GIRONA NOTICIES.COM
+ Periodisme

Seguridad en los CMS, prevención de vulnerabilidades

Actualidad Empresarial | 25/04/2023 | 00:00

El Informe de Investigación sobre Amenazas a Sitios Web 2022 de Sucuri, llevado a cabo por sus expertos en Investigación y Remediación, analizó las amenazas actuales y tendencias futuras en seguridad online. Este equipo de expertos analizó datos sobre malware basado en web, software vulnerable y ataques para identificar los tipos más comunes de infecciones y amenazas. El análisis reveló que los backdoors de sitios web y el spam de SEO mantienen su vigencia, y que se presentan grandes riesgos como consecuencia del redireccionamiento de sitios web a páginas web de spam, mediante plugins vulnerables.

El informe también señaló un aumento significativo de los ataques de robo de tarjetas de crédito en sitios web de comercio electrónico. Dentro de esta categoría, se destacan los sitios que utilizan plugins de WooCommerce, que experimentaron cargas maliciosas creadas específicamente para el sitio web de cada víctima. Asimismo, los sitios web de nivel medio se mantuvieron como los principales objetivos de las amenazas.

Por otra parte, la mayoría de los sitios web se encuentran comprometidos a causa de plugins y extensiones vulnerables, más que a archivos CMS obsoletos. Incluso en caso de sitios web actualizados puede existir el riesgo de vulnerabilidad si la misma no se remedia a tiempo.

Por qué es importante el análisis de riesgos para la seguridad de los CMS

En los últimos años, se han multiplicado las amenazas a la ciberseguridad. Entre los ataques cibernéticos más destacados del 2022 se encuentra el caso de Medibank, una aseguradora con sede en Australia víctima de un ataque que afectó a casi 10 millones de clientes. Asimismo, el Consejo Superior de Investigaciones Científicas (CSIC) también fue afectado, y la productora de contenido Bandai Namco Holdings Inc. afirmó haber sufrido un acceso no autorizado a sus sistemas internos en varias empresas del Grupo en Asia.

Estos sucesos marcaron la relevancia de la seguridad a la hora de alcanzar un buen desarrollo web, destacando la importancia de la auditoría y actualización periódica de los sitios web y las plataformas CMS con el fin de poder hacer frente a los retos de seguridad modernos.

Aunque las plataformas CMS como los blogs suelen pasarse por alto como objetivos potenciales de los piratas informáticos, estos pueden ser víctimas de ciberataques mediante la aplicación de tecnologías de uso común, la interacción con clientes finales y su gran potencial para aumentar la visibilidad de las marcas.

Preocupaciones comunes sobre la seguridad del CMS

En primer lugar, el CMS puede dar lugar a la inyección de código, una técnica consistente en insertar código adicional en un sitio web sin el consentimiento del desarrollador, lo que puede ocasionar consecuencias no deseadas, constituyendo uno de los ciberataques más frecuentes.

Por otra parte, la falsificación de peticiones entre sitios es otro tipo de ataque que consiste en engañar a los visitantes del sitio para que envíen peticiones no deseadas, lo que puede dar lugar al robo de datos y la manipulación de cuentas, entre otros riesgos.

Finalmente, Cross-site scripting (XSS) es otro tipo de ataque de inyección, que consiste en la ejecución de código desde un navegador web en lugar del CMS o los archivos del sitio web. Muchos lenguajes de codificación son susceptibles a este tipo de ataques, lo que los convierte en un grave problema para los desarrolladores.

Plataformas CMS de código cerrado y de código abierto

Al elegir un CMS, dentro de la elección también se deberá tener en cuenta el tipo de proveedor y si será de código abierto o cerrado.

En primer lugar, los sistemas de gestión de contenidos (CMS) de código abierto se encuentran disponibles de manera gratuita y su mantenimiento es realizado por una comunidad de desarrolladores que pueden encontrarse en distintas regiones del mundo. Estos CMS brindan a los desarrolladores la posibilidad de contribuir al proyecto al hacer público el código fuente. Como consecuencia, el público puede modificar y mejorar con libertad los CMS de código abierto. Aunque el software de código abierto ofrece la posibilidad de compartirse y así mejorar de manera rápida y continua, también puede ser vulnerable a la explotación, debido a que el código fuente está abierto a todo el mundo, lo que facilita la manipulación del código con fines maliciosos y el ataque a sitios web o distribución de malware.

Por otro lado, los sistemas de gestión de contenidos (CMS) propietarios o CMS de código cerrado, no son de acceso público, por lo que solo los desarrolladores internos tienen acceso al código fuente. Para mantener los CMS de código cerrado, debe abonarse una suma dineraria por su mantenimiento, pudiendo adaptar la distribución según el modelo comercial de cada cliente de pago. Los CMS de código cerrado se encuentran protegidos con el objetivo de mantener el valor del producto, y se comercializan como un sistema pulido.

En comparación, los sistemas de gestión de contenidos de código abierto carecen de una directiva de seguridad clara, por lo que no tienen por objetivo principal resolver los problemas de seguridad para el usuario final. A diferencia de los CMS de código cerrado, los CMS de código abierto carecen de un equipo de seguridad dedicado exclusivamente a esta cuestión. Como ejemplo, WordPress es un CMS de código abierto que recomienda a los usuarios que sospechen que su sitio ha recibido un ciberataque que adquieran elementos de ciberseguridad o eliminen su

sitio web. Esto se debe a que no se hacen responsables de la seguridad de los sitios web de sus usuarios.

