Guide à l'attention des développeurs / hébergeurs de sites web marchands sur le niveau minimum de sécurité pour le traitement de numéros de cartes bancaires

Préambule

Ce guide n'a pas vocation à se substituer à une démarche de certification PCI DSS.

L'objet de ce guide est de fournir aux développeurs / hébergeurs de solutions de paiement en ligne les informations de bonnes pratiques pour mettre en place les « *mesures de sécurité minimales* » requises pour contrer les attaques les plus simples et les plus fréquemment utilisées par des attaquants externes.

Introduction

De nombreux 'petits/moyens' commerces qui souhaitent développer des offres de « *e-business* » s'adressent à des prestataires pour assurer le développement et/ou l'hébergement d'une solution de paiement. Dans la mesure où les développeurs / hébergeurs de e-commerces sont des acteurs indirects de la chaîne de paiement par cartes, leur sécurité fait partie intégrante de la stratégie globale de protection des données de cartes bancaires.

Une solution recommandée par le Groupement des Cartes Bancaire est de dé corréler la fonction de transaction commerciale de la fonction de paiement par carte bancaire. Cette seconde fonction nécessite une très haute protection en raison de la sensibilité des numéros de cartes. L'un des moyens les plus simples pour la réaliser est de faire appel à un prestataire de paiement spécialisé qui est certifié selon le référentiel PCI DSS. Ainsi, le commerçant et son hébergeur , sous réserve qu'ils ne conservent pas le numéro de carte par ailleurs, sont exempts de la certification PCI DSS.

Néanmoins, dans le cas où le commerçant a choisi de développer lui-même ou de faire développer la fonction de paiement par un prestataire, il doit entrer dans une démarche de mise en conformité de son système d'information aux exigences de PCI DSS. Selon les volumes de transaction par carte bancaire qu'il traite par an, il devra se conformer aux exigences des classes 1, 2, 3 ou 4 déterminés par les réseaux internationaux. Ce guide s'adresse aux commerçants de tous les niveaux.

Ces acteurs n'ont pas toujours une bonne connaissance de la démarche de certification PCI DSS. Rappelons qu'elle vise à vérifier la conformité des mesures de protection d'un système d'information, qui stocke, transfère, traite des données de cartes bancaires, au référentiel détaillé de PCI DSS (environ 300 points de contrôle).

Or, il apparait lors des audits que, dans de nombreux cas, les sites web ne respectent pas les règles élémentaires de bonnes pratiques pour le développement ou l'hébergement de systèmes web sécurisés (Top 10 des vulnérabilités de sites web [1]).

Ce guide a également pour but de fournir aux commerçants les éléments de dialogue et les points de contrôles sur l'offre qui peut leur être proposée par leurs prestataires.

Eléments de contexte

En 2011, le rapport annuel de la société Verizon [2] mentionne que 92% des brèches proviennent d'attaques externes. Ce chiffre est en forte progression (+22%). La raison n'est pas due à une multiplication des hackers (hyper-spécialistes), mais à la mise à disposition par ceux-ci de logiciels d'attaques « *sur étagère* » utilisables par des non spécialistes.

Ces attaques utilisent dans la moitié des cas des failles basiques des systèmes et en particulier celles des sites web. Le constat est que dans 92% des cas les attaques étaient **simples à réaliser** et basées sur des **vulnérabilités identifiées depuis très longtemps**. Il est révélateur de dire que 96% des brèches auraient pu être évitées par l'application de mesures de sécurité relevant simplement des bonnes pratiques.

Ce sont ces mêmes constats que relève Patrick Pailloux, le Directeur de l'Agence nationale pour la sécurité des systèmes d'information (ANSSI) dans son discours[1] de clôture des Assises de la Sécurité 2011 en disant « *[…] la réalité vraie, celle que l'on constate tous les jours, c'est que nos systèmes d'informations sont très souvent perméables, et que très souvent, des acteurs malveillants en ont très largement profité.* », et d'ajouter « *Il faut reprendre le pouvoir sur nos propres systèmes* ».

Les référentiels de bonnes pratiques

Plusieurs documents de référence pour la communauté des développeurs sur le web décrivent en détail les attaques les plus simples qui utilisent des vulnérabilités de programmation de sites web. Le plus connu est celui de « *l'Open Web Application Security Project* » plus connu sous son acronyme OWASP. Il remet à jour régulièrement le classement des 10 vulnérabilités les plus utilisées pour compromettre des sites web et accéder aux systèmes d'information qui les hébergent et par la suite aux données qui y sont stockées.

De nombreux faits divers de vols de plusieurs millions de numéros de cartes bancaires reposent sur ce type d'attaques.

