

...ÊTRE EN CONFORMITÉ AVEC LA NORME ICP

À la fin du mois de décembre 2007, toute entreprise acceptant des transactions par carte de paiement devra être en conformité avec la norme de sécurité des données ICP (Industrie des Cartes de Paiement). Créée pour répondre au problème grandissant des enfreintes à la sécurité qui ont valu à des milliers de consommateurs le vol ou la corruption des informations de leurs cartes, cette norme est le fruit de la collaboration entre les géants de l'industrie de la carte de paiement, comme MasterCard et Visa, ayant abouti à la création d'une série de règles communes en matière de sécurité.

La norme exige que les entreprises développent et mettent en place des politiques de sécurité assurant une gestion sécurisée des données des cartes de crédit et un contrôle d'accès des réseaux vers lesquels sont envoyées les informations concernant les titulaires de cartes. Le non respect de la norme entraînera des amendes substantielles et une possible exclusion permanente des programmes de paiement par carte. Si vous acceptez les paiements par carte, si vous recevez, traitez ou conservez des informations de transactions par carte, les étapes simples ci-dessous vous aideront à respecter la norme ICP.



1 Établir et maintenir un réseau sécurisé

Exigences ICP 1 et 2

Le contrôle d'accès réseau est essentiel pour assurer la sécurité des données des titulaires de carte de paiement. Des pare-feu réseaux et personnels administrés de manière centralisée doivent être configurés pour arrêter le trafic entrant et sortant qui pourrait compromettre votre sécurité. Grâce aux solutions de contrôle d'accès réseau (NAC), vous êtes sûr que les ordinateurs invités appartenant, par exemple, à des sous-traitants, auront uniquement accès à votre réseau s'ils disposent du pare-feu approuvé par votre entreprise et que celui-ci est actif.

En plus du contrôle du réseau et de la connexion Internet, vous devez aussi sécuriser les ordinateurs individuels en adoptant des normes industrielles strictes qui vous permettront de garantir que les systèmes sont verrouillés suite à une certaine période d'inactivité et d'appliquer des méthodes d'utilisation des mots de passe plus sécurisées. Assurez-vous que des mots de passe forts sont utilisés et changés régulièrement et que les anciens mots de passe sont refusés. NAC peut aussi être utilisé pour créer des politiques de sécurité et vérifier la conformité grâce à de nombreuses mesures de sécurité. Il peut aussi interdire aux ordinateurs non conformes d'accéder aux ressources vitales de l'entreprise.

2 Protéger les données des titulaires de carte

Exigences ICP 3 et 4

Seules les personnes autorisées doivent avoir accès aux données des cartes de crédit et, lorsque possible, le numéro des cartes doit être masqué afin que seule une partie du numéro soit visible. Les informations concernant les titulaires de carte conservées sur le disque dur doivent être cryptées afin de ne pas pouvoir être lues en cas de perte ou de vol de l'ordinateur. Définissez des politiques de transmission sécurisée des informations de cartes de crédit et faites en sorte que seules les données cryptées soient envoyées par courriel sur un réseau public. Assurez-vous que la politique de sécurité de votre passerelle de messagerie bloque les courriels contenant des données de titulaires de carte non cryptées.

La perte de données sensibles peut aussi être empêchée en verrouillant les ports afin de, par exemple, désactiver la connexion sans fil, et en interdisant l'utilisation de clés USB ou de tout autre appareil de stockage de mémoire de masse.

3 Maintenir un programme de gestion de la vulnérabilité

Exigences ICP 5 et 6

Installez un logiciel de sécurité sur tous les ordinateurs de l'entreprise et assurez-vous qu'il est entièrement mis à jour. De solides politiques de sécurité centralisées pour des contrôles planifiés et sur accès efficaces et pour une bonne administration des correctifs de sécurité sur tous les systèmes de développement, de test et de production vous procureront une visibilité et un contrôle total du réseau. Vos politiques de sécurité doivent permettre l'activation du service de mise à jour des correctifs de Microsoft sur toutes les machines Windows. Conjointement à l'utilisation des pare-feu personnels, une solution NAC vous garantira que l'accès à votre réseau sera uniquement autorisé aux ordinateurs invités disposant d'un logiciel antivirus, mis à jour, actif et approuvé par votre entreprise. Elle vous permettra aussi de vérifier l'état des correctifs sur les ordinateurs et de mettre en quarantaine tout ceux qui ne sont pas conformes à votre politique de sécurité. Idéalement, la solution devrait inclure une source de données identifiant tous les correctifs critiques et importants et effectuer une vérification contextuelle des correctifs correspondant à un ordinateur donné. La passerelle web doit aussi être incluse à tout programme de gestion des vulnérabilités afin de bloquer le téléchargement Internet de malwares sur les ordinateurs.

