https://www.reflectiz.com/blog/how-to-prepare-new-pci-dss-v4/?

Comment préparer votre entreprise en ligne à la nouvelle norme PCI DSS v4

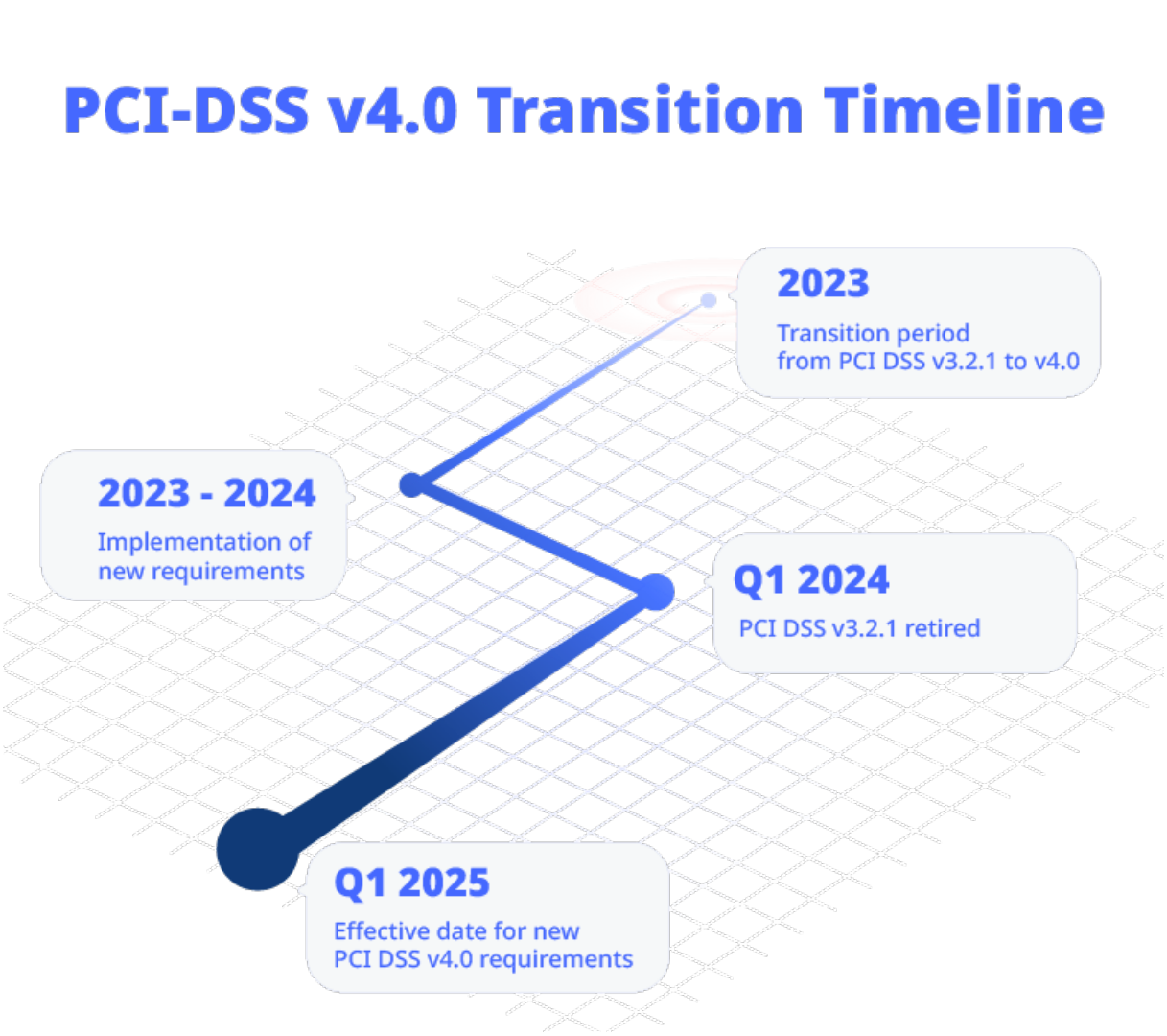
Vie privéeConformité en matière de sécurité

11 sept. 2023 Temps de lecture : 6 min

La norme de sécurité des données de l'industrie des cartes de paiement v3.2.1 sera officiellement retirée le 31 mars 2024, et bien que les organisations n'aient pas besoin de valider les nouvelles exigences PCI DSS v4.0 avant le 31 mars 2025, il y a deux raisons pour lesquelles vous devez mettre en place les améliorations de sécurité qu'elle décrit.

La première est que la mise en œuvre des nouvelles exigences veillera à ce que votre entreprise atteigne une meilleure base de normes techniques et opérationnelles, ce qui signifie une meilleure protection contre la fraude et le vol de données pour vos clients. La seconde est que la mise à niveau de vos procédures pour répondre aux nouvelles exigences dès maintenant révélera tous les domaines dans lesquels vous n'êtes pas à la hauteur, mais vous aurez encore le temps de les corriger avant la date limite.