[1] http://www.ssi.gouv.fr/fr/anssi/publications/discours-de-patrick-pailloux-lors-de-la-conference-de-cloture-des-assises-de-la.html

Plus récemment le rapport [3] du « *centre pour la protection des infrastructures nationales anglaises (CNPI)* » donne des conseils sur les meilleurs conseils pour se protéger contre les attaques les plus utilisées par les hackers. Pour ce dernier rapport, il s'agit de conseils élémentaires et de bon sens. Leur mise en œuvre réduit notablement la surface d'attaque visible par les agresseurs.

Bien entendu, il faut citer le référentiel PCI DSS [4] qui n'est pas un guide de bonne pratique en soi, mais un référentiel qui permet au développeur de prendre conscience des points de contrôles que les auditeurs vont vérifier lors de leur certification PCI DSS.

Enfin nous ne pouvons qu'inciter les différents acteurs à consulter les guides de bonnes pratiques pour la sécurisation de systèmes d'informations sur le site gouvernemental de l'ANSSI [5].

Les vulnérabilités les plus fréquemment utilisées

Ce chapitre ne vise pas à répéter les conseils de l'OWASP à partir desquels les développeurs informatiques trouveront les éléments techniques utiles à l'implémentation des mesures de sécurité. Il est plus destiné à des commerçants ou à des dirigeants de prestataires de service.

L'attaque par injection (injection flaw)
Elle consiste à utiliser une zone de saisie d'un critère de recherche dans un formulaire web pour y « *injecter* » un code exécutable. Au lieu de saisir son critère de recherche (par : exemple un numéro de compte), l'attaquant saisie les caractères d'une formule logique (ex : 'or'1'='1). Le logiciel qui analyse la zone de saisie va « *interpréter* » les caractères en exécutant la commande.

L'attaque par cross-site scripting (XSS)
Elle consiste à utiliser les zones de saisies d'une page web (ex : nom, prénom, etc.) via le navigateur pour forcer l'exécution d'une commande exécutable (script). Cette attaque peut permettre de détourner une session utilisateur (Man in the middle), défigurer un site web ou voler des identités d'utilisateurs légitimes.

La violation de gestion d'authentification
Cette attaque utilise une mauvaise implémentation des fonctions d'authentification sur un site web. L'attaquant peut compromettre les mots de passe ou des jetons de session pour s'approprier les droits d'accès d'utilisateurs légitimes (et donc de ses privilèges).

La référence directe non sécurisée à un objet
Cette attaque peut survenir lorsqu'un développeur référence par son nom explicite, un objet qu'il manipule (fichier, enregistrement de base de données, etc.). L'attaquant peut alors manipuler ces références pour accéder aux donnes exposées.

La falsification de requêtes intersites (CSRF cross site request forgery)
Cette attaque force le navigateur d'une victime correctement authentifiée à envoyer une requête HTTP falsifiée à une autre application web connue pour ses vulnérabilités. L'application cible identifie la requête comme provenant d'un utilisateur légitime.

La mauvaise configuration de sécurité
L'attaque consiste à utiliser le fait que les logiciels utilisés pour le développement du site web ne sont pas à leur dernière version de mise à jour et qu'il existe des failles connues sur les versions utilisées.

Le stockage cryptographique non sécurité
Sur un site web, les moyens de protection des données sensibles utilisent des algorithmes ou des clés faibles. Les attaquants peuvent copier les données et par la suite les décrypter.

Le manque de restriction d'accès URL
Un utilisateur autorisé sur certaines pages web peut modifier dynamiquement le nom de l'URL pour accéder à des pages qui normalement nécessitent une authentification. Certaines applications ne restreignent pas suffisamment l'accès à des pages sensibles.

Protection insuffisante de la couche transport
L'attaque consiste à surveiller et écouter le trafic réseau des utilisateurs. Il peut s'agir de sites web dont l'authentification n'est pas protégée en HTTPS lors de la phase d'authentification. Les identifiants et mots de passe circulent en clair et leur interception peut conduire à une usurpation d'identité.

Redirection et renvois non validés d'URL
L'attaquant crée des liens vers des redirections non validées (sites de phishing ou de logiciels malveillants) et invite les utilisateurs à cliquer dessus. Les victimes sont enclines à cliquer sur ces liens, puisqu'ils semblent pointer vers un site valide. L'attaquant utilise les renvois (forwards) non sûrs pour contourner des contrôles de sécurité.

Les bonnes pratiques élémentaires

Se concentrer sur les contrôles essentiels : beaucoup d'entreprises font l'erreur de viser un très haut niveau de sécurité sur certains points tout en négligeant complètement les autres. On est bien mieux protégé lorsque les normes élémentaires sont appliquées dans l'ensemble de l'organisation.

