

...EL CUMPLIMIENTO DEL ESTÁNDAR PCI

A partir de diciembre de 2007, cualquier organización que acepte pagos mediante tarjeta deberá cumplir con el estándar de seguridad de datos PCI (Payment Card Industry). Este estándar ha sido elaborado de forma conjunta por las principales empresas de pago con tarjeta, incluidas MasterCard y Visa, para poner fin a las frecuentes brechas de seguridad que afectan a los datos de miles de usuarios de tarjetas de crédito.

Mediante este estándar se pretende imponer una serie de políticas y medidas de seguridad que aseguren la privacidad de las transacciones de pago, así como el almacenamiento de estos datos. Cualquier empresa que no cumpla con los mínimos de seguridad establecidos podrán enfrentarse a cuantiosas multas e incluso a la expulsión de los programas de pago por tarjeta. Siga estos sencillos pasos para asegurarse el cumplimiento del estándar de seguridad de datos PCI.



1 Cree y mantenga una red segura

Requisitos PCI 1 y 2

El control del acceso a la red es fundamental para garantizar la seguridad de los datos. El cortafuegos de la red, así como cortafuegos personales, deberían detener el tráfico de entrada y de salida que no es necesario para su negocio. Mediante una solución de control de acceso a la red (NAC) podrá verificar que los ordenadores invitados en su empresa, por ejemplo de algún representante, disponen de una protección actualizada.

Además de controlar la conectividad a su red y a Internet, también deberá proteger cada ordenador, por ejemplo cerrando la sesión de forma automática tras un período de inactividad e imponiendo una política de contraseñas. Dichas contraseñas deberían ser seguras, cambiarse con frecuencia y no repetirse. Las soluciones NAC permiten crear políticas de seguridad para verificar el estado de cada ordenador en la red y evitar la entrada de ordenadores infractores.

2 Proteja los datos de tarjetas de crédito

Requisitos PCI 3 y 4

Sólo personas autorizadas deberían tener acceso a los datos almacenados de tarjetas de crédito, y siempre que sea posible se mostrará sólo parte del número. La información en los discos de almacenamiento debería estar encriptada, de manera que los datos serían ilegibles en el caso de robo. Debe introducir políticas seguras para la transmisión de datos de tarjetas de crédito y utilizar mensajes cifrados en redes públicas. Su pasarela de correo debería bloquear mensajes no encriptados que contengan datos confidenciales.

La pérdida de este tipo de datos también puede prevenirse cerrando puertos que no se utilizan, por ejemplo desactivando la conectividad inalámbrica, y bloqueando el uso de dispositivos de almacenamiento USB.

3 Disponga de un seguimiento de vulnerabilidades

Requisitos PCI 5 y 6

Debe disponer de programas de seguridad en todos los ordenadores de la empresa y asegurarse de que se mantienen actualizados. Mediante un sistema de políticas centralizadas podrá garantizar la disponibilidad del escaneado en acceso en cada ordenador y controlar los parches de seguridad necesarios para cada sistema en su red. En el caso de ordenadores con Windows, tendrá que tener siempre activo el servicio de actualización de Microsoft. Una solución NAC comprobará cada equipo que se conecta a la red y sólo permitirá el acceso a aquellos que cumplen con las normas antivirus y cortafuegos establecidas. También le permitirá verificar los parches instalados y ofrecer los que faltan desde un área de cuarentena. Del mismo modo, la pasarela de acceso a Internet tendrá que incluirse en el programa de seguimiento de vulnerabilidades para evitar la descarga de programas maliciosos desde las estaciones de trabajo.

4 Realice un exhaustivo control de acceso

Requisitos PCI 7, 8 y 9

Deberá prohibir el uso de programas de conexión remota por los riesgos que conllevan. Si su empresa *requiere* el uso de este tipo de programas, cada ordenador debería contar con sus propias credenciales de acceso, usar encriptado y tener activadas otras opciones de seguridad. Elija un fabricante de seguridad que sea capaz de identificar y bloquear aplicaciones no deseadas.

Utilice una solución NAC para evitar el acceso no autorizado a cualquier ordenador o servidor en los que almacene datos de tarjetas de crédito. Utilice algún mecanismo de control para bloquear conexiones 802.1x o que impida la obtención de direcciones IP desde el servidor DHCP. El acceso inalámbrico por parte de invitados o contratistas debe estar controlado de manera que los ordenadores que no cumplan con la política de seguridad interna quedarán en cuarentena. Todos los equipos que contengan datos de tarjetas de crédito deben estar en una sala de acceso restringido.

5 Monitorice y verifique el estado de su red

Requisitos PCI 10 y 11

Una vez instalados los sistemas de protección y prevención de intrusiones en toda la red, es muy importante que verifique el estado de funcionamiento de los mismos. Además de revisar las vulnerabilidades de cada sistema, deberá también mantener un registro con *todas* las peticiones de acceso – satisfactorias y fallidas – durante los últimos tres meses. La integración de un producto de seguridad que incluya protección contra intrusiones y una solución NAC que compruebe de forma continua su estado y actualización le facilitarán enormemente las tareas de monitorización y verificación.

6 Redacte una política de seguridad interna

Requisito PCI 12

El estándar de seguridad de datos PCI requiere la creación de políticas detalladas de seguridad para empleados e invitados. Las medidas de seguridad descritas en este documento le pueden servir de guía.

ESTÁNDAR DE SEGURIDAD DE DATOS PCI

- 1 Disponer de un cortafuegos para proteger datos de tarjetas de crédito
- 2 No utilizar las credenciales predeterminadas en los diferentes parámetros de seguridad
- 3 Proteger los datos almacenados de tarjetas de crédito
- 4 Encriptar la transmisión de datos a través de redes públicas
- 5 Disponer de protección antivirus actualizada
- 6 Desarrollar y mantener sistemas y aplicaciones seguras
- 7 Restringir al máximo el acceso a los datos de tarjetas de crédito
- 8 Asignar un identificador único a cada usuario con acceso
- 9 Restringir de forma física el acceso a los sistemas con datos de tarjetas de crédito
- 10 Controlar el acceso a los recursos de la red y a los datos de tarjetas de crédito
- 11 Comprobar con frecuencia la seguridad de sistemas y procesos
- 12 Redactar una política de seguridad interna

Sophos NAC Advanced y Sophos Enterprise Security and Control ofrecen la mejor protección y asistencia las 24 horas del día. Para más información sobre los productos de Sophos, visite www.esp.sophos.com.

Sophos es un líder mundial en seguridad y control de sistemas informáticos. Ofrecemos protección completa para empresas, educación y gobiernos: defensa contra programas malintencionados, intrusión, programas espía, aplicaciones no deseadas, spam y abuso de políticas internas, además de control de acceso a la red (NAC). Nuestros productos, caracterizados por su gran precisión y facilidad de uso, protegen a más de 100 millones de usuarios en más de 150 países. Con más de 20 años de experiencia y una red global de centros de análisis de amenazas, respondemos rápidamente ante amenazas emergentes y mantenemos el más alto nivel de satisfacción del cliente.

Boston, EE.UU. • Mainz, Alemania • Milán, Italia • Oxford, GB • París, Francia
Singapur • Sydney, Australia • Vancouver, Canadá • Yokohama, Japón

© Copyright 2007. Sophos Plc. Todos los derechos reservados. Otras marcas registradas por sus propietarios.

fo/071025

SOPHOS
secured.