Que faire pour être en conformité avec la norme PCI DSS ?

Lâ€™avÃ¨nement du e-commerce et des Marketplaces sâ€™est accompagnÃ© dâ€™un risque croissant de violation des donnÃ©es bancaires. Pour faire face Ã cette menace et afin dâ€™amÃ©liorer la sÃ©curitÃ© des donnÃ©es des consommateurs et leur confiance dans lâ€™Ã©cosystÃ¨me de paiements, 5 acteurs ont lancÃ© - en 2006 - le Conseil de sÃ©curitÃ© des cartes de paiement (PCI SSC). Cette dÃ©marche a permis dâ€™homogÃ©nÃ©iser les diffÃ©rents programmes normatifs de sÃ©curitÃ© alors en vigueur, pour crÃ©er une norme commune : la Payment Card Industry Data Security Standard (PCI DSS).

La PCI DSS, quelle importance ?

Cette norme mondiale dÃ©signe lâ€™ensemble des exigences de sÃ©curitÃ© des donnÃ©es applicables Ã lâ€™industrie des cartes de paiement. Elle nâ€™a pas Ã©tÃ© rendue obligatoire, ni au regard de la loi amÃ©ricaine, ni aux yeux du gouvernement franÃ§ais. Toutefois, la PCI DSS est imposÃ©e contractuellement par les principaux acteurs du marchÃ© des cartes de paiement. La certification Ã cette norme est depuis devenue une rÃ©fÃ©rence en matiÃ¨re de protection des donnÃ©es de paiement des consommateurs.

Lâ€™impact dâ€™une cyberattaque est tout aussi important pour lâ€™entreprise victime - peu importe sa taille, que pour ses clients. Les consÃ©quences peuvent se traduire autant, pour une organisation, par une perte de revenus, de clients, de confiance et dâ€™un prÃ©judice pour lâ€™image de lâ€™entreprise, que par un risque accru de phishing, dâ€™usurpation dâ€™identitÃ© ou de vol de fonds pour le consommateur. Il est donc plus quâ€™important que toute sociÃ©tÃ© - qui traite les donnÃ©es de titulaires de cartes de paiement - fasse le nÃ©cessaire pour maintenir ces donnÃ©es en sÃ©curitÃ©.

Que faire pour Ãªtre en conformitÃ© ?

La documentation officielle, publiÃ©e par le Conseil PCI SSC, comporte quelque 1 800 pages organisÃ©es en 12 exigences auxquelles toute entreprise, commerÃ§ant comme fournisseur, doit se conformer. Voici ce que vous devez savoir sur la conformitÃ© PCI DSS :

Installer et gÃ©rer une configuration avec pare-feux pour protÃ©ger les donnÃ©es des titulaires de cartes : Lâ€™exigence de la PCI DSS requiert lâ€™utilisation de pare-feux, afin dâ€™empÃªcher tout accÃ¨s non-autorisÃ© aux systÃ¨mes. Ceux-ci contrÃ´lent la transmission de donnÃ©es entre le rÃ©seau interne dâ€™une organisation.

Ne pas utiliser les paramÃ¨tres par dÃ©faut du fournisseur pour les mots de passe systÃ¨me et autres paramÃ¨tres de sÃ©curitÃ© : Lâ€™utilisation des paramÃ¨tres de sÃ©curitÃ© par dÃ©faut augmente la vulnÃ©rabilitÃ© des systÃ¨mes. Les paramÃ¨tres et mots de passe par dÃ©faut dÃ©finis doivent Ãªtre changÃ©s et les comptes par dÃ©faut non utilisÃ©s dÃ©sactivÃ©s ou supprimÃ©s.

ProtÃ©ger les donnÃ©es des titulaires de cartes : Il est nÃ©cessaire de formaliser et mettre en oeuvre des procÃ©dures et processus qui rÃ©gissent la gestion des traitements apportÃ©s aux donnÃ©es (mise Ã jour, chiffrement, stockage, suppression).

Chiffrer la transmission des donnÃ©es des titulaires de cartes sur les rÃ©seaux publics ouverts : Il sâ€™agit notamment de la transmission des donnÃ©es par Internet et Ã lâ€™aide des technologies sans fil comme le Bluetooth, les communications GPRS et satellite.

Utiliser et mettre rÃ©guliÃ¨rement Ã jour logiciels et programmes antivirus : Il faut Ã©galement installer, maintenir et assurer le bon fonctionnement des antivirus pour protÃ©ger les systÃ¨mes contre les malwares.

DÃ©velopper et maintenir des systÃ¨mes et applications sÃ©curisÃ©es : Il est important de vÃ©rifier en permanence que les logiciels sont Ã jour - pour Ãªtre Ã lâ€™abri des derniÃ¨res vulnÃ©rabilitÃ©s.