Ne conserver que les données utiles : si vous n'avez pas besoin de ces données, ne les conservez pas. En revanche, les données utiles doivent impérativement être identifiées, surveillées et stockées en lieu sûr.

Sécuriser les services d'accès à distance : restreindre les autorisations à des réseaux et adresses IP prédéfinis, pour limiter les accès publics. Les entreprises ont aussi intérêt à restreindre l'accès aux informations sensibles au sein de leur réseau interne.

Surveiller les comptes des employés ayant les droits les plus larges : la meilleure approche consiste à faire confiance à l'utilisateur après avoir vérifié sa probité lors de l'embauche, et en lui accordant des droits d'accès limités en fonction de son rôle ou de ses responsabilités. Les managers doivent fournir des consignes de sécurité claires et vérifier que les collaborateurs respectent effectivement les règles et procédures en place.

Vérifier régulièrement les comptes utilisateurs : s'assurer que les comptes actifs sont valides, utiles, correctement configurés et que les droits d'accès correspondants sont adéquats (les moins permissifs possibles). Veiller à supprimer les comptes non actifs ou ceux des employés qui sont partis.

Gérer et analyser les logues : il ne s'agit pas de les étudier ligne à ligne, mais de s'intéresser aux principaux problèmes. L'important est d'abaisser le délai de détection des infractions à quelques jours seulement. Pour protéger au mieux les données, privilégier les processus de surveillance et d'alerte les plus intelligents, efficaces et réactifs.

Sensibiliser les employés aux méthodes d'ingénierie sociale et aux différents vecteurs d'attaques qu'elles représentent : leur apprendre à s'interroger avant de cliquer sur un lien et à se méfier des pièces jointes aux e-mails dont ils ne connaissent pas l'expéditeur.

Comment vérifier son niveau de vulnérabilité ?

Les tests de vulnérabilité et de pénétration : c'est certainement la première chose à faire que de savoir d'où on part et quels sont les améliorations à faire. Un test de vulnérabilité peut être automatique et se faire à distance à partir d'outils du marché. Le test de pénétration pour sa part est réalisé par des experts qui vont utiliser un savoir-faire ciblé sur l'environnement particulier qu'ils analysent.

Comme l'impose PCI DSS, les tests de vulnérabilité doivent être réalisés de façon trimestrielle afin de vérifier que les évolutions régulièrement apportées aux systèmes n'ont pas augmenté le niveau de vulnérabilité aux attaques externes.

L'audit de code : cette mesure peut être nécessaire pour analyser des applications déjà existantes qui ont pu ressortir comme vulnérables lors des tests évoqués ci-dessus. Les guides techniques de l'OWASP permettent de réaliser des audits de code et de corriger les failles.

La sensibilisation et la formation des développeurs : bien sûr le meilleur moyen de ne pas avoir de faille dans une application est de programmer selon les règles de l'art pour une bonne sécurité. Là aussi des guides existent comme « *l'OWASP Developer's Guide* ». Ceci n'exclu pas de faire régulièrement des tests de vulnérabilité.

La mise en œuvre des mesures correctives

Une fois bien identifié l'état des lieux des vulnérabilités potentielles l'entreprise peut utiliser l'approche par priorités [6] proposé par le PCI SSC pour planifier un projet de mise en œuvre des mesures correctives.

Synthèse

La sécurité des données bancaires concerne tous les acteurs sans exception, y compris les hébergeurs. Rappelons que les exigences PCI DSS s'appliquent à toute entité qui stocke, traite ou transmet les données sensibles.

Encore une fois 92% des attaques constatées sont techniquement simples, par conséquent la mise en œuvre systématique des protections et des vérifications basiques bien connues du monde IT et des RSSI est un pré-requis impératif pour bien protéger les données sensibles cartes bancaires.

Références

[1] OWASP Foundation, "*OWASP Top 10 – 2010 Les Dix Risques de Sécurité Applicatifs Web les Plus Critiques "*, (Open Web Application Security Project)

[2] Verizon, "2011 Data Breach Investigation Report"

[3] Centre for the Protection of National Infrastructure; "*Development and implementation of secure web application"*, August 2011 (Organisme national anglais en charge de la protection des infrastructures critiques du pays – En France ses missions sont assurées par l'ANSSI)

[4] Payment Card Industry – Data Security Standard, *Requirements and Security Assessment Procedures*, Version 2.0, October 2010

[5] Le lien vers le site de l'ANSSI : http://www.ssi.gouv.fr/fr/bonnes-pratiques/

[6] Payment Card Industry – PCI DSS Prioritized Approach for PCI DSS 2.0, May 2011