CHECKLIST DE LA CONFORMITÉ A LA NORME PCI DSS 3.2

PROTÉGER LES DONNÉES STOCKÉES DU TITULAIRE

Exigence DSS 3

Protéger les données stockées du titulaire

FAIRE:

- ☐ Appliquer des politiques documentées de conservation et d'élimination des données afin de limiter la collecte et la durée de conservation des données de titulaire. (3.1)
- ☐ Interroger vos employés pour vérifier que les politiques sont suivies et que des procédures trimestrielles sont en place pour éliminer les données du titulaire, en dehors de votre politique de conservation. (3.1.b)
- ☐ S'assurer que les données stockées et les données en transit sont illisibles. (3.4, 4.1)
- ☐ Crypter les données de carte et protéger les clés cryptées. (3.5)
- ☐ Masquer vos données PAN lorsqu'elles doivent être vues (voir plus haut) en utilisant le moins de chiffres possible (afficher moins que les 6 premiers et les 4 derniers). (3.3)
- ☐ Créer un diagramme des flux relatifs au titulaire de carte pour tous les flux de données à travers votre organisation. (1.1.3)
- ☐ Utiliser un outil de découverte de données pour repérer les données sensibles mal placées dans votre environnement.

A EVITER:

- ☐ Stocker des données d'identification sensibles après autorisation. (3.2)
  - o **Exception:** votre organisation est émettrice et dispose d'une justification commerciale.
- ☐ Stocker des données PAN masquées.
  - o **Solution:** les crypter.

Exigence DSS 4

Crypter la transmission des données du titulaire sur les réseaux publics ouverts

A FAIRE:

- ☐ Identifier la destination des données du titulaire et s'assurer que vos polices ne font pas l'objet d'une violation sur le trajet et que ne sont utilisés que des clés ou des certificats fiables. (4.1)
- ☐ Sélectionner un échantillon de transmissions entrantes et sortantes et vérifier que la cryptographie est maintenue lors du transit. (4.1.c)

A EVITER:

- ☐ Envoyer des PAN par technologie de messagerie utilisateur final, par exemple courrier électronique, SMS ou messagerie instantanée. (4.2)
- ☐ Employer de nouvelles technologies utilisant les protocoles SSL/prédécesseur de TLS. (version 1.0 ou antérieure)
- ☐ Faire migrer les données du titulaire vers des systèmes utilisant SSL/prédécesseur de TLS. (version 1.0 ou antérieure)

PROTÉGEZ-VOUS CONTRE LES MENACES EXTERNES

Exigence DSS 1

Installer et gérer une configuration de pare-feu pour protéger les données du titulaire

A FAIRE:

- ☐ Installer un pare-feu au niveau de chaque connexion Internet (chaque appareil) et entre toute zone démilitarisée (DMZ) et la zone de réseau interne (1.1.4, 1.4)
- ☐ Configurer vos pare-feu avec une description des groupes responsables des composants réseau et une justification professionnelle pour tous les services/protocoles/ports de la configuration. (1.1.5, 1.1.6)
- ☐ Examiner la configuration des pare-feu et des routeurs au moins tous les 6 mois et s'assurer que tout trafic autre, non configuré (entrant ou sortant) est refusé. (1.1.7, 1.2.1)
- ☐ Créer des configurations de routeurs qui bloquent les connexions entre les parties non approuvées du réseau et les données de titulaire. (1.2, 1.3)
- ☐ Charger quelqu'un de vérifier chaque jour les journaux de pare-feu.

