SÉCURITÉ DES CLIENTS LÉGERS ET DES SYSTÈMES EMBARQUÉS KASPERSKY LAB

Comparaison avec la norme PCI DSS v3.1

La norme PCI DSS 3.1 réglemente de nombreuses exigences en matière de sécurité technique et de paramètres de systèmes utilisant les données de carte de crédit. Les sous-sections 5.1, 5.1.1, 5.2, 5.3 et 6.2 de la norme PCI DSS v3.1 prévoient la réglementation stricte de la protection antivirus liée aux nœuds finaux fonctionnant avec les données détaillées du titulaire d'une carte. Il est fréquent, même si cela ne constitue pas une règle officielle, que les fonctions de contrôle des appareils et de contrôle d'applications soient considérés comme relevant également de l'audit du logiciel antivirus de la norme PCI DSS.

5.1

Exigences de la norme PCI DSS :

Déployer des logiciels antivirus sur tous les systèmes régulièrement affectés par des logiciels malveillants (en particulier PC et serveurs).

Procédures de test :

Sur un échantillon de composants du système comprenant tous les types de systèmes d'exploitation généralement affectés par des logiciels malveillants, vérifier que des logiciels antivirus sont déployés et, le cas échéant, qu'une technologie de protection antivirus est en place.

Directives :

Les systèmes normalement sécurisés sont l'objet d'attaques constantes utilisant les codes d'exploitation largement publiés, souvent de type « jour zéro » (une attaque exploitant des vulnérabilités inconnues jusqu'à présent). En l'absence de solution antivirus régulièrement mise à jour, ces nouvelles formes de logiciel malveillant peuvent attaquer les systèmes et désactiver un réseau ou compromettre les données.

5.1.1

Exigences de la norme PCI DSS :

S'assurer que tous les programmes anti-virus sont capables de détecter et d'éliminer tous les types de logiciel malveillant connus, et d'assurer une protection efficace.

Procédures de test :

Examiner la documentation du fournisseur et les configurations d'anti-virus pour vérifier que les programmes d'anti-virus détectent tous les types de logiciel malveillant connus, éliminent tous les types de logiciel malveillant connus et protègent contre tous les types de logiciel malveillant connus.

Directives :

Il est important de se protéger contre TOUS les types et toutes les formes de programmes malveillants.

5.2

Exigences de la norme PCI DSS :

S'assurer que tous les mécanismes antivirus sont maintenus à jour, effectuent régulièrement des scans et génèrent des journaux d'audit qui sont conservés selon la condition 10.7 de la norme PCI DSS.

Procédures de test :

5.2.a Examiner les politiques et les procédures pour vérifier que les logiciels antivirus et les définitions d'anti-virus sont maintenus à jour.

5.2.b Examiner les configurations anti-virus, y compris l'installation du logiciel maître, pour vérifier que les mécanismes anti-virus sont configurés pour effectuer automatiquement les mises à jour et pour effectuer régulièrement des scans.

5.2.c Examiner un échantillon de composants du système, y compris tous les types de systèmes d'exploitation généralement affectés par des logiciels malveillants, pour vérifier que le logiciel anti-virus et les définitions sont à jour et que des scans sont effectués régulièrement.

5.2.d Examiner les configurations anti-virus, y compris l'installation du logiciel maître et un échantillon des composants du système pour vérifier que la production de journaux de logiciel anti-virus est activée et les journaux sont conservés conformément à la condition 10.7 de la norme PCI DSS.

Directives :

Même les meilleures solutions anti-virus sont limitées du point de vue de l'efficacité si elles ne sont pas maintenues et mises à jour avec les dernières mises à jour de sécurité, fichiers de signature ou protection contre les logiciels malveillants.

Les journaux d'audit permettent de surveiller l'activité des virus et des logiciels malveillants, ainsi que les réactions contre les logiciels malveillants. Par conséquent, il est impératif que la solution antivirus soit configurée pour générer des journaux d'audit et gérer ces derniers conformément à la condition 10.

5.3

Exigences de la norme PCI DSS :

S'assurer que les mécanismes anti-virus fonctionnent de manière active et ne peuvent pas être désactivés ou altérés par les utilisateurs, sauf autorisation spécifique de la direction au cas par cas, sur une base limitée dans le temps.

