La importancia de mantener el software actualizado en los servidores web

La importancia de mantener el software actualizado en los servidores web. Cada cierto tiempo se desatan olas de ataque de malware, DDoS y otras variantes, cuyo propósito principal es robar la información sensible de la Compañía en cuestión.

Datos de clientes, medios de pago, documentos de identidad y otro tipo de data que puede ser explotada por este tipo de atacantes, es la que está en juego.

Caso Microsoft Exchange

Hace pocos días se supo de una campaña de Zero day (en total se identificaron 4 exploits) contra los servidores de Microsoft Exchange por ejemplo.

Un exploit de día cero es una vulnerabilidad que el proveedor de software desconocía anteriormente.

«Día cero» se refiere al hecho de que los desarrolladores tienen «cero días» para solucionar el problema recién expuesto, que podría haber sido explotado por los piratas informáticos.

El ataque habría hecho vulnerables a las empresas y agencias que tienen sus propios servidores físicos si estuvieran utilizando los productos de Microsoft afectados, Exchange Server 2013, 2016 y 2019. El ataque no afectó a Exchange Online, el servicio de servidor en la nube de Microsoft.

¿Qué es Microsoft Exchange Server?

Microsoft Exchange Server es una bandeja de entrada de correo electrónico, un calendario y una solución de colaboración. Los usuarios van desde gigantes empresariales hasta pequeñas y medianas empresas en todo el mundo.

Patrón de ataque

Se inyectan web shells o pequeños scripts protegidos por contraseñas, en las máquinas infectadas para robar la información.Esto incluye secuestro de servidores web, que se controlan de forma remota sin requerir credenciales.

¿Cómo combatirlo?

Actualizando o usando los parches que corrigen las vulnerabilidades o, en caso trágico, desconectando este tipo de servidores hasta cuando se supere la crisis.

Hay quien achaca este tipo de ataques a estamentos chinos pero en realidad, independientemente de su procedencia es un asunto de hábitos de consumo, de uso y de seguridad integral de las empresas, algo que se puede prevenir si se mantienen los programas y los servidores actualizados.

La seguridad debe seguir siendo una prioridad durante toda la vida de su sitio

Una vez que el servidor está instalado y configurado, la seguridad debe seguir siendo una prioridad. El sistema operativo elegido y la aplicación instalada (que puede ser, por ejemplo, Prestashop, WordPress, Joomla) se volverán cada vez menos seguros con el tiempo.

Los sistemas y las aplicaciones, a pesar de la gran atención prestada por los desarrolladores, están sujetos a errores o, peor aún, a violaciones de seguridad. Afortunadamente, estos defectos se identifican muy rápidamente y se corrigen con la misma rapidez. Los autores de malware siguen estas correcciones muy de cerca y desarrollan su software basándose en estas fallas. Después de escribir software malicioso, el atacante busca, a través de robots, sistemas o aplicaciones que aún no se han actualizado. Para no dejar la puerta abierta a este software, ¡debe mantener constantemente actualizado su sistema y aplicación!

Por ignorancia, muchos propietarios de sitios prefieren mantener los sistemas operativos y las aplicaciones en el mismo estado en el que estaban después de su instalación,

creyendo que una actualización no puede hacer nada excepto por problemas de compatibilidad. Por lo tanto, este lema pone en peligro la seguridad de un sitio web y ya no es tan cierto hoy como en el pasado. La compatibilidad entre versiones se ha convertido en algo fundamental para los desarrolladores. Además, si se va a realizar una modificación para restaurar el funcionamiento de una aplicación, en la mayoría de los casos, esta modificación permite resolver un problema importante de seguridad o rendimiento.

¿Cómo limitar el riesgo de infección del sistema de información?

Actualice los componentes del sistema de información

La única forma de prevenir este riesgo es aprender sobre el descubrimiento de nuevas vulnerabilidades para actuar rápidamente. Posteriormente, es importante aplicar los parches de seguridad a todos los componentes del sistema de información.. Se espera un retraso máximo de un mes después de la publicación del editor.

Política de actualización

También es recomendable definir una política de actualización que especifique: La forma en que se realiza el inventario de los componentes del sistema de información. Fuentes de información relacionadas con la publicación de actualizaciones. Las herramientas para implementar los parches en el parque. La posible calificación de las medidas correctoras y su despliegue progresivo en los equipos. Los componentes de fecha que ya no son compatibles con los fabricantes deben aislarse del resto del sistema . Esta medida

también afecta a la red (filtrado estricto de flujos) pero también a los secretos de autenticación (dedicados a estos sistemas).

Monitorear la obsolescencia del software utilizado

El uso de un sistema o software obsoleto representa un riesgo adicional de sufrir un ciberataque. Tan pronto como ya no se realizan parches en un sistema, este se vuelve vulnerable. Muchas herramientas maliciosas en la web aprovechan esta falta de parches de seguridad de los proveedores.

Aún existen precauciones para evitar la obsolescencia de estos sistemas

Crear y mantener un inventario de sistemas y aplicaciones de sistemas de información. Favorecer soluciones cuyo soporte esté garantizado al menos durante el tiempo de uso. Realice un seguimiento de las actualizaciones de software y las fechas de finalización del soporte. Mantener la homogeneidad de la infraestructura de TI. La acumulación de varias versiones de software puede causar problemas y por tanto complicar el seguimiento de la flota. Limite las dependencias operativas de un software a otro (adhesiones de software). De hecho, la duración del soporte de estas soluciones no es equivalente. Incluir en los contratos con los proveedores de servicios y cláusulas de supervisión de parches de seguridad y gestión de obsolescencia. Identificar los tiempos y recursos necesarios para la migración de cada software en fase de declive (prueba de no regresión, respaldo de datos y procedimiento de migración, etc.).

Leer también: Seguridad, ¿el talón de Aquiles del 5G? ; Gestión de crisis: ¿Cómo reaccionar en las horas posteriores a un ataque de Ransomware? ; Proxy o VPN, ¿Cuál elegir? ¿Qué nos conviene?