GIRONA NOTICIES.COM
+ Periodisme

¿Cómo saber si un sitio web es seguro?

Actualidad Empresarial | 28/04/2023 | 00:00

La frecuencia de los ciberataques en la actualidad ha convertido a la seguridad de los sitios web en una prioridad. Con el fin de evaluar la seguridad de los sitios web, existen diversas opciones, como verificar si posee un certificado SSL válido, comprobar la legitimidad del sitio web y sus enlaces, y asegurarse de que la información de tarjetas de crédito no se comparta en el sitio web. Al respecto, Aplyca ofrece diferentes opciones para asegurar las páginas web.

¿Qué es un ciberataque o ataque informático?

Un ataque informático consiste en el intento malicioso de acceder, dañar o destruir sistemas informáticos, redes o dispositivos electrónicos. Los mismos pueden ser realizados tanto por individuos como por grupos con diversos objetivos, entre los cuales se destacan el robo de datos, la extorsión, el espionaje y el sabotaje, entre otros.

De acuerdo al diario El País de España, durante 2022 el 94 % de las empresas reconoció haber sido víctima de algún tipo de incidente de ciberseguridad, lo cual posiciona a España como el tercer país con más ataques informáticos en el mundo.

A causa de la rápida evolución de las tecnologías digitales, los delitos cibernéticos han evolucionado para volverse más sofisticados y difíciles de detectar. A causa de ello, es fundamental que los usuarios de tecnología se mantengan al tanto de los diferentes tipos de ataques y las medidas de seguridad recomendadas para prevenirlos en primera instancia o, en caso de que ya hayan tenido lugar, mitigar sus efectos.

¿Qué son el phishing, vishing y malware?

Los ciberataques pueden presentarse en diversas formas, y cada tipo de ataque tiene sus particularidades y objetivos específicos. Para perpetrar estos actos, los ciberdelincuentes utilizan diferentes técnicas que incluyen desde la ingeniería social hasta el malware y los ataques de denegación de servicio (DoS).

Phishing: El phishing consiste en un tipo de ataque de ingeniería social que mediante engaños a los usuarios hace que los mismos compartan en forma voluntaria información personal y financiera. Para llevarlos a cabo, los delincuentes se hacen pasar por una empresa o persona legítima.

Vishing: Es una variante del phishing que se vale de técnicas de voz para efectuar el engaño.

Malware: El malware es un software malicioso que tiene por objetivo dañar o tomar el control de sistemas informáticos sin el consentimiento del usuario. En contraposición, los ataques de denegación de servicio (DoS) buscan abrumar a los sistemas con tráfico para afectar su funcionamiento habitual.

¿Cómo ocurre usualmente un ciberataque?

Los sitios web son atacados mediante cinco técnicas diferentes:

A través de las pantallas de inicio de sesión. Cuando buscan acceder de una manera no autorizada a los sistemas, los hackers y bots malintencionados suelen atacar primeramente a las pantallas de inicio de sesión.

La seguridad de la contraseña también es crucial. Las contraseñas débiles como la combinación de números sucesivos o repetidos representan el 99,9 % de las formas de piratear cuentas, junto a la falta de autenticación multifactor.

Los sitios web obsoletos ofrecen fácil acceso a usuarios no autorizados. Por ello, si se utiliza una versión obsoleta de un CMS, es posible que el sistema de seguridad no esté actualizado y, por lo tanto, haga que el sitio web sea vulnerable.

Configuración, plugins y temas: Un informe de ZDNet sobre seguridad de sitios web destaca que un gran número de los hackeos de sitios web tiene por causa a vulnerabilidades en plugins y temas, problemas de configuración y falta de mantenimiento por parte de administradores web.

Código abierto: Los piratas informáticos suelen atacar los CMS de código abierto más populares, como WordPress, Joomla y Drupal, debido a que su uso está muy extendido y su código se encuentra abierto. Sumado a ello, estos CMS suelen ser utilizados por usuarios que carecen de conocimientos técnicos, lo que los convierte en un blanco fácil para los piratas informáticos.

