PC INNOVATION

IDEAS QUE NOS HACEN CRECER

PUNTOS DE SEGURIDAD PARA TUS SERVIDORES

33 4161 0710

HTTPS://SERVIDORES.PCINNOVATION.MX/

JESÚS DAVID GUZMÁN GALLEGOS

PRODUCT MANAGER SERVIDORES VIRTUALES

ELABORADO POR: DAVID GUZMÁN, ELEAZAR CARRILLO CAMARENA Y FECHA DE ÚLTIMA REVISIÓN: 04/10/2023

LAS BUENAS PRÁCTICAS EN INFORMÁTICA Y CIBERSEGURIDAD

Si queremos poder dormir tranquilos con un alta probabilidad de que nuestro servidor está en las mejores condiciones posibles de seguridad, debemos de trabajar de forma preventiva evitando lo siguiente:

1. Ataques cibernéticos.
2. Hackers.
3. Ransomware.
4. Virus.

Además, debemos de realizar las "buenas prácticas informáticas", que mejoran el rendimiento de tu servidor y reducir las fallas en procesos críticos de tu empresa, administrando los siguientes puntos:

1. Espacio en Disco Duro: tu espacio disponible no debe ser menor a un 10% de tu total de tu disco duro. Adicionalmente, deberás darle mantenimiento desfragmentando y optimizando así tu disco duro y generando espacio libre.
2. Procesamiento (CPU): No debe exceder al 99% en un lapso no mayor a 1 minuto.
3. Uso de la Memoria RAM: No debes de exceder el total de tu RAM disponible
4. Posibles daño en tu disco duro: Revisar la integridad de tu disco duro en caso de errores en sectores.
5. Servicios críticos: Actualizaciones de sistemas operativos, fallas en servicios propios de tus aplicaciones contables y comerciales.
6. Usuarios y sus privilegios: Tus usuarios solo cuenten con los permisos necesarios para abrir sus aplicaciones y sus archivos.
7. Contraseñas: Crea o solicita a tus usuarios contraseñas que cuenten con los requisitos que se solicitan en mejores prácticas de contraseñas.

PUNTOS DE SEGURIDAD PARA TU SERVIDOR

Para todo esto, es imprescindible realizar los siguientes 10 puntos de seguridad en tu servidor en el orden que a continuación presentamos:

1) Firewall.
Tener tu cortafuegos ACTIVO, configurar y habilitar SOLO los puertos necesarios a rangos de IP específicas y seguras, para que tus aplicaciones y servicios en tu servidor funcionen correctamente y de forma segura. TSPlus Advanced Security es un Software de protección contra hackers que permite realizar conexiones seguras a tu servidor, usando una combinación de whitelist, Bloqueos de IP y listas de IP de Hackers reportadas, es requisito indispensable tener FIREWALL activado para su correcto funcionamiento.

- Es necesario configurar reglas en el firewall de nuestro Sistema Operativo, con la finalidad de no habilitar todos los puertos o simplemente tenerlo inactivo, ya que esto expone gravemente a nuestro servidor de ataques.
- Configurar y administrar tu firewall fisico, modem o dispositivo que cumpla una función de cortafuegos
- Bloquear puertos que sean atacados comúnmente como puertos de escritorio remoto 3389, FTP 20 y 21, puertos orientados a servicios web 80, 8080, 8088, 8888 y 443, entre otros.

2) Permisos en usuarios
En un sistema operativo, los permisos o privilegios, son un derecho que sé les proporciona a los usuarios, para ejecutar un programa, realizar cambios en el sistema operativo, borrar un archivo, básicamente pueden permitir hacer o no hacer cualquier cosa en tu servidor.

Recomendaciones para los usuarios con privilegios o permisos de administradores:

- El usuario “administrador” solo debe de emplearse para mantenimientos de software, instalaciones o configuración de programas que requieran permisos elevados.
- Tener 2 usuarios administradores, 1 para temas administrativos y otro para respaldo del mismo usuario administrador.
- No usar usuarios administradores en ambientes operativos, ejemplo: “captura de pólizas en Contpaqi contabilidad o capturar y timbrar facturas”. El tener personas que no tienen un perfil de sistemas y que tengan privilegios de administrador en un servidor, puede ocasionar los siguientes problemas:
- Que se instalen aplicaciones de dudosa procedencia.
- Generar procesos que afecten tu servidor.
- Apagar o reiniciar tu servidor por error.
- Borrar todos tus datos o bases de datos, etc.