A EVITER:

- ☐ Stocker les données de titulaire de carte dans le DMZ ou tout réseau non fiable.
  - o **Solution:** créer une zone de réseau interne sécurisée. (1.3.6)

Exigence DSS 2

Ne pas utiliser les mots de passe système et autres paramètres de sécurité par défaut définis par le fournisseur

A FAIRE:

- ☐ Identifier un administrateur système responsable des composants système. (2.2.4)
- ☐ Maintenir un inventaire de tous les composants du système qui se trouvent dans le champ d'application de la norme PCI DSS. (2.4)
- ☐ Documenter les politiques de modification des mots de passe par défaut définis par le fournisseur, des paramètres sans fil par défaut et supprimer les comptes par défaut avant d'installer un système sur votre réseau. (2.1, 2.1.1, 2.5)
- ☐ Documenter les normes de configuration des composants système relatives aux failles de sécurité, limiter les accès au service/protocole en fonction des besoins et suivre des normes de plus en plus strictes. (2.2, 2.2.2)

A EVITER:

- ☐ Mettre en applications plusieurs fonctions sur un même serveur, car cela risque de créer des conflits de permission. (2.2.1)
- ☐ Partir du principe que vos fournisseurs maintiennent une recherche anti-virus.
    - o **Exigence:** Il est de votre responsabilité de vous assurer que les fournisseurs sont à jour et procèdent à des scans réguliers.

Exigence DSS 5

Protéger tous les systèmes contre les logiciels malveillants et mettre à jour régulièrement les logiciels ou programmes anti-virus

A FAIRE:

- ☐ Mettre à jour régulièrement les logiciels antivirus sur les systèmes fréquemment affectés et déterminer si d'autres systèmes sont en danger/ont besoin d'un anti-virus. (5.1, 5.1.1, 5.1.2)
- ☐ Automatiser les scans anti-virus et maintenir des journaux d'audit anti-virus pour vos systèmes. (5.2)
- ☐ S'assurer que seuls les administrateurs peuvent modifier ou désactiver les anti-virus. (5.3)
- ☐ Documenter les procédures de protection contre les logiciels malveillants. (5.4)

A EVITER:

- ☐ Attendre, pour identifier un logiciel malveillant, de constater les dégâts qu'il cause.
  - o **Solution:** installer un logiciel capable d'observer les anomalies de comportement et d'alerter le personnel concerné.

Exigence DSS 6

Développer et gérer des systèmes et des applications sécurisés

A FAIRE:

- ☐ Mettre en place une procédure pour vous tenir informé des derniers points faibles de la sécurité et identifier le niveau de risque. (6.1)
- ☐ Installer tous les correctifs de sécurité développés par les fournisseurs. (6.2.a)
- ☐ Documenter l'impact, les parties autorisées, le test de fonctionnalité et les procédures d'annulation de toutes les procédures de contrôle des modifications. (6.4.5)
- ☐ Utiliser des procédures de développement strictes et des pratiques de codage sécurisées (6.3)

A EVITER:

- ☐ Attendre plus d'un mois pour installer les correctifs de sécurité développés par les fournisseurs pour les niveaux de risques identifiés comme critiques. (6.2.b)
- ☐ Tester les logiciels développés en interne dans votre environnement de production, utiliser des données de production lors des tests ou laisser les comptes/identifiants de test après la publication du logiciel. (6.3.1, 6.4.1, 6.4.3)

PROTÉGEZ-VOUS CONTRE LES MENACES INTERNES

Exigence DSS 7

Restreindre l'accès aux données du titulaire aux seuls individus qui doivent les connaître

A FAIRE:

- ☐ Créer une liste des rôles ayant accès à l'environnement des données du titulaire comprenant la définition de chaque rôle, leur niveau de privilège et les permissions nécessaires pour permettre à chaque rôle de fonctionner. (7.1, 7.3)
- ☐ Créer une liste des moindres privilèges pour tous les employés et un paramètre « refuser tous » pour tous les paramètres de contrôle d'accès (7.1.2, 7.2.3)
- ☐ Demander l'approbation documentée des parties autorisées pour l'affectation ou la modification des privilèges dans le CDE. (7.1.4)

A EVITER:

- ☐ Donner des permissions excessives à un rôle à l'occasion de cette « sale journée » où ils peuvent en avoir besoin.
  - o **Solution:** utiliser un modèle de moindres privilèges accordant des permissions uniquement en fonction des besoins professionnels.
  - o **Solution:** octroyer l'accès uniquement pour la période nécessaire.