Las 10 vulnerabilidades a sitios web más comunes y sus prevenciones

Para mejorar la seguridad web es importante comprender las vulnerabilidades que pueden presentarse en las aplicaciones. Con este fin, la Fundación OWASP ha realizado una lista de las vulnerabilidades de seguridad principales de las aplicaciones web que afectan en mayor medida al desarrollo, la ciberseguridad y los empresarios.

La Fundación OWASP es una organización sin ánimo de lucro que tiene por objetivo mejorar la

seguridad del software de diversos sectores. Una de sus principales contribuciones es la compilación del OWASP Top 10, que consiste en una lista de las vulnerabilidades de seguridad de aplicaciones web más críticas. La misma es realizada tras el análisis de datos sobre aplicaciones procedentes de diversas fuentes.

Control de acceso defectuoso: Consiste en una falla en la restricción del acceso de los usuarios a los recursos dentro de sus permisos asignados. Cuando esto sucede, los usuarios tienen la posibilidad de realizar acciones que requieren permisos diferentes a los que poseían originalmente, así como a la divulgación, modificación o destrucción no autorizada de datos.

Fallas Criptográficas: Consisten en debilidades o deficiencias en las técnicas para encriptar la información, que pueden comprometer el sistema o exponer datos sensibles, lo cual incluye información de identificación personal y números de tarjetas de crédito, que requieren una protección extra. Los métodos utilizados normalmente para la protección de datos dependen del tipo de datos y de si están sujetos a leyes de privacidad de datos como el GDPR de la Unión Europea.

Inyecciones (Injections): Este tipo de vulnerabilidades incluye diferentes variables entre las cuales se destacan el cross-site scripting, la inyección SQL y la inyección XML. Las mismas identificarse mediante la revisión del código fuente. Otra técnica utilizada a tales fines es la automatización a los fines de probar todos los parámetros y entradas de datos posibles, con la finalidad de detectar vulnerabilidades. Las aplicaciones pueden recibir ataques de inyección si aceptan datos introducidos por el usuario sin la validación, el saneamiento o el filtrado correspondiente, o cuando se utilizan datos hostiles para extraer información sensible.

El diseño inseguro y la implementación insegura son dos problemas distintos en la seguridad del software. Un diseño seguro puede seguir presentando vulnerabilidades si su implementación no es la adecuada. Por otra parte, un diseño inseguro no puede solucionarse solo mediante la implementación debido a que carece de los controles de seguridad adecuados. Por consiguiente, no realizar una evaluación precisa de los riesgos empresariales asociados al software o sistema que se está desarrollando puede dar lugar a niveles bajos de seguridad. Esto resalta la importancia de llevar a cabo una evaluación adecuada de los riesgos y de las consideraciones de diseño en el desarrollo de software.

Mala configuración de la seguridad: Los errores en la configuración de la seguridad pueden deberse a diversos factores que pueden aumentar la vulnerabilidad del sitio a los ataques. Algunos ejemplos de errores de configuración son los permisos mal configurados para servicios en la nube, la habilitación de funciones innecesarias que pueden producir puertos abiertos o privilegios elevados, y no cambiar las credenciales de inicio de sesión de la cuenta por defecto.

Componentes vulnerables y obsoletos: Los componentes obsoletos que siguen en uso pueden suponer un riesgo importante, ya que las vulnerabilidades pueden ya ser conocidas por los piratas cibernéticos. Las aplicaciones pueden sufrir ataques si no ejecutan la última versión del software o si no queda claro cuál biblioteca o versión de componente se encuentra en uso. Sumado a ello, los componentes que no se analizan en busca de vulnerabilidades también

pueden encontrarse en riesgo.

Fallos de identificación y autenticación: Los fallos de autenticación e identificación tienen lugar cuando la identidad del usuario, la autenticación y la información de la sesión no son confirmadas debidamente antes de que se permita al mismo acceder a los sistemas y datos. Entre los factores que pueden afectar a la seguridad de una aplicación debido a estos fallos se encuentran el permiso de crear contraseñas débiles; la utilización de almacenes de datos de contraseñas de texto plano con hash débil; e incluso permitir bots que puedan llevar a cabo ataques automatizados como fuerza bruta y relleno de credenciales.

