qualoom®

Seguridad en Ecommerce

Cualquier sistema de información puede ser objeto de ataques de ciberseguridad así como de técnicas de fraude. Es por esto que cualquier negocio debe estar bien informado acerca de los protocolos de seguridad en sistemas de comercio electrónico.

Se estima que ya en 2014 las pérdidas por fraudes derivados de falta de conocimiento en la securización de sistemas de E-Commerce ascendieron a casi 3 mil millones de dólares. Las últimas previsiones, a raíz del alza del comercio electrónico como consecuencia de la pandemia mundial del COVID-19, cifran estas pérdidas en hasta 25 mil millones de dólares anuales para el año 2024. Esta tendencia demuestra la necesidad de establecer medidas de prevención que permitan mantener seguros y funcionales los, cada vez más habituales, negocios en el mundo digital.

Por medio de este portfolio realizaremos un viaje a través de las principales amenazas y riesgos de seguridad que afectan a estos sistemas y las principales formas para defendernos de ellos.

qualoom®

¿Qué tipo de amenazas e incidencias pueden afectar a tu sistema de E-commerce?

- Fraude financiero
- Phising
- Ataques DDoS
- Inyección SQL
- Troyanos
- Spam
- Bots
- Ataques de fuerza bruta
- Ataques de contenido cruzado (XSS)

Fraude financiero

Transacciones no autorizadas, solicitudes falsas de reembolso, devolución de productos adquiridos ilegalmente o bienes dañados son solo algunos ejemplos de actividades fraudulentas que cuestan cantidades significativas a los negocios online.

Spam

¿Nunca has recibido correos extraños con remitentes desconocidos? Los formularios de contacto y los sistemas de comentarios son una invitación para dejar enlaces infectados que tienen como objetivo dañar tu negocio y a tus clientes. Además, esto no sólo afecta a la seguridad de tu sitio web sino que también puede echar por tierra esa reputación e imagen comercial que tanto te ha costado conseguir.

Phising

¿Te suena el término? Es una de las amenazas más comunes que tiene el mundo del comercio electrónico, consigue en pocas palabras en suplantar a tu negocio para engañar a tus clientes. Los piratas informáticos se hacen pasar por un negocio legítimo a través del correo electrónico para que los clientes se confíen y revelen su información personal. ¿Crees que tus clientes confiaran en ti después de algo así?

Bots

Muchos son nuestros aliados, están desarrollados para rastrear sitios web en busca de vulnerabilidades, precios e inventario, pero de estos solo unos pocos tienen la legítima finalidad de ofrecer los resultados dentro de un servicio de búsqueda público, de utilidad tanto para los potenciales clientes como para los empresarios.

Por desgracia algunos de estos bots son desarrollados y ejecutados por piratas informáticos con el objetivo de utilizar dicha información para optimizar el precio de sus propias tiendas online y obtener el inventario más vendido en los carritos de compras, lo que tiene como resultado una disminución de ventas e ingresos en la tienda escaneada.

Ataques DDoS

Los ataques de denegación de servicio distribuido (DDos o DoS) consiste en inhabilitar tu sitio web y bloquear el servicio que ofreces en él, esto afecta gravemente a las ventas generales. Este tipo de ataques inundan tus servidores con innumerables peticiones hasta que sucumben y consiguen bloquear tu página web.

Ataques de fuerza bruta

Estos ataques tienen como objetivo el panel de administración y otros servicios administrativos de su tienda en línea, en un intento de averiguar su contraseña mediante la fuerza bruta. Utilizan programas que establecen una conexión con su sitio web y ejecutan todas las combinaciones posibles para descifrar sus contraseñas.

InyecciónSQL

Las inyecciones de SQL son ataques destinados a acceder a tu base de datos utilizando los formularios de búsqueda, contacto, registro, etc. de tu página web. Mediante estos ataques consiguen introducir un código malicioso en tu base de datos para extraer datos privados y, en algunos casos, manipularlos o incluso eliminarlos completamente.