Restreindre lâ€™accÃ¨s aux donnÃ©es des titulaires aux seules personnes concernÃ©es : La sÃ©curisation de son SI passe par la mise en place de systÃ¨mes et processus pour gÃ©rer et restreindre les accÃ¨s aux donnÃ©es.

Attribuer un identifiant unique Ã chaque personne ayant accÃ¨s Ã un ordinateur : Lâ€™organisme doit aussi sâ€™assurer que seules les personnes dÃ»ment autorisÃ©es ont accÃ¨s Ã certains systÃ¨mes et composants spÃ©cifiques. Lâ€™authentification Ã deux facteurs comme les cartes Ã puce, les clÃ©s USB cryptographiques ou la biomÃ©trie permet de sâ€™assurer du respect des autorisations.

Restreindre lâ€™accÃ¨s physique aux donnÃ©es : Lâ€™accÃ¨s aux salles serveur et centres de donnÃ©es doit Ãªtre rÃ©glementÃ©, tandis que les Ã©quipements sur lesquels se trouvent ces donnÃ©es doivent Ãªtre surveillÃ©s et protÃ©gÃ©s contre toute altÃ©ration.

Tracer et surveiller tous les accÃ¨s aux ressources rÃ©seau et aux donnÃ©es des titulaires de cartes : Des processus de journalisation des actions de chaque utilisateur doivent Ãªtre dÃ©ployÃ©s (accÃ¨s aux donnÃ©es, privilÃ¨ges, tentatives de connexion non valides, modifications apportÃ©es aux mÃ©canismes dâ€™authentification). Et ceux-ci doivent Ãªtre examinÃ©s rÃ©guliÃ¨rement.

Tester rÃ©guliÃ¨rement les systÃ¨mes et processus de sÃ©curitÃ© : Des tests dâ€™intrusions doivent Ãªtre menÃ©s chaque annÃ©e, et aprÃ¨s toute modification importante sur le rÃ©seau. Les analyses de vulnÃ©rabilitÃ©s et la maintenance de la topologie du rÃ©seau et des pare-feux doivent Ã©galement faire partie de ces tests.

Maintenir une politique de sÃ©curitÃ© abordant la sÃ©curitÃ© des informations pour employÃ©s et prestataires : Une politique formalisÃ©e, revue Ã frÃ©quence rÃ©guliÃ¨re et maintenue Ã jour doit

encadrer tous les processus de sÃ©curitÃ© des informations, prendre en compte un programme de sensibilisation des collaborateurs et un processus formel de communication.

Quelles sont les implications pour votre entreprise ?

Les entreprises qui souhaitent se mettre en conformitÃ© avec la norme PCI DSS devraient donc, en premier lieu, analyser et comprendre la maniÃ¨re dont les donnÃ©es sont rÃ©cupÃ©rÃ©es, stockÃ©es et organisÃ©es. Pour gÃ©rer en toute sÃ©curitÃ© le traitement des donnÃ©es et Ã©viter de dÃ©penser dâ€™importantes ressources financiÃ¨res et matÃ©rielles, de nombreuses entreprises utilisent une solution dâ€™hÃ©bergement chez un tiers, prestataire de services de paiement (PSP). Ce partenaire de confiance prend en charge tous les aspects relatifs Ã la sÃ©curitÃ© des transactions, afin que lâ€™entreprise nâ€™ait plus quâ€™une poignÃ©e de contrÃ´les simples Ã mettre en oeuvre, tels que lâ€™utilisation de mots de passe forts.

Pour Ãªtre en rÃ¨gle, il est donc indispensable de protÃ©ger son rÃ©seau et ses infrastructures, et ce quelle que soit la taille de lâ€™entreprise - sans oublier de mettre Ã lâ€™abri les ressources les plus prÃ©cieuses pour de lâ€™organisation, Ã savoir ses donnÃ©es. Il est Ã©galement important de renforcer les contrÃ´les dâ€™accÃ¨s, chiffrer les communications et les transmissions de donnÃ©es, ainsi que de garantir lâ€™intÃ©gritÃ© des donnÃ©es transmises.

Et maintenant ?

Depuis, la directive sur les services de paiements 2 (DSP2 en franÃ§ais ou PSD2 en anglais) est entrÃ©e en vigueur en juin 2021 - aprÃ¨s plusieurs reports dÃ¨s septembre 2019. Câ€™est une directive europÃ©enne qui s'applique Ã toutes les entreprises susceptibles de s'engager avec des clients europÃ©ens, amÃ©liorant la rÃ©glementation PCI DSS dÃ©finie en 2006. Lâ€™un des changements majeurs est l'exigence d'une authentification forte du client (SCA) pour les transactions en ligne.