21/12/2019

E-skimming, qué es y cómo proteger tu tienda contra esta técnica maliciosa



Uno de los principales negocios de los ciberdelincuentes es la venta de información confidencial robada, como datos personales o credenciales de acceso. Dentro de toda esa información sustraída ilícitamente, mediante técnicas fraudulentas como el phishing o campañas de malware, una de la que más beneficios genera es la venta de información bancaría de tarjetas de crédito y débito.

Tradicionalmente, el robo de tarjetas de crédito o skimming se hacía directamente en los cajeros automáticos. Los delincuentes utilizando diferentes dispositivos clonan las tarjetas y roban el código PIN. Este tipo de fraude ha pasado del mundo offline al digital dando como resultado el denominado e-skimming.

El FBI (Federal Bureau of Investigation) de los EE.UU. ha publicado una alerta avisando del incremento de campañas maliciosas cuyo objetivo es robar datos bancarios e información personal de los clientes que realizan compras por Internet, principalmente, en pequeños y medianos comercios.

¿Qué es el e-skimming y cómo lo llevan a cabo?

El **e-skimming o web skimming es una técnica utilizada por ciberdelincuentes para obtener información bancaria y personal de tiendas online legítimas** que posteriormente será vendida en el mercado negro, o utilizada directamente por los ciberdelincuentes en su propio beneficio.

El primer paso que deben llevar a cabo los ciberdelincuentes consiste en obtener acceso a la tienda online, para ello se suelen valer de **vulnerabilidades no parcheadas en el gestor de contenidos o mediante campañas de phishing.** Una vez han conseguido acceso a la tienda, modifican parte de su código fuente para que, cuando el cliente introduce información personal o bancaria, sea enviada al banco y también robada. De esta forma, tanto el cliente como el comercio no son conscientes del robo, ya que el pago es correcto, sin embargo, toda esa información ya está en manos de los ciberdelincuentes.

Este tipo de técnica afecta, principalmente, a aquellos comercios online cuya **pasarela de pago está integrada dentro de la propia tienda**, ya que toda la información bancaria es gestionada internamente. Las tiendas online que utilizan una **pasarela de pago de un tercero tampoco están libres de riesgo**, ya que, aunque los datos de la tarjeta no son gestionados por el comercio, la información personal de los clientes puede ser sustraída igualmente.

¿Cómo prevenir el e-skimming?

Para reducir el riesgo de que la tienda se vea afectada por esta técnica maliciosa se deben seguir las recomendaciones de seguridad que se describen a continuación.

Software actualizado

Todo el software utilizado en la empresa debe estar actualizado a la última versión disponible. Esta premisa se aplica también al gestor de contenidos utilizado para el comercio electrónico, el servidor que lo aloja y todo el software que tenga instalado, de esta manera, los ciberdelincuentes no podrán valerse de vulnerabilidades conocidas para obtener acceso.

Además, antes de realizar cualquier actualización de software en los entornos de producción, es recomendable realizar, previamente, las pruebas en entornos de preproducción, para comprobar que todo funciona correctamente tras la actualización.

Credenciales de acceso robustas

Es importante que las credenciales de acceso al e-commerce sean robustas, ya que una de las maneras que tienen los ciberdelincuentes de conseguir acceso a la tienda es por medio de ataques automatizados, probando distintas combinaciones de usuarios y contraseñas mediante técnicas de fuerza bruta. Utilizando nombres de usuario no comunes y contraseñas robustas se reduce, en gran medida, la posibilidad de que un ciberdelincuente consiga acceso a la web.

En caso de ser posible, se debe habilitar un doble factor de autenticación para el acceso al panel de administración de la tienda, así en caso de que un ciberdelincuente consiga las credenciales de acceso no podrá completar el proceso de inicio de sesión al desconocer el segundo factor de autenticación.

Concienciación

La concienciación siempre es uno de los aspectos más importantes en la ciberseguridad de una empresa, ya que los usuarios son el eslabón más importante. Cuando un usuario está concienciado con la ciberseguridad es menos probable que realice acciones que puedan comprometer la seguridad de la organización como caer en un phishing, ejecutar archivos potencialmente maliciosos o utilizar credenciales de acceso inseguras. Por ello, desde INCIBE ponemos a disposición de los empresarios un kit de concienciación con el que mejorar la ciberseguridad de la empresa desde el corazón de la misma, los empleados.

Segmentar la red

Aunque esta técnica no reduce directamente el riesgo de sufrir un incidente de seguridad relacionado con el e-skimming, minimiza los riesgos de que otras partes de la red de la organización se vean afectadas por un incidente que afecte a la tienda. Cuando la red de la empresa cuanta con un servidor propio donde está alojado el e-commerce, siempre se debe ubicar en una zona desmilitarizada o DMZ. Así, aunque un ciberdelincuente consiga acceso a la tienda o al servidor que la aloja, no podrá acceder fácilmente al resto de la red de la empresa, con el consiguiente riesgo para la seguridad de la información que esto supondría.

Cómo mantener la integridad de la web

Los comercios online tienen la posibilidad de ofrecer diferentes métodos de pago a sus clientes, siendo uno de ellos la tarjeta de crédito o débito. Para poder aceptar pagos por este medio, los comercios deben disponer de una pasarela de pago, bien sea integrada dentro de la propia tienda, bien externalizada en un tercero de confianza, como puede ser una entidad bancaria.

Integridad del código fuente de la tienda

Para robar información personal como la de tarjetas de crédito mediante e-skimming, los ciberdelincuentes utilizan dos vías principales: modificar el código de algún archivo existente de la tienda o hacer que esta cargue archivos maliciosos de otras fuentes. Para proteger la tienda de estas dos técnicas se han de habilitar y configurar dos estándares de seguridad. Esta parte requiere conocimientos técnicos, por lo que siempre es recomendable contar con la ayuda de un profesional:

- CSP o Content Security Policy, mecanismo por el cual solamente se permite cargar archivos de fuentes previamente autorizadas. Así, los ciberdelincuentes no podrán ejecutar código malicioso procedente de sitios no autorizados.

- SRI o Subresource Integrity, mecanismo por el cual no se permite ejecutar archivos modificados sin permiso, evitando así que si los ciberdelincuentes puedan ejecutar código malicioso que se encuentre dentro de archivos legítimos.
- Contratar los servicios de un proveedor de seguridad externo también ayudará a reducir los riesgos de sufrir un incidente de seguridad, ya que este tipo de servicios velan por la seguridad de sus clientes.

Pasarela de pago de un tercero

Una alternativa para aquellas tiendas que no desean gestionar ninguna información bancaria de sus clientes, y por lo tanto reducir el riesgo y las consecuencias del e-skimming en su negocio es **contratar la pasarela de pago a una entidad de confianza como puede ser un banco.** Estas pasarelas, generalmente, se encuentran en un entorno seguro controlado por la entidad contratada, por lo que la empresa no tiene que aplicar ninguna media de seguridad sobre la misma, ya que toda la responsabilidad quedará delegada en la entidad contratada.

Proteger la información personal y bancaria de los clientes de técnicas maliciosas como el e-skimming es una responsabilidad que cualquier comercio electrónico debe cumplir para mantener una buena reputación, no lo dudes más y protege a tus clientes y a ti mismo del e-skimming.

Fuente: INCIBE

https://www.incibe.es/protege-tu-empresa/blog/e-skimming-y-proteger-tu-tienda-esta-tecnica-maliciosa