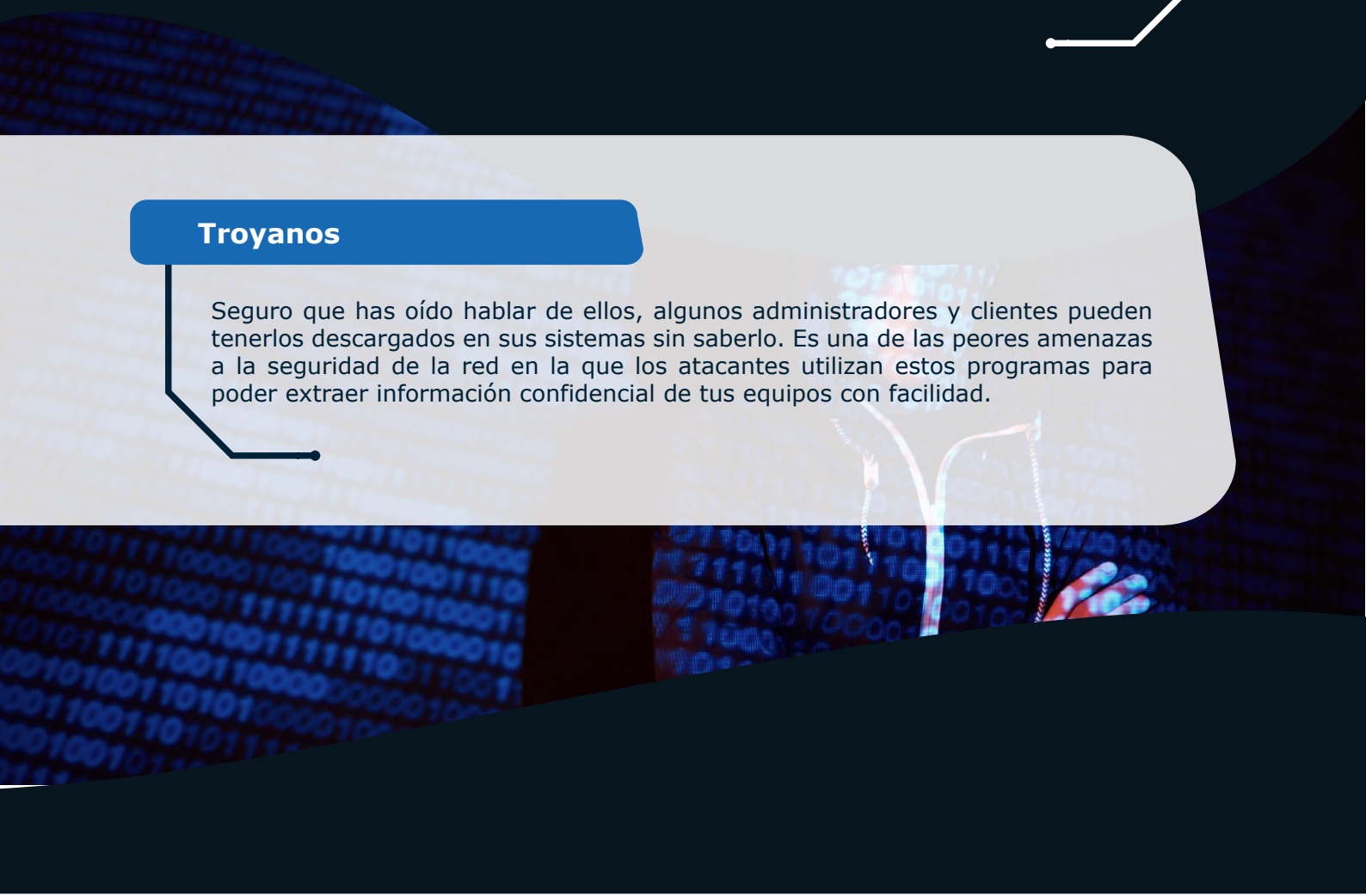
Ataques de contenido cruzado (XSS)

Los ataques de XSS (Cross-Site Scripting) son un tipo de inyección que utilizan los piratas informáticos para introducir scripts maliciosos en sitios web que de otro modo serían benignos y confiables. Estos ataques ocurren cuando un atacante usa una aplicación web para enviar código malicioso, generalmente en forma de un script del lado del navegador, a un usuario final diferente. Los fallos de seguridad que permiten que estos ataques tengan éxito están bastante extendidos y ocurren en cualquier lugar donde una aplicación web tenga entradas de datos provenientes de la salida de otras actividades de navegación.