Exigence DSS 8

Identifier et authentifier l'accès aux composants du système

A FAIRE:

- ☐ Définir et documenter des procédures d'identification et d'authentification de l'utilisateur sur tous les composants du système. (8.1, 8.4)
- ☐ Affecter aux utilisateurs un identifiant unique, tester les contrôles des privilèges et révoquer l'accès des utilisateurs inactifs/qui ne travaillent plus pour la société. (8.1.1, 8.1.2, 8.1.3, 8.1.4)
- ☐ Surveiller tous les comptes utilisés par les fournisseurs et autres tiers, puis les désactiver lorsqu'ils ne sont plus utilisés. (8.1.5)
- ☐ Verrouiller l'identifiant utilisateur pendant 30 minutes après six tentatives d'accès échouées. (8.1.6, 8.1.7)
- ☐ Suivre les directives relatives aux bonnes pratiques énoncées dans la norme DSS en matière de définition de mots de passe, y compris la composition d'un mot de passe robuste, le codage des informations d'authentification, la vérification de l'identifiant avant réinitialisation et une réinitialisation tous les 90 jours. (8.2.1, 8.2.2, 8.2.3, 8.2.4)
- ☐ Incorporer l'identification multifacteurs pour tous les accès administrateur non-console et les accès distants au CDE. (8.3)

A EVITER:

- ☐ Utiliser le même mot de passe pour plusieurs comptes ou appareils, si l'un d'entre eux est compromis, ils le seront tous.
- ☐ Utiliser des identifiants utilisateur ou des méthodes d'authentification partagés dans le CDE. (8.5)

Exigence DSS 9

Restreindre l'accès physique aux données du titulaire

A FAIRE: (le cas échéant)

- ☐ Documenter la procédure régissant l'accès physique aux systèmes CDE, dresser une liste de tous les appareils, en limitant l'accès aux rôles qui en ont besoin et en contrôlant l'ensemble grâce à des jetons d'autorisation et à la mise en place d'une surveillance. (9.1.1a, 9.1.1b, 9.2, 9.3, 9.9.1)
- ☐ Créer une autorisation visiteurs et des contrôles d'accès qui garantissent que les visiteurs sont identifiés, documentés et surveillés dans les zones ayant accès à l'environnement du titulaire de carte. (9.4)
- ☐ Mettre en place des contrôles rigoureux pour les supports physiques introduits dans les locaux, utiliser le courrier suivi pour les supports sortant des locaux et s'assurer que les supports détruits ne peuvent pas être reconstitués. (9.5, 9.6, 9.8)
- ☐ Former les employés aux processus d'identification des fournisseurs externes nécessitant un accès physique et identifier/signaler les comportements suspects. (9.9.2, 9.9.3)

PROTÉGEZ-VOUS CONTRE L'EXCÈS DE CONFIANCE

Exigence DSS 10

Suivre et surveiller tous les accès aux ressources réseau et aux données du titulaire

A FAIRE:

- ☐ Mettre en œuvre des pistes d'audit pour tous les systèmes, des alertes en cas d'activité suspecte et un plan d'intervention pour ces anomalies. (10.1, 10.2, 10.6.2.b))
- ☐ Suivre toutes les actions des administrateurs, les tentatives de connexion, les modifications de compte et les pauses dans les pistes d'audit. (10.2.3, 10.2.4, 10.2.5, 10.2.6)
- ☐ S'assurer que chaque journal d'audit consigne l'identifiant utilisateur, le type d'événement, la date et l'heure, la réussite ou l'échec de l'événement, son origine et les ressources affectées. (10.3)
- ☐ Conserver l'ensemble des journaux d'audit pour une durée minimale d'un an, avec les 3 derniers mois disponibles pour analyse. (10.7)
- ☐ Éviter la manipulation des pistes d'audit et utiliser un logiciel pour signaler les modifications des journaux. (10.5)
- ☐ Élaborer une procédure qui examine chaque jour les journaux système des CHD et une procédure qui examine tous les autres composants système en fonction des résultats de votre analyse des risques. (10.6.1, 10.6.2)

