

La solution Intellinx pour une conformité à la norme PCI DSS

Le défi

La Norme en matière de sécurité des données liée à l'industrie des cartes bancaires (PCI DSS) a été conçue par les principales sociétés de carte de crédit comme un guide aux entreprises traitant des paiements par carte afin de lutter contre les fraudes à la carte de crédit, le piratage, les faiblesses de la sécurité et autres menaces. La norme définit 12 exigences auxquelles les commerçants et les fournisseurs de services stockant, traitant ou transmettant des données de titulaire de carte doivent se conformer.

L'un des plus grands défis auxquels les entreprises doivent faire face dans leurs efforts de mise en conformité à la norme PCI DSS est la section 10.2.1 qui leur exige « d'installer des pistes d'audit automatisées pour tous les composants du système afin de reconstituer tous les accès d'un utilisateur individuel aux données d'un titulaire de carte. » Par ailleurs, la section 10.2.2 exige que « toutes les actions effectuées par une personne jouissant d'avantages de base ou administratifs » soit incluses dans le journal. Se conformer à ces exigences constitue une tâche complexe car la plupart des applications, patrimoniales et modernes, ne disposent pas de mécanismes d'enregistrement dans les journaux qui leur permettent de reconstituer des événements d'accès d'utilisateur à des données de titulaire de carte. De même, lorsque de tels journaux existent, ils comportent uniquement des actions de mise à jour et non des interrogations d'utilisateur et autres actions en lecture seule.

Le développement d'une solution interne pour répondre à ces exigences peut réclamer d'immenses efforts car des milliers de programmes d'application de ces entreprises risquent de devoir être modifiés. Toute solution suivant l'accès aux bases de données de l'entreprise n'est pas envisageable pour deux raisons : elle ne ferait le suivi que des actions de « mise à jour » effectuées dans la base de données et elle ne couvrirait pas les actions « lues ». Par ailleurs, dans la majorité des cas, l'utilisateur concerné n'est pas capturé car nombre d'applications utilisent un identifiant d'utilisateur générique pour l'accès à la base de données. L'agrégation du journal est une solution parfois envisagée. Ce type de solution peut aider les entreprises à se conformer aux exigences de la DSS mais il se fie aux données fournies par les journaux existants et ces journaux ne disposent pas de données suffisantes pour que l'agrégation du journal permette la conformité à la section 10.2.

La solution Intellinx

Intellinx est une révolution dans la détection et la prévention des menaces internes grâce à sa solution prête à l'emploi pour la conformité aux exigences 10.2.1 et 10.2.2 de la norme DSS, en générant automatiquement une piste d'audit complète avec une relecture visuelle des écrans et des frappes de touche d'utilisateur, dans toutes les applications des plates-formes principales. La piste d'audit comprend à la fois des actions de mise à jour et des actions en lecture seule, pour les utilisateurs finaux, réguliers et privilégiés.

Grâce à sa solution novatrice pour les agents de sécurité et les auditeurs internes, Intellinx propose une visibilité inégalée de l'activité de l'utilisateur final en permettant d'aller au-delà des exigences de la DSS. Les règles de fraude configurables suivent les modèles comportementaux de l'utilisateur au niveau de l'écran d'application, générant ainsi des alertes sur les exceptions, en temps réel, et permettant à l'auditeur interne de localiser immédiatement les suspects. La technologie en instance de brevet d'Intellinx propose une solution sans agent, basée sur le reniflage des transmissions réseau, sans encombrement ni temps d'inactivité.

La valeur métier d'Intellinx

- Conformité à la norme PCI DSS, sections 10.2.1 et 10.2.2 et solution prête à l'emploi.
- Diminution des pertes liées aux fraudes internes et autre activité malveillante en temps réel (l'ACFE estime que les entreprises américaines perdent en moyenne 5 % de leurs revenus en raison des fraudes internes).
- Solution visant à décourager les utilisateurs frauduleux potentiels en les informant simplement que leurs actions seront enregistrées.
- Renforcement de l'efficacité de la sécurité de l'information en lançant une alerte à la détection d'un comportement suspect et en procurant une visibilité complète aux agents de sécurité de toutes les actions de chaque utilisateur final suspect donné, comme s'ils regardaient par-dessus son épaule.
- Amélioration de l'efficacité de l'audit interne en permettant des enquêtes sur tout événement s'étant produit dans le passé en recherchant, par exemple, les utilisateurs qui ont eu accès à un compte client particulier, pendant une période donnée, sur toutes les applications internes de l'entreprise.
- Réduction du temps de solution (« Time to value » accéléré) - Fonctionnalité prête à l'emploi d'enregistrement/de lecture/de recherche avec génération automatique de piste d'audit légale.