Ante la eventualidad de este tipo de ataques, el navegador de un usuario final no tiene forma de saber que no se debe confiar en la secuencia de comandos recibida desde el servidor y la ejecutará. Debido a que el usuario cree que el script proviene de una fuente confiable, el script malicioso puede acceder a las cookies, tokens de sesión u otra información confidencial del usuario retenida por el navegador y utilizarla con ese sitio web

Troyanos

Seguro que has oído hablar de ellos, algunos administradores y clientes pueden tenerlos descargados en sus sistemas sin saberlo. Es una de las peores amenazas a la seguridad de la red en la que los atacantes utilizan estos programas para poder extraer información confidencial de tus equipos con facilidad.



¿Qué tipo de medidas puedes adoptar para no caer en estas amenazas?

No te alarmes por todo lo que acabas de leer, existen soluciones para todos estos riesgos que puedes aplicar a tu negocio online. Las tiendas de comercio electrónico con una seguridad ideal tienen algunas características en común:

- No economizan en hardware robusto
- No depende demasiado de aplicaciones o complementos de terceros, como Adobe Flash

Ahora vamos a analizar con más detalle estas características y todas sus funciones para ayudarte a mejorar la seguridad de tu sitio web.

- **Encriptación de datos**
- **Uso de software antivirus y anti-malware**
- **Utilización de pasarelas de pago seguras**
- **Securización de servidores y paneles de administración**
- **Protección en capa de red**
- **Plugins de seguridad**
- **Servicios de firewall en capa de aplicación (WAF)**
- **Política de backup sólida**
- **Política de actualizaciones**
- **Seguimiento de actividades maliciosas**
- **Educar correctamente a los usuarios de la plataforma**

1/ Encriptación de datos

Los certificados SSL y el protocolo HTTPS son muy recomendables para encriptar las comunicaciones entre los usuarios y tu sitio web, de hecho, muchos navegadores elevan las alertas de seguridad cuando el usuario accede a un sitio web que no está habilitado. Estas medidas previenen que los piratas informáticos inspeccionen las comunicaciones y les imposibilita el acceso a datos importantes, como pueden ser los números de tarjeta de crédito o las contraseñas personales. También es recomendable la transición de HTTP a HTTPS implementando una regla de redirección obligatoria para que los usuarios que intenten acceder por el protocolo no seguro (HTTP) sean redirigidos a la dirección con el protocolo óptimo (HTTPS).

Si su plataforma de comercio electrónico cuenta con múltiples componentes interconectados entre sí, tales como servidores web, balanceadores de carga, servidores de base de datos, servidores de ficheros, etc. Es recomendable que el intercambio de información entre dichos servicios también esté encriptado para mantener sus comunicaciones seguras ante posibles brechas de seguridad en el data center donde estos servicios estén hospedados.

Por último, es muy recomendable implementar una política sólida de encriptación de datos en reposo en todos los servicios de almacenamiento de su plataforma de TI. Esto imposibilitará el acceso a la información de su sitio web por parte de terceros en caso de una brecha de seguridad en el data center donde estos se hospeden.

2/ Uso de software antivirus y anti-malware

Los piratas informáticos pueden utilizar la información de una tarjeta de crédito robada para realizar pedidos desde cualquier parte del mundo. Un antivirus o un software antifraude pueden ayudarte con este grave problema de comercio electrónico. Estas herramientas usan algoritmos sofisticados para marcar cualquier transacción maliciosa y ayudarte a tomar más medidas de seguridad. También proporcionan una puntuación de riesgo de fraude que puede ayudar a los propietarios a determinar si una determinada transacción es legítima.

Si tu sitio web permite a los usuarios subir ficheros (por ejemplo, para personalizar un avatar de usuario o aportar documentación relevante), este tipo de herramientas se encargarán de analizar estos ficheros antes de almacenarlos de forma permanente. Si se detecta cualquier tipo de anomalía dentro del fichero, este puede descartarse automáticamente o incluso enviar una notificación de alerta a los administradores para hacer seguimiento del usuario que ha intentado realizar la subida.

3/ Utiliza pasarelas de pago seguras

Si bien puede hacer que el procesamiento de pagos sea más conveniente, tener números de tarjetas de crédito almacenados en su base de datos es una gran responsabilidad. Es nada menos que una invitación abierta para los piratas informáticos en la que se pone en juego la reputación de tu marca y la información confidencial de tus clientes.