Procédures de test :

5.3.a Examiner les configurations anti-virus, y compris l'installation du logiciel maître et un échantillon des composants du système pour vérifier que le logiciel anti-virus fonctionne activement.
5.3.b Examiner les configurations anti-virus, y compris l'installation du logiciel maître et un échantillon des composants du système pour vérifier que le logiciel anti-virus ne peut pas être désactivé ou altéré par les utilisateurs.
5.3.c Interroger le personnel responsable et observer les processus pour vérifier que les logiciels anti-virus ne peuvent pas être désactivés ou altérés par les utilisateurs, sauf autorisation spécifique de la direction au cas par cas, sur une base limitée dans le temps.

Directives :

Un anti-virus qui fonctionne continuellement et qui ne peut pas être altéré offrira une sécurité persistante contre les logiciels malveillants.
L'utilisation de contrôles basés sur une politique sur tous les systèmes pour assurer que les protections contre les logiciels malveillants ne puissent pas être altérées ou désactivées aidera à empêcher que les faiblesses du système ne soient exploitées par les logiciels malveillants.
Des mesures de sécurité supplémentaires peuvent également être mises en oeuvre pour la période pendant laquelle la protection anti-virus n'est pas active, par exemple déconnecter le système sans protection d'Internet lorsque la protection anti-virus est désactivée, et effectuer un scan complet une fois qu'elle est réactivée.

6.2

Exigensces de la norme PCI DSS :

S'assurer que tous les logiciels et les composants du système sont protégés de vulnérabilités connues en installant les correctifs de sécurité applicables fournis par le fournisseur. Installer les correctifs de sécurité stratégiques dans le mois qui suit leur commercialisation.
Remarque : *les correctifs de sécurité critiques doivent être identifiés selon le processus de classement des risques défini par la condition 6.1*

Procédures de test :

6.2.a Examiner les politiques et procédures relatives à l'installation des correctifs de sécurité pour vérifier que les processus sont définis pour installer les correctifs de sécurité critiques pertinents fournis par le fournisseur dans le mois qui suit leur commercialisation et installer tous les correctifs de sécurité critiques pertinents fournis par le fournisseur dans un délai acceptable (par exemple, dans les trois mois).
6.2.b Pour un échantillon de composants du système et de logiciels associés, comparer la liste des correctifs de sécurité installés sur chaque système avec la liste des correctifs de sécurité les plus récents du fournisseur, pour vérifier que les correctifs de sécurité critiques pertinents fournis par le fournisseur sont installés dans le mois qui suit leur commercialisation et que tous les correctifs de sécurité critiques pertinents fournis par le fournisseur sont installés dans un délai acceptable (par exemple, dans les trois mois).

Directives :

Les systèmes normalement sécurisés sont l'objet d'attaques constantes utilisant les codes d'exploitation largement publiés, souvent de type « jour zéro » (une attaque exploitant des vulnérabilités inconnues jusqu'à présent). Si les correctifs les plus récents ne sont pas mis en œuvre dès que possible sur les systèmes critiques, un individu malveillant pourrait exploiter cette faiblesse pour attaquer ou désactiver un système, ou pour accéder à des données sensibles.
Établir une priorité des correctifs pour l'infrastructure critique garantit que les systèmes et les dispositifs de haute priorité sont protégés des vulnérabilités aussi tôt que possible après la commercialisation d'un correctif. Envisager de donner la priorité à l'installation de correctifs, de sorte que les correctifs de sécurité pour les systèmes critiques ou à risque soient installés dans les 30 jours et les correctifs de sécurité moins critiques dans les 2-3 mois.
Cette condition s'applique à tous les correctifs applicables pour tous les logiciels installés.

OPTIMISATION DE L'EFFICACITÉ - GESTION INTÉGRÉE

Kaspersky Embedded Systems Security offre à vos équipes de sécurité une visibilité totale et un contrôle intégral de chaque terminal.
Grâce à son évolutivité, la solution permet d'effectuer et d'accéder à l'inventaire, la gestion des licences, la connexion et le dépannage à distance depuis une seule et même console d'administration : Kaspersky Security Center.
Le spécialiste de la sécurité peut gérer tous les agents par le biais d'une console locale, une fonction très utile pour vos distributeurs automatiques de billets et vos terminaux de points de vente, des réseaux segmentés et isolés.

MAINTENANCE ET ASSISTANCE

Nous intervenons 24 h sur 24, 7 jours sur 7 et 365 jours par an dans plus de 200 pays, à partir de nos 34 agences réparties dans le monde entier dans le cadre des offres d'assistance de notre contrat de maintenance et d'entretien (MSA).
Nos services professionnels restent à l'écoute pour vous garantir de profiter au maximum des avantages de votre installation de sécurité Kaspersky Lab.

Pour en savoir plus sur la protection efficace de vos terminaux, contactez l'équipe commerciale Kaspersky Lab chargée des entreprises.

KASPERSKY lab