¿Por qué es importante la seguridad del sitio web?

¿Por qué es importante la seguridad del sitio web? Todos los que usan Internet se han encontrado con este término de seguridad del sitio web, pero la mayoría de ellos se pregunta qué es exactamente esto. Es proteger el sitio web o proteger a Internet en su conjunto. Bueno, si usted es un usuario personal o un usuario comercial, su sitio web necesita protección. Debido a que cualquier infracción en su sitio afectará su negocio en línea. Por otro lado, crear y mantener su sitio web significa que usted es serio acerca de su negocio.

La seguridad del sitio web es un término que muchos piensan que esto se asocia con las élites y los que tienen un gran negocio. Los piratas informáticos quieren que usted crea que es una especie de proceso misterioso, y no todos tienen que preocuparse por eso, lo cual no es el caso real. De hecho, la seguridad del sitio web no hace ninguna diferencia; Si eres de élite o no, habrás estado en alerta y tomará todas las medidas posibles para garantizar tu seguridad. Es igual a cómo salvaguardas tu identificación personal, los datos bancarios, se trata del sentido común.

La amenaza a la seguridad del sitio web es sobre malware, piratería y otras inyecciones dudosas de códigos, etc., la intención de los delincuentes es explotar las vulnerabilidades en su sitio. Las vulnerabilidades pueden ser una contraseña débil o alguna otra falla técnica, o un script cruzado, etc.

Hay muchas cosas involucradas de valor en los sitios web

Su sitio web es su marca, su tienda y, a menudo, su primer

contacto con los clientes. Si no es seguro, esas relaciones comerciales críticas pueden verse comprometidas. Las amenazas pueden venir de muchas formas: infectar un sitio web con malware para propagar ese malware a los visitantes del sitio, robar información de los clientes, como nombres y direcciones de correo electrónico, robar tarjetas de crédito y otra información de transacciones, agregar el sitio web a una red de bots de sitios infectados , e incluso secuestrar o estrellar el sitio.

Una sola brecha de seguridad podría ser una sentencia de muerte para una pequeña empresa. La mayoría de los estados ahora tienen leyes estrictas de violación de datos, y muchos vienen con multas, sanciones y otros costos. Incluso si una brecha de seguridad en un sitio web de una pequeña empresa no desencadena una brecha de datos, puede tener un gran impacto en la confianza de los clientes si los clientes se enteran de ello.

Un sitio web desprotegido es un riesgo de seguridad para los clientes, otras empresas y sitios públicos / gubernamentales. Permite la propagación y escalada de malware, ataques a otros sitios web e incluso ataques contra objetivos nacionales e infraestructura. En muchos de estos ataques, los piratas informáticos intentarán aprovechar el poder combinado de miles de computadoras y sitios para lanzar estos ataques, y los ataques rara vez conducen directamente a los piratas informáticos.

Para decirlo breve y directo, la pérdida de reputación comercial está directamente relacionada con la caída de los ingresos.
Algunas personas pueden no pensar en la seguridad web como una forma de generar confianza con los clientes. Pueden pensar que es simplemente una forma de prevenir ataques maliciosos.

Si bien la prevención es importante:

¿Cómo la seguridad web mejora la confianza con los clientes?

Los consumidores están nerviosos por los riesgos de seguridad de internet. Por ejemplo, el robo de identidad ha sido la queja número uno de los consumidores ante la Comisión Federal de Comercio cada año durante los últimos trece años. Los consumidores parecen sentir, porque es de sentido común, que la mayoría de las pequeñas empresas no pueden pagar la mejor seguridad y, por lo tanto, es más probable que su sitio web presente un mayor riesgo, ya sea comprando o simplemente navegando.

Cuanto más pueda hacer una pequeña empresa para generar confianza en la seguridad de su sitio web, más probable es que los clientes visiten, se queden, compren, regresen y recomienden. Es por eso que los sellos de seguridad son importantes. No solo brindan seguridad a los clientes de que el sitio web es seguro y la empresa es consciente de los riesgos, sino que también están acostumbrados a ver estos sellos en los sitios web, sino que tienden a darse cuenta cuando un sitio no tiene ninguno.