A EVITER:

- ☐ Donner accès au journal d'audit à n'importe qui sans justification liée au rôle. (10.5.1)
- ☐ Procéder à l'examen quotidien des pistes d'audit à l'aide d'une méthode manuelle ; la perte de temps peut être importante.
- ☐ Stocker les journaux d'audit pour les technologies ouvertes au public sur ces machines ; leur sécurité peut être compromise. (10.5.4)

Exigence DSS 11

Tester régulièrement les processus et les systèmes de sécurité

A FAIRE:

- ☐ Documenter chaque point d'accès sans fil autorisé avec une justification professionnelle. (11.1.1)
- ☐ Mettre en œuvre des procédures visant à tester les points d'accès sans fil autorisés et non autorisés chaque trimestre et à prendre les mesures appropriées. (11.1, 11.1.2)
- ☐ Effectuer des scans de vulnérabilité internes (avec un personnel qualifié) et externes (avec un fournisseur de service de scan approuvé, ASV pour Approved Scanning Vendor) chaque trimestre et à chaque modification importante du réseau, en corrigeant et en scannant à nouveau toutes les vulnérabilités identifiées. (11.2)
- ☐ Exécuter une fois par an des tests de pénétration internes et externes (avec un personnel qualifié ou des tiers) en corrigeant et testant à nouveau tout risque exploitable détecté. (11.3)
- ☐ Déployer un outil de détection de changement pour alerter le personnel de toute modification non autorisée des fichiers critiques du système et effectuer des comparaisons de fichier critique au moins une fois par semaine. (11.5)
- ☐ Mettre en œuvre un processus pour répondre aux alertes générées par la solution de détection de changement. (11.5.1, 11.6)

A EVITER:

- ☐ S'en tenir au strict minimum en matière de tests.
    - o **Solution:** procéder à des examens plus fréquents que le strict minimum ; vous réagirez aux menaces plus tôt, avant qu'elles ne soient exploitées.

Exigence DSS 12

Maintenir une politique régissant les informations de sécurité pour l'ensemble du personnel

A FAIRE:

- ☐ Publier une politique de sécurité révisée annuellement, qui documente l'ensemble des appareils et des services critiques du CDE, définir un accès approprié (en ce qui concerne les rôles, l'usage de cet accès et le lieu) et mettre en place une procédure d'évaluation des risques. (12.1, 12.2, 12.3, 12.4)
- ☐ Suivre chaque année une formation de sensibilisation à la sécurité avec l'ensemble du personnel qui a accès au CDE. (12.6)
- ☐ Affecter aux rôles des responsabilités en termes de documentation des procédures, d'analyse des alertes de sécurité, d'administration des comptes et de surveillance d'accès à toutes les données. (12.5)
- ☐ Conserver une documentation sur les prestataires de services. Elle comprendra la liste des services fournis, une sélection avec vérification préalable (y compris avec une évaluation des risques), l'acceptation par le prestataire de services de la responsabilité des CHD et un processus de surveillance de la conformité des fournisseurs à la norme PCI DSS. (12.8.1, 12.8.2, 12.8.3, 12.8.4, 12.8.5)
- ☐ Créer un plan d'action, testé annuellement, en cas de violation du système, définissant les missions de chaque rôle, les actions spécifiques aux différentes menaces/alertes, les mesures à prendre pour les systèmes critiques et la sauvegarde des données, les exigences légales en matière de rapports et de notification aux marques de cartes. (12.10)