Ces derniers mois sont le moment de s'assurer que tout est en place, et dans cet article, nous examinons comment vous pouvez les utiliser au mieux pour assurer une transition réussie vers la v4.0 pour votre entreprise.



PCI-DSS v4.0

Nous espérons que vous avez déjà une idée de ce que la nouvelle norme apporte, mais si ce n'est pas le cas, vous pouvez lire notre aperçu de la version 4.0 de PCI-DSS ici pour vous mettre à jour.

En bref, la nouvelle norme apporte des mises à jour et des clarifications pour de nombreuses exigences existantes et en ajoute également de nouvelles, notamment :

• Augmentation de la longueur minimale des mots de passe

• l'extension de l'utilisation de l'authentification multi-facteur (MFA)

• l'élargissement du champ d'application aux applications mobiles, à l'Internet des objets (IoT) et au cloud

• mettre davantage l’accent sur les rôles, les responsabilités et les exigences en matière de rapports ;

Mais en plus de noter ces changements, il convient également de reconnaître qu’ils signalent un changement dans la pensée sous-jacente à la nouvelle norme vers une philosophie Zero Trust.

Le Zero Trust est un cadre et une stratégie de cybersécurité qui fonctionnent selon le principe fondamental « ne jamais faire confiance, toujours vérifier ». Il part du principe qu’aucun utilisateur, appareil ou composant réseau ne doit être automatiquement approuvé, quel que soit son emplacement à l’intérieur ou à l’extérieur du réseau, car les cybercriminels attaqueront en utilisant n’importe quel vecteur. Dans une architecture Zero Trust, l’accès aux ressources et aux données n’est accordé qu’après qu’elles aient été dûment authentifiées et autorisées.

Alors que vous vous préparez pour la version 4.0, il est important de reconnaître que vous intégrez les éléments clés d’une stratégie Zero Trust dans l’ADN de votre entreprise, en ajoutant des contrôles d’accès stricts, une surveillance continue, une vérification de l’identité et le principe du moindre privilège, qui garantit que les utilisateurs et les appareils n’ont accès qu’aux ressources spécifiques dont ils ont besoin pour effectuer leurs tâches.

L’approche personnalisée

Bien que les exigences soient désormais plus strictes, vous disposez également d’une plus grande flexibilité dans la manière dont vous les respectez. La version 4.0 a introduit une autre option pour répondre à la conformité, appelée **approche personnalisée**. Cela permet aux entreprises de concevoir leurs contrôles de sécurité pour répondre aux exigences de chaque objectif, ce qui signifie que vous êtes libre d’utiliser des solutions telles que **Reflectiz** pour vous aider à le faire.

Vous pouvez toujours utiliser l’approche définie existante si cela convient à l’entreprise. Les organisations utilisent l’approche définie depuis des années pour mettre en œuvre et valider les exigences PCI DSS et elles peuvent toujours le faire avec la version 4.0. Elle convient peut-être mieux aux organisations qui ont déjà mis en place des contrôles pour répondre à une exigence et qui sont à l’aise avec les méthodes actuelles de validation. Elle peut également convenir aux organisations qui découvrent la norme PCI DSS et qui recherchent des directives plus spécifiques sur la façon d’atteindre leurs objectifs de sécurité.

Si vous choisissez l'approche personnalisée, il est important de collaborer avec votre évaluateur pour vous assurer qu'il comprend parfaitement vos contrôles personnalisés et que vous comprenez ses exigences et ce qu'il testera.

Ressources pour le changement

Si vous avez une longueur d'avance sur la préparation à l'état de préparation, le Conseil des normes de sécurité PCI encourage les organisations qui ont déjà mis en œuvre les nouveaux contrôles à les faire évaluer. Cela vous aidera à comprendre lesquelles de vos mesures sont adéquates et vous aidera également à identifier et à combler les lacunes restantes.

Si vous êtes encore au courant de l'état de préparation, le Conseil aide les parties prenantes à comprendre les changements à venir et à y répondre grâce à des ressources sur son blogue Perspectives PCI.

Vous pouvez également obtenir beaucoup d'informations et de conseils lors d'événements en personne, c'est pourquoi Reflectiz participera à la convention PCI DSS. Cette année, l'événement américain aura lieu du 12 au 14 septembre à Portland, dans l'Oregon. C'est l'occasion idéale pour les membres de la communauté de se connecter, de partager leurs connaissances et de découvrir les nouveautés des esprits les plus brillants en matière de sécurité des paiements.

Mises à jour des exigences

Vous trouverez ici toutes les modifications apportées aux exigences. Nous vous recommandons également de consulter notre article sur la liste de contrôle de conformité ici, ainsi que notre article sur les nouvelles exigences ici. Nous les appelons « meilleures pratiques » dans ce dernier article (ce qu'elles sont !), mais rappelez-vous qu'à partir du 31 mars 2025, elles deviennent officiellement des exigences.

Il n'est pas nécessaire de répéter ici toutes les informations de ces liens, mais il convient de souligner certains des changements les plus importants dont Reflectiz s'occupe.

6.3.2 vous oblige à maintenir un **inventaire** de logiciels sur mesure et personnalisés.