En la actualidad, hay más de 1,3 billones de sitios web en la red mundial y las personas confían en los motores de búsqueda cuando desean obtener información sobre esos sitios. Por lo tanto , la optimización de motores de búsqueda es más importante que nunca y es necesario que cada webmaster comprenda el verdadero significado de SEO y el potencial que puede ofrecer a cada negocio.

Google y otros motores de búsqueda (para quienes normalmente no quieres estar en la lista traviesa) advierten a tus clientes y les impiden ingresar a tu sitio web. Últimamente, Google, por ejemplo, ha intensificado el juego aún más.

En promedio, alrededor de 30 000 sitios web son pirateados cada día y, en realidad, la mayoría de estos 30,000 sitios son pequeñas empresas legítimas que distribuyen, sin saberlo, códigos maliciosos para los ciberdelincuentes.

Cuando su sitio es hackeado y agregado a diferentes listas negras, el cliente potencial no puede acceder a los productos o servicios ofrecidos.

De todos modos, si un cliente potencial visita su sitio y recibe una advertencia o una infección, existe una posibilidad extremadamente baja de que el cliente vuelva a visitar su sitio.

¿Qué industrias deben ser particularmente cuidadosas al asegurar su sitio web?

Ninguna industria es inmune. Hackear no es solo robar datos. Los piratas informáticos quieren crear pozos de agua donde pueden ocultar malware como una forma de propagar el malware a cualquier visitante de ese sitio. También desean enlistar esos sitios comprometidos en ataques de Denegación de Servicio Distribuido (DDS) en otros sitios. Cualquier sitio puede

cumplir esa función. Cuando se trata de robo de datos, los servicios financieros, la atención médica y el comercio minorista parecen ser especialmente populares.

Elección del proveedor de alojamiento web

La empresa de alojamiento es una clave para la seguridad del sitio web. El host proporciona la infraestructura sobre la cual se construirá el sitio. Al igual que construir una casa, necesita una base sólida para estar seguro. También es importante cómo se construye la casa, que es una pieza importante que los propietarios de sitios web a veces no entienden completamente. Si bien el host proporciona la infraestructura, el sitio también debe ser seguro. De hecho, los sitios web son ahora un punto de entrada mucho más popular que los servidores o las redes, y representan hasta el 80%, según un informe reciente de Verizon. A menudo utilizamos la analogía de un complejo de apartamentos. El anfitrión proporciona la seguridad para el edificio, por lo tanto, si la puerta frontal se cuelga y no hay un sistema de timbre, eso es responsabilidad del anfitrión, del casero, del dueño del conjunto. Sin embargo, si deja la puerta de su apartamento abierta o una ventana, esa es su responsabilidad.

Aprendiendo de los errores: la limpieza del sitio web es más costosa que la protección

Como propietario de un sitio web que descubre que su sitio web ha sido pirateado, lo primero que debe hacer es buscar «Cómo limpiar un sitio pirateado». Sí, encontrará muchas publicaciones de blog y artículos sobre el mismo, pero eventualmente todos te recomendarán lo mismo: haga que un profesional lo haga por usted.

Realizar una eliminación de malware de WordPress de manera que pueda estar seguro de que está limpio no es una tarea fácil. Es por eso que un servicio como este puede costar más de 150 dólares por sitio e incluso entonces, dependiendo del proveedor de servicios, no puede estar seguro de si el sitio se limpió correctamente o no.
El proceso de limpieza de malware de un sitio web es mucho más acerca de conocer las vulnerabilidades y el modo de pensar de un hacker, que solo revisar manualmente los archivos.

El malware a menudo se oculta de los archivos originales y en la base de datos, y los atacantes hacen un gran esfuerzo para asegurarse de que no podrá eliminar sus puertas traseras tan fácilmente.

Es caro, por cierto. No solo el ¶servicio de limpieza de malware en sí, sino la pérdida de ingresos y el daño a la reputación son los que pueden consumir mucho tiempo y dinero para recuperarse.
Leer también: seguridad en WordPress, cómo prevenir ataques; POST ANTERIOR SOBRE QUE ES LA SEGURIDAD WEB OJO; ¿Porqué se cae un servidor web o una página web?