En contraposición, los CMS de código cerrado cuentan con equipos de seguridad especializados, además de amplias opciones de soporte para solucionar cualquier posible problema, lo cual constituye una de sus características destacadas.

Medidas para proteger los sistemas de gestión de contenidos

Gracias a los sistemas de gestión de contenidos (CMS), es posible diseñar y poner en marcha un sitio web con facilidad, por lo que existe una gran variedad de estos CMS a disposición de todo tipo de clientes, sin importar el tamaño de la empresa o si se trata de particulares.

Sin embargo, debido a la gran difusión de este tipo de software, el riesgo de ciberataques es mayor, ya que los delincuentes eligen invertir más energía en encontrar los puntos débiles de estos sistemas.

Una de las soluciones disponibles es la instalación de parches de seguridad, que es capaz de reducir significativamente el riesgo de ataques a los CMS. De todas formas, existen otras medidas que los propietarios de sitios web pueden tomar para mejorar la seguridad de su CMS. En este sentido, algunas de las alternativas disponibles son las copias de seguridad periódicas, las contraseñas seguras y la limitación de los privilegios de los usuarios.

Actualizaciones rápidas

Es importante estar atento a las actualizaciones cuando se utiliza un CMS popular, ya que los hackers se mantienen al tanto de las vulnerabilidades conocidas. En este sentido, cobra relevancia la pronta aplicación de actualizaciones, especialmente las que abordan vulnerabilidades conocidas. Sin embargo, los CMS personalizados pueden ser difíciles de actualizar, ya que los cambios realizados en el sistema pueden afectar su funcionalidad o dejar vulnerabilidades disponibles. Para evitar estos problemas, es recomendable la realización de cambios en módulos de programa independientes, y no en los módulos principales del CMS, que reciben actualizaciones periódicas.

Gestión rápida de parches

Una alternativa para reducir los ataques a la seguridad es la instalación de parches de seguridad. Para ello, se sugiere su instalación apenas se publiquen, o activar la función de actualización automática que la mayoría de los fabricantes incluyen.

Autenticación de dos factores

Para producir el aumento de la seguridad del acceso al área de administración, es recomendable la utilización de la autenticación de dos factores (2FA), en combinación con el nombre de usuario y la contraseña habituales. Esto es posible mediante el empleo de herramientas como Google Authenticator, capaz de generar una contraseña única y sensible al tiempo. Con este fin, se necesita una aplicación de smartphone, y la contraseña generada caduca a los 60 segundos. Asimismo, existe un plug-in para este sistema en varios programas de gestión de contenidos que incluyen Typo3 y WordPress.

Accesos

Otra recomendación frecuente es la restricción del acceso del administrador a determinadas direcciones IP o rangos de direcciones IP mediante extensiones o un archivo .htaccess.

Sumado a ello, se sugiere proteger el ordenador del webmaster instalando software antimalware, que debe mantenerse actualizado. Asimismo, utilizar una conexión FTP cifrada puede evitar el robo de credenciales FTP.

Para proteger la cuenta de administrador, se recomienda activar todas las funciones de seguridad disponibles de manera simultánea, como 2FA, contraseñas seguras y cuentas de correo electrónico dedicadas. De la misma manera, es relevante la restricción de los permisos de usuario a las funciones esenciales y la aplicación de políticas de seguridad de usuario que requieran 2FA además de otras medidas de seguridad.

¿Es un Headless CMS un CMS seguro?

Un CMS headless es considerado más seguro que un CMS tradicional desde todas las perspectivas. El mismo se conforma por una capa de backend y se conecta a diferentes frontends mediante API, lo cual permite reducir las amenazas a la ciberseguridad.

La ausencia de base de datos también contribuye positivamente a la reducción de posibilidades de una brecha de seguridad. Otro beneficio de estos sistemas es que los CMS headless requieren menos actualizaciones, lo cual implica que los cambios ligeros en determinados componentes pueden no afectar a la seguridad y el rendimiento de todo el sistema. Además, la continuidad del sitio web se encuentra protegida ante problemas temporales. Finalmente, a medida que el CMS sea más seguro, más fácil será la adaptación a futuras demandas.

Debe tenerse en cuenta que es crucial elegir un sistema CMS headless que tenga un historial sólido, y aplique tanto tecnologías como protocolos de seguridad que minimicen o eviten los ciberataques. Asimismo, el software escogido debe respetar los estándares del sector, y es importante que la infraestructura utilice las mejores prácticas de seguridad.

Aplyca y la ciberseguridad

A la hora de implementar soluciones en estrategia de contenidos bajo altos estándares de calidad y seguridad en las organizaciones, Aplyca invita a todos aquellos que busquen alcanzar estos objetivos a comunicarse con ellos con el fin de implementar CMS seguros.

Autor: Redacció

https://gironanoticies.com/empresarial/203521-seguridad-en-los-cms-prevencion-de-vulnerabilidades.htm