6.4.3 se concentre sur la **gestion** des scripts qui sont chargés et exécutés dans le navigateur du consommateur lors des transactions de paiement.

Selon cette section, les organisations doivent gérer tous les scripts de page de paiement qui sont chargés et exécutés dans le navigateur du consommateur de la manière suivante :

• Autorisation de script : une méthode doit être implémentée pour confirmer que chaque script est autorisé.

• Intégrité du script : Une méthode doit être implémentée pour assurer l'intégrité de chaque script.

• Inventaire des scripts : Un inventaire de tous les scripts doit être tenu avec une justification écrite de la raison pour laquelle chaque script est nécessaire.

Ces mesures visent à minimiser la probabilité d'une attaque par ce vecteur en s'assurant que les scripts sont explicitement autorisés et que leur intégrité est maintenue. En tenant un inventaire de tous les scripts avec une justification écrite de la raison pour laquelle ils sont nécessaires, les organisations peuvent mieux gérer et contrôler ceux qui sont chargés et exécutés sur leurs pages de paiement. Cela permet de protéger les utilisateurs contre des menaces telles que Magecart ou les attaques de clonage Web, qui fonctionnent en falsifiant ou en modifiant les scripts.

La solution Reflectiz vous aide à répondre à ces deux exigences en créant et en **maintenant un inventaire** de tous les scripts et logiciels internes et tiers et en **alertant** les utilisateurs de toute tentative de les compromettre.

11.6.1 vient, encore une fois, en réponse au danger croissant des attaques par écrémage du Web. Il fait appel à un mécanisme capable de détecter la falsification des en-têtes HTTP et du contenu des pages de paiement tel qu'il est reçu par le navigateur du client. Il exige de ce « mécanisme » qu'il signale rapidement de tels changements. Encore une fois, **Reflectiz détecte et alerte** les utilisateurs de ces changements et vous donne le contrôle de donner le feu vert aux comportements appropriés, de bloquer ceux qui sont à risque et de renvoyer les autres aux équipes de sécurité pour une enquête plus approfondie.

Faire le travail

Le processus de transition

Voici quelques conseils pour savoir par où commencer le processus de transition :

• Impliquer tous les départements et fonctions dans le plan de transition.

• Définir clairement les rôles et les responsabilités pour chaque exigence.

• Utiliser une gestion de projet efficace, maintenir des plans précis et suivre les progrès.

• Documenter minutieusement les politiques et procédures pour soutenir la mise en œuvre du contrôle de sécurité, y compris les nouvelles exigences en matière de documentation dans la norme PCI DSS v4.0.

Faire appel à des partenaires de confiance

• Éduquer et former le personnel sur leurs rôles en matière de sécurité des données et de conformité PCI DSS.

• Travailler en partenariat avec des professionnels qualifiés (PCIPs, ISAs, QSAs) pour la mise en œuvre du contrôle de sécurité.

• Utiliser des technologies et des solutions validées par rapport aux normes de sécurité pour protéger les données de paiement.

Effectuez vos propres évaluations

• Commencez à vous préparer à l'évaluation PCI-DSS le plus tôt possible.

• Effectuer des évaluations des lacunes afin d'identifier les domaines nécessitant des améliorations.

• Tester régulièrement les contrôles de sécurité pour s'assurer d'une bonne mise en œuvre.

• Établir une communication ouverte avec l'équipe d'évaluation avant l'évaluation.

Traiter la sécurité comme un processus continu

Reconnaître que la norme PCI DSS v4.0 prend en charge des processus de sécurité continus et à long terme. À tous les niveaux de votre organisation, vous devez penser que la sécurité n'est pas seulement une réflexion après coup, mais qu'elle fait partie intégrante de chaque processus et qu'elle constitue un engagement continu.

• Choisissez des contrôles de sécurité qui correspondent aux besoins de l'entreprise et de la sécurité.

• Organiser régulièrement des séances de formation et de sensibilisation du personnel.

• Intégrer la sécurité dans les pratiques quotidiennes et la culture organisationnelle.

• Traiter la sécurité comme un processus continu visant à réduire les incidents et les violations de sécurité.

En suivant ces étapes, les entreprises peuvent améliorer leur préparation aux évaluations de conformité PCI DSS v4.0 et maintenir des pratiques de sécurité solides au fil du temps.

Nous pouvons vous aider

Le fait que la norme PCI-DSS v4.0 vous permette d'adopter une approche personnalisée pour répondre à ses exigences signifie que vous pouvez utiliser des solutions innovantes telles que la plateforme Reflectiz pour gérer votre posture de sécurité et élever votre niveau de conformité avant avril 2025.

Reflectiz s'engage à vous aider à protéger votre entreprise et vos clients en respectant et en maintenant les normes PCI DSS, et pour les 30 prochains jours, nous vous offrons accès complet à notre tableau de bord PCI innovant GRATUIT ! Cet outil puissant, mais simple, élimine les conjectures lors de la surveillance de votre niveau actuel de conformité à la norme PCI-DSS v4.0, ce qui vous permet d'identifier les failles de sécurité et d'y répondre efficacement.