Fallos en el software y en la integridad de los datos: Consiste en el riesgo potencial de confiar en actualizaciones de software y datos sin verificar su procedencia, que los atacantes pueden utilizar para inyectar malware a través de actualizaciones aparentemente legítimas. Actualmente, hay una gran cantidad de software que poseen funciones de actualización automatizadas que no comprueban la integridad de las actualizaciones, lo cual los hace vulnerables a estos ataques.

Fallos en el registro y la supervisión de la seguridad: Una supervisión y un registro eficientes son fundamentales a la hora de detectar y minimizar el impacto de un ataque que se encuentre en curso. En este sentido, los fallos se producen cuando no se registran transacciones importantes, como las de alto valor, los intentos de inicio de sesión e intentos fallidos de inicio de sesión, o cuando no se generan entradas de registro para errores y advertencias, o si las mismas son poco claras o inadecuadas. Sumado a ello, las actividades sospechosas no se supervisan para las API y las aplicaciones, los registros de seguridad solo se encuentran disponibles de manera local y las aplicaciones no pueden detectar ataques en curso o emitir alertas oportunas.

Falsificación de peticiones del lado del servidor (SSRF): Estos fallos tienen lugar cuando las aplicaciones recuperan fuentes remotas solicitadas por los usuarios sin corroborar primero el destino. Esto habilita la posibilidad a los atacantes de enviar peticiones específicas a la aplicación a través de una fuente inesperada. Estas vulnerabilidades se presentan cuando las aplicaciones recuperan URL para facilitar el cambio de tareas a los usuarios finales, permitiéndoles acceder a otras funciones a través de la URL recuperada mientras se encuentran en la aplicación. Con la creciente complejidad de la arquitectura de la nube, los ataques de este tipo han aumentado su frecuencia.

¿Son los Headless CMS seguros?

Para evaluar el nivel de seguridad de un Headless CMS debe comprenderse la diferencia entre un CMS tradicional y un Headless CMS en cuanto a su forma de trabajo.

CMS Tradicionales: Los CMS tradicionales brindan a los creadores de contenidos y a los usuarios no técnicos la oportunidad de crear y publicar plantillas con estilo, que luego son almacenadas en una base de datos y mostradas al usuario final basándose en una plantilla predeterminada. El front-end y el back-end de un CMS tradicional son codependientes, lo que puede ocasionar vulnerabilidades.

CMS Headless: En una arquitectura Headless, el contenido suele otorgarse a través de una red de distribución de contenidos (CDN) y no en una base de datos. El front-end y el back-end de un CMS headless están desacoplados, lo que permite poner los esfuerzos en la creación y el almacenamiento de contenidos. Además, la API publica el contenido headless en formato de solo lectura, lo que lo hace menos vulnerable a los ciberataques, ya que se puede esconder detrás de capas de código, esto incluye una capa de aplicación y otra capa de seguridad, lo que reduce con creces el riesgo de ataques.

Sin lugar a dudas, gracias a su arquitectura los Headless CMS ofrecen una mayor seguridad con respecto a la arquitectura de un CMS tradicional. Una de las ventajas más importantes es su gran resistencia a los ataques DDoS, ya que no posee una base de datos propia y se conecta a distintos front-ends mediante API. Además, requiere un menor número de actualizaciones y anula la posibilidad de problemas a causa de continuidad comprometida cuando exista una brecha.

Aplyca y la ciberseguridad

Aplyca se erige como una excelente opción a la hora de implementar soluciones para estrategias de contenidos empresariales con los más altos estándares de calidad y seguridad, con el fin de evitar sufrir un ataque informático.

Autor: Redacció

https://gironanoticies.com/empresarial/203960-como-saber-si-un-sitio-web-es-seguro.htm