Si eres víctima de una violación de seguridad y los piratas informáticos se pueden apoderar de los datos de las tarjetas de crédito de tus clientes, todo lo que te quedaría por hacer es despedirte de tu negocio por las fuertes multas que te obligarían a declararte en bancarrota.

Para salvar tu negocio de este terrible e irreparable destino sólo debes seguir algunas pautas:

- Nunca debes almacenar información de tarjetas de crédito en tus servidores
- Asegúrate de que la seguridad de sus pasarelas de pago no esté en riesgo

Lo recomendable en este caso es utilizar sistemas de procesamiento de pagos de terceros para llevar a cabo el proceso fuera del sitio. Las opciones populares incluyen PayPal, PayTPV, MyMoid o Adyen.

Si decides no hacer uso de estos servicios y tienes claro que quieres almacenar estos datos tan delicados, como números de de tarjetas de crédito y otros datos personales de tus clientes, debes obtener una acreditación de cumplimiento del estándar de seguridad PCI-DSS, que dará garantía de la seguridad de tu empresa dentro de la industria de gestión de tarjetas de pago.

4/ Securización de servidores y paneles de administración

La mayoría de plataformas de comercio electrónico implementan contraseñas por defecto que son ridículamente fáciles de adivinar. Si no se cambian estas contraseñas estás exponiendo tu sitio a ataques por parte de piratas informáticos. Utiliza siempre contraseñas complejas y cámbialas frecuentemente para prevenir accesos no autorizados.

De la misma forma, si tu infraestructura de TI expone de una manera u otra interfaces de administración o acceso a datos (SSH, SFTP, etc.) es recomendable aplicar una política de contraseñas robustas.

5/ Protección en capa de red

Otra recomendación efectiva de comercio electrónico es usar software de firewall, VPN e IDS/IPS para reducir la superficie de ataque de su infraestructura de comercio electrónico y analizar el tráfico que fluye entre, desde y hacia tu plataforma de servidores.

Este tipo de herramientas permiten regular y securizar el tráfico que entra y sale de tu infraestructura, ofreciendo permeabilidad selectiva y solo habilitando la entrada de tráfico confiable. También protegen contra amenazas como inyecciones SQL, XSS, ataques dirigidos y escáneres de puertos, entre otros.

6/ Plugins de seguridad

La mayoría de soluciones de comercio electrónico implementan sistemas de plugins para su extensión por parte del mismo fabricante o de terceros. Entre toda la oferta de plugins es habitual encontrar diversas herramientas que ayudan a mejorar la seguridad de su página web implementando mecanismos como los mencionados en el punto anterior y automatizando otros, como por ejemplo:

- Implementación de políticas seguras de robustez, rotación y caducidad de contraseñas
- Análisis periódico de vulnerabilidades conocidas
- Análisis y reparación de permisos de los ficheros del sitio
- Introducción de cabeceras de seguridad HTTP
- Encriptación de datos en reposo

7/ Servicios de firewall en capa de aplicación (WAF)

Este tipo de herramientas permiten identificar numerosos tipos de amenazas mediante el análisis en detalle del tráfico que recibe tu sitio web. Puede implementar este tipo de soluciones de dos formas, mediante la instalación de plugins o contratando servicios de terceros que reciban el tráfico de tus clientes y solo reenvíe el tráfico autorizado a tu infraestructura.

La mayoría de plugins y proveedores de este tipo de soluciones ofrecen herramientas para la detección y remediación de múltiples tipos de ataques, como por ejemplo:

- SQL Injection
- Cross Site Scripting (XSS)
- Ataques DoS y DDoS
- Ataques de fuerza bruta
- Vulnerabilidades de ámbito general reportadas en OWASP.
- Vulnerabilidades conocidas de productos comerciales populares como Magento, Woocommerce, Prestashop, entre otros.
- Baneo de IPs por pertenencia a listas de baja reputación de terceros
- Baneo de IPs de ISPs anónimos (Red TOR y proveedores de VPN)
- Baneos por origen geográfico.
- Baneo de bots maliciosos
- Etc.

Habitualmente los proveedores de CDN también ofrecen este tipo de soluciones de forma integrada, con lo que es posible aportar seguridad a su sitio a la vez que se mejora el rendimiento del mismo.

