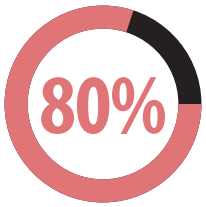
FUNDAMENTOS DE LA SEGURIDAD DE DATOS DE PAGO

Parche

¿CUÁL ES EL RIESGO?



de los hackeos podría ser prevenido fortaleciendo contraseñas y instalando parches del software

(Informe de investigación de Verizon sobre vulnerabilidad de datos de 2017)

El software sin parches es una de las causas principales de compromiso de datos de los negocios.

A menudo, el software tiene defectos o errores que cometieron los programadores cuando escribieron el código. Los proveedores, con frecuencia, emiten actualizaciones, conocidas como parches, para solucionar estas vulnerabilidades del software. Cuando las empresas no aplican los parches del software de los proveedores, los hackers aprovechan estas vulnerabilidades para irrumpir en sus computadoras y sistemas, y robar los datos de pago.

PRÁCTICAS RECOMENDADAS PARA APLICAR LOS PARCHES

La instalación oportuna de parches de seguridad es esencial para minimizar el riesgo de una vulnerabilidad de datos. Para aplicar los parches con rapidez, es importante que conozca la forma en que su software se actualiza con regularidad con estos parches y quién es responsable de ello (¡podría ser usted!).

Identifique qué proveedores le envían parches

El recurso de preguntas que debe hacer a sus proveedores puede ayudar a las empresas a identificar qué proveedores les envían parches, incluyendo proveedores de su terminal de pagos, aplicaciones de pagos, otros sistemas de pagos (cajas registradoras, registradoras de efectivo, PC, etc.), sistemas operativos (Android, Windows, iOS, etc.), aplicaciones (incluyendo su navegador web) y software de negocios.

Hable con sus proveedores sobre los parches

Asegúrese de que sus proveedores actualicen sus terminales de pago, sistemas operativos, etc., de forman que puedan darle soporte a los parches de seguridad más recientes. Pregúnteles la forma en que se añaden los parches (algunos se instalan en forma automática cuando están disponibles) y quién es responsable de ello. Averigüe cómo le notificarán sobre los nuevos parches de seguridad, y asegúrese de recibir y leer tales avisos.

Instale los parches

Siga las instrucciones de sus proveedores e instale los parches a la brevedad posible.

No ignore el comercio electrónico

Las empresas de comercio electrónico deberían estar atentas a los parches de su proveedor de servicios de pago. Pregunte a su proveedor de hosting de comercio electrónico si emite parches para su sistema (y con qué frecuencia). Asegúrese de actualizar el sistema operativo, la plataforma de comercio electrónico y/o aplicación web para que sean compatibles con los parches más recientes.

RECURSOS

Visite **pcissc.org/Merchants** donde encontrará más recursos

El recurso de preguntas que debe hacer a sus proveedores puede ayudar a las empresas a identificar qué proveedores les envían parches.

La Guía de pagos seguros proporciona a las empresas la información básica para protegerse contra el robo de datos de pago.

Vea este video rápido animado para que conozca la forma en que las empresas pueden minimizar las posibilidades de una vulnerabilidad a sus datos instalando los parches con rapidez.

Las herramientas de detección de vulnerabilidades proporcionadas por los proveedores de detección aprobados por PCI también pueden ayudar a las empresas a buscar de forma automática sus redes para descubrir las vulnerabilidades e informar cuando se requiera aplicar algún parche.

La lista de integradores calificados de PCI y revendedores (QIR) es un recurso que las empresas pueden aprovechar para encontrar instaladores de servicios de pago que hayan recibido capacitación del PCI Security Standards Council sobre parches y otros fundamentos de seguridad de datos de pago.

PCI Security Standards Council