant que votre entreprise présente dans les meilleurs délais votre attestation de conformité PCI-DSS. Dans le cas où vous ne pourriez pas répondre à cette demande, vous savez qu'il y a des risques de pénalités ou plus probablement des frais supplémentaires à verser. Mais, plus grave, il y a un risque de résiliation de votre contrat d'acceptation ou d'autres formes de répercussions si cette validation n'est pas fournie à une certaine date à votre acquéreur.

Une recherche rapide sur le Web montre des pages écrites dans un jargon déroutant, des informations apparemment contradictoires et une absence d'orientation claire. Que devez vous faire maintenant?

Dans ce document, nous allons nous concentrer sur les actions initiales à réaliser dés que vous recevez cette notification afin de vous simplifier tout le processus de génération de votre attestation de conformité.

Sachez que cette attestation de conformité est déclarative et que vous allez devoir répondre à un questionnaire (SAQ) qui va vous permettre de savoir si vous êtes conforme ou pas vis à vis des exigences que présente PCI-DSS. Si vous n'êtes pas en conformité avec des dispositions requises vous aurez à indiquez pour chacune d'elles quand et comment vous le serez.

PREMIERE ETAPE: déterminer votre niveau tel que défini par le réseau de cartes .

Pourquoi est-il important de comprendre dans quel niveau vous êtes ? Chaque niveau est défini suivant le nombre de transactions annuel, ce qui est un critère simple d'évaluation du risque. Mais chaque réseau a son propre programme de conformité basé sur le nombre de transactions pour leurs cartes seulement. Pour rendre les choses plus confuses, les réseaux de cartes diffèrent dans leurs définitions de niveau et les exigences que doit remplir la validation de la conformité.

Par exemple, selon les critères de Visa le Niveau 4 regroupe les commerçants qui ont jusqu'à 1 million de transactions Visa par an et pour MasterCard les organisations qui ont jusqu'à 1 million de transactions MasterCard chaque année sont dans le niveau 3. Quant à American Express il n' ont pas de catégorie de niveau 4.

A chaque niveau correspond des exigences spécifiques de validation de la conformité. Alors que vous pouvez être un marchand de niveau 4 selon les classifications de Visa, vous pouvez être un marchand de niveau 2 selon American Express. L'exigence de validation de la conformité pour un commerçant American Express de niveau 3 est de fournir des test de vulnérabilités tous les trimestres. Un niveau 4 Visa est tenu de le faire selon la demande de la banque acquéreur.

Allez consulter les pages suivantes pour déterminer de quel niveau vous êtes par réseau de cartes:

- Visa

- MasterCard
- Discover
- American Express

En cas de doute, prenez le nombre de transactions par marque de carte, contactez votre banque acquéreur et demander la confirmation de votre niveau. Les banques acquéreurs ont le pouvoir de décision ultime sur les niveaux de leurs marchands, de sorte que vous devez vérifier vos hypothèses avec votre banque.

DEUXIEME ETAPE: déterminer ce que vous avez besoin de soumettre à validation de la conformité.

Une fois que vous savez à quel niveau vous êtes, vous pouvez maintenant déterminer ce que vous devez fournir à votre banque acquéreur afin de montrer validation de la conformité. Si vous répondez aux exigences des marques de cartes pour le niveau 4, puis les étapes restantes à effectuer avant de commencer votre validation de la conformité sont de déterminer qui SAQ est appropriée pour soumettre à votre organisation, et - si vous êtes tenu de soumettre trimestriellement externe scans - pour sélectionner une Scanning Vendor agréé (ASV).

Ce tableau reflète ce que votre banque acquéreur serait vous attend à soumettre afin de valider la conformité; Cependant, gardez à l'esprit que l'acquéreur peut modifier leurs exigences à tout moment, donc il vaut la peine de vérifier les attentes avant le début des travaux.

Il existe cinq types de SAQ: A à D. Les facteurs qui affectent la version dont vous avez besoin pour compléter dépend si vous utilisez vos propres systèmes de cartes de crédit de traiter les paiements, les données des titulaires magasins et d'accepter en personne et / ou par voie électronique, entre autres choses :

Type de SAQ	Description	Nombre questions (v3.0)	ASV Scan Requis
A	Carte non présente: toutes les fonctions de traitement des paiements sont externalisée, pas de stockage électronique de données de titulaire de carte	14	Non
A-EP	E-commerce re-diriger vers un tiers, fournisseur de services conforme PCI pour le traitement des paiements, pas de stockage électronique de données de titulaire de carte	139	Oui
B	Commerçants avec seulement des machines à impression ou seulement des terminaux de paiement autonome dial-out : Non e-commerce ou pas de stockage électronique de données	41	Non
B-IP	Commerçants avec des terminaux de paiement IP autonome (Internet) connectés: Non e-commerce ou pas de stockage électronique de données	83	Oui
C	Commerçants avec les systèmes d'application de paiement connectés à Internet: Non e-commerce ou pas de stockage électroniques des données des titulaires de cartes	139	Oui
C-VT	Marchands avec les terminaux de paiement virtuelle sur le Web: Pas de e-commerce ou pas de stockage électronique	73	Non

	des données des titulaires de cartes		
D-commerçant	Tous les autres commerçants ou ceux qui stockent électroniquement les données des titulaires de cartes	326	Yes
D-fournisseur de services	Les fournisseurs de services admissibles SAQ	347	Yes
P2PE	Terminaux de paiement dans une solution de P2PE PCI validé seulement: Non e-commerce ou stockage électronique de données des titulaires de la carte	35	No

ASV sont des organisations qui effectuent des tests externes trimestriels de vulnérabilité pour les commerçants et ont été qualifiés et pré-approuvée par le PCI Council. Il est nécessaire que toutes les entreprises qui présentent des analyses de réseau trimestriels utilisent un prestataire qui a obtenu le statut ASV. Notez que votre organisme sera tenu de soumettre des scans sans défaut, cela signifie qu'il n'y a aucun défaut de vulnérabilité trouvé et que les les scans ont été attestés à la fois par vous et votre ASV.
Souvent, les organisations choisissent d'effectuer leurs premières analyses avant la fin du trimestre de telle sorte que toutes les vulnérabilités ou des défauts trouvés peuvent être corrigés. Ainsi une nouvelle analyse effectuée à la fin du trimestre pourra montrer des rapports de vulnérabilité sans défaut.