8/ Política de backup sólida

La pérdida de datos debido a un mal funcionamiento del hardware o ciberataques no es infrecuente, y si no se realizan copias de seguridad de los datos con regularidad se corre el riesgo de perderlos para siempre. Debes hacerlo tú mismo y no confiar en que nadie más lo haga por ti. Emplea servicios de respaldo automático para que incluso si se te olvida hacerlo manualmente, todos tus datos estén respaldados por las copias de seguridad automáticamente.

Te recomendamos que de un almacenamiento de copias de seguridad externo a la infraestructura que hospeda tu sitio web principal. De esta forma, en caso de que dicho sitio esté comprometido, tienes una garantía adicional de que podrá recuperar sus datos. Este tipo de copia de seguridad es especialmente efectiva ante ataques ransomware.

9/ Política de actualizaciones

Es de vital importancia mantener tus sistemas al día en términos de parches de seguridad y versiones de producto. Todos los fabricantes suelen ofrecer mejoras de seguridad y correcciones de vulnerabilidades de forma periódica o excepcional, tanto a nivel de sistema operativo como en productos de TI (Servidor web, base de datos…), así como en plataformas de E-commerce y plugins de terceros.

Mantener tus sistemas al día te protege ante posibles ataques que hagan uso de vulnerabilidades conocidas. Los piratas informáticos a menudo implementan bots dedicados a buscar este tipo de vulnerabilidades para poder explotarlas tan pronto son identificados; es por ello que un sitio sin actualizar es un potencial foco de ataques y fraudes económicos.

10/ Seguimiento de actividades maliciosas

Si no quieres que ningún ataque malintencionado pase desapercibido, debes implementar mecanismos de auditoría y monitorización adecuados para detectar cualquier actividad sospechosa. Esto puede ahorrarte muchos dolores de cabeza (sin mencionar todo lo que te puedes ahorrar a nivel económico) ya que, potencialmente, puede ayudarte a detectar una transacción fraudulenta antes de que se lleve a cabo. Puedes utilizar un software de monitorización especial para rastrear la actividad en tiempo real y mantenerte al día sobre cualquier transacción o actividad cuestionable; como en las siguientes posibles situaciones:

- Un estafador que usa diferentes tarjetas para realizar varios pedidos, o pedidos en los que la persona que usa la tarjeta no es su titular.
- Una misma dirección IP realiza un número anormalmente alto de compras con gran cantidad de usuarios diferentes y en un marco de tiempo reducido.
- Un usuario ha intentado subir un script malicioso utilizando el formulario de subida de imágenes de su perfil de usuario.
- Un usuario con permisos de administración está intentado acceder al sistema de base de datos con multitud de contraseñas diferentes.

11/ Educar correctamente a los usuarios de la plataforma

Todo tu personal debe conocer las leyes y políticas relacionadas con la protección de la información del usuario. No se deben compartir las credenciales de inicio de sesión y los miembros del equipo deben ser debidamente supervisados, especialmente el personal que tiene acceso a información confidencial del cliente.

Todas y cada una de las veces que un empleado presente su renuncia, debes eliminar sus datos y revocar todos sus accesos para evitar que cometan un delito cibernético contra su empresa.

Algunos fallos en la seguridad no ocurren por parte del equipo de tu negocio sino por la de tus clientes. Los usuarios pueden estar usando contraseñas débiles o incluso pueden haber entregado información confidencial en sitios de phishing y haberla dejado en manos de piratas informáticos.

Puedes resolver estas amenazas de seguridad educando a tus clientes. Puedes informarles sobre los riesgos asociados con las prácticas de seguridad poco recomendadas y exigirles el uso contraseñas seguras, también puedes presentarles cómo funciona el phishing e implementar procesos de validación de correo electrónico antes de permitir el envío de datos sensibles.

Las contraseñas seguras requieren una buena combinación de caracteres, símbolos y números que son casi imposibles de adivinar o usar la fuerza bruta. También puedes evitar que los usuarios creen perfiles con contraseñas débiles. Si los usuarios están usando contraseñas débiles o la información que envía es sensible y susceptible de piratería, puedes adoptar el sistema de autenticación de dos factores.

¿Te interesa?

Contacta con nosotros