4 Mettre en place de solides mesures de contrôle de l'accès

Exigences ICP 7, 8 et 9

L'utilisation d'un logiciel d'accès à distance ou peer-to-peer doit être bloquée sauf si nécessaire à l'entreprise, en effet, une telle utilisation comporte des risques. En cas d'utilisation, chaque ordinateur doit utiliser un nom utilisateur et un mot de passe unique et le cryptage et toutes autres fonctions de sécurité doivent être activés. Choisissez un éditeur de sécurité capable d'identifier ces applications potentiellement indésirables et d'empêcher leur utilisation par des utilisateurs non autorisés.

Utilisez une solution NAC pour interdire aux utilisateurs non autorisés d'accéder aux ordinateurs et serveurs sur lesquels sont archivées les données des titulaires de carte. Utilisez un mécanisme qui bloque l'accès au commutateur réseau à l'aide du protocole 802.1x ou qui empêche l'utilisateur de récupérer une adresse IP valide à l'aide de DHCP. L'accès sans fil des invités ou partenaires commerciaux doit être restreint et tout ordinateur non conforme à votre politique de contrôle d'accès réseau doit être mis en quarantaine. Tout accès physique non autorisé aux équipements et supports contenant les données des titulaires de carte doit être restreint de manière appropriée.

5 Surveiller et tester régulièrement les réseaux

Exigences ICP 10 et 11

À présent que vous avez installé un logiciel antimalware et un système de prévention des intrusions pour protéger votre réseau et vos ordinateurs contre les menaces du jour zéro, il est vital de procéder à la surveillance et au test de bon fonctionnement. De même que vous effectuez une vérification continue des failles sur tous les systèmes du réseau, vous devriez aussi conserver une trace de toutes les tentatives d'accès – fructueuses ou infructueuses – pendant au moins trois mois. Le choix d'une solution de sécurité pour systèmes d'extrémité qui intègre la prévention des intrusions sur l'hôte et d'une solution de contrôle d'accès réseau qui garantit l'installation, le bon fonctionnement et la mise à jour de votre protection faciliteront la procédure de test.

6 Maintenir une politique de sécurité de l'information

Exigence ICP 12

Une conformité efficace à la norme de sécurité des données ICP (PCI DSS) exige la création et la maintenance de toute une série de processus et de mesures de sécurité pour les employés et les invités dans le cadre d'une politique complète de sécurité des informations des titulaires de carte. Les mesures de sécurité du présent guide sont un excellent point de départ.

Sophos NAC Advanced et Sophos Enterprise Security and Control vous offre la protection, l'automatisation et le savoir-faire dont vous avez besoin pour protéger votre entreprise 24h/24. Pour en savoir plus sur les produits Sophos et les évaluer, veuillez vous rendre sur www.sophos.fr.

LA NORME ICP

- 1 Installer et maintenir une configuration pare-feu pour protéger les données des titulaires de carte
- 2 Ne pas utiliser les paramètres par défaut de l'éditeur pour les mots de passe système et autres paramètres de sécurité
- 3 Protéger les archives de données des titulaires de carte
- 4 Crypter la transmission des données des titulaires de carte sur des réseaux publics
- 5 Utiliser et régulièrement mettre à jour le logiciel antivirus
- 6 Développer et maintenir des systèmes et des applications sécurisés
- 7 Restreindre l'accès des données des titulaires de carte aux personnes qui ont besoin de les connaître
- 8 Attribuer un code d'utilisateur exclusif à chaque personne ayant accès à l'ordinateur
- 9 Restreindre l'accès physique aux données des titulaires de carte
- 10 Assurer un suivi et une surveillance de tout accès aux ressources du réseau et aux données des titulaires de carte
- 11 Tester régulièrement les systèmes et les processus de sécurité
- 12 Maintenir une politique en matière de sécurité de l'information

Sophos est l'un des plus grands éditeurs mondiaux de solutions de sécurité et de contrôle informatiques. Nous offrons une protection et un contrôle complets aux entreprises et aux organisations éducatives et gouvernementales en assurant leur défense contre les malwares connus et inconnus, les spywares, les intrusions, les applications indésirables, le spam et les violations de politiques de sécurité, tout en leur assurant un contrôle d'accès réseau complet (NAC). Fiables et simples à utiliser, nos produits protègent plus de 100 millions d'utilisateurs dans plus de 150 pays. Nos 20 ans d'expérience et notre réseau international de centres d'analyse des menaces nous permettent de répondre rapidement aux menaces émergentes et d'atteindre les niveaux de satisfaction clientèle les plus élevés du secteur. Sophos est une société internationale siégeant à Boston aux États-Unis et à Oxford au Royaume-Uni.

Boston, EU • Mayence, Allemagne • Milan, Italie • Oxford, RU • Paris, France
Singapour • Sydney, Australie • Vancouver, Canada • Yokohama, Japon

© Copyright 2007. Sophos Plc. Tous droits réservés. Toutes les autres marques appartiennent à leurs propriétaires respectifs.

fo/071025

SOPHOS
secured.