3) Contraseñas Seguras.

El uso de contraseñas seguras es un punto principal para la integridad de nuestro servidor, disminuye la probabilidad de que los hackers con métodos especiales obtengan tu contraseña de acceso. Evita que usuarios ajenos a tu servidor siguiendo las siguientes recomendaciones:

1. Contraseña 15 caracteres o más, utilizando mayúsculas, minúsculas, números y caracteres especiales, esto te ayudará a reforzar el acceso a tu servidor.
2. Cambia tu contraseña regularmente cada 3 meses.
3. Usa la Política de seguridad de tu Servidor para hacer obligatoria las políticas de seguridad de contraseñas para todos tus usuarios actuales y nuevos.TSPlus Advanced Security detiene rápidamente los ataques de hackers (brute force) a tu servidor y evitando que no tenga que procesar miles de intentos fallidos de inicio de sesión de intrusos.

4) Actualizaciones en su sistema operativo.

Es importante mantener tu sistema operativo con todas las actualizaciones, ya que en ellas nos proporcionan los parches de seguridad necesarios para asegurar los huecos de seguridad encontrados, programa la instalación de tus actualizaciones en un horario específico, no operativo, para el correcto funcionamiento de tu servidor y no se detenga tu operación.

.

5) Antivirus.

Cuenta siempre con un antivirus y que esté siempre actualizado, porque siempre estamos expuestos al incorrecto funcionamiento de nuestro servidor, ya sea descargando archivos o instalando programas, existen diversos antivirus, en los cuales se encuentra ESET, KASPERSKY, entre otros.

6) Licencias Originales.
Cuenta siempre con licencias originales para tus programas dentro del servidor, ya sea para tu sistema operativo, tu antivirus, paquetería ofimática, software administrativo, entre otros software de uso diario.

7) Fuentes no confiables.
Evita el acceso o utilización de correos en un Servidor, evita abrir correos con spam, no abras enlaces que puedan contener algún virus que pueda perjudicarte en tu servicio. Los usuarios operativos en un Servidor en la nube no deben tener acceso a exploradores web.

Aplicaciones que te pueden apoyar para las fuentes no confiables::

1. TSPlus Advanced Security: Te ayudará, entre otras muchas cosas, a que tus usuarios operativos no usen exploradores webs, regedit, power shell, además te ayudará a manejar escritorios seguros, donde solo podrán acceder a lo indispensable en su sesión dentro del servidor.

Evita el acceso a páginas bancarias desde un navegador no confiable o no reconocido, Evita recordar tus datos bancarios en cualquier navegador o sitio web, para esto diversos Antivirus cuentan con un navegador seguro para realizar tus transacciones de manera segura.

8) Autentificación de doble factor 2FA.
Se recomienda utilizar herramientas de doble autentificación con la finalidad de corroborar que el usuario sea el que se va a conectar y no algún otro usuario sin sus respectivas credenciales, esto ayudara a mejorar el acceso de personal a tu servidor así como te brindara una mejor seguridad. Esta autentificación de dos factores, podrás aplicarlo para tu inicio remoto, para ello existe 2FA de ts plus, Microsoft Authenticator, Google Autenthicator, solo por mencionar algunos.

9) Respaldos.

A pesar de contar con tu servidor en la nube, siempre es importante contar con respaldos en diversas plataformas, para ello es necesario emplear herramientas especiales para respaldos automatizados:

1. Servicios NAS en servidores dedicados.
2. Backups: Software de respaldos automáticos.
3. Procesos automáticos propios de servidores virtuales como son snapshots.
4. Respaldar tu información importante en plataformas como Google Drive, One Drive o servicios particulares como lo es un servidor FTP propio.

10) Monitorización Continua.

Debemos implantar en nuestra empresa un sistema que permita monitorizar la gestión de los datos y detectar aquellos posibles fallos o actuaciones incorrectas.

Remote Mananagement puedes monitorear el estado de tu firewall y configurar una alerta para cuando se desactive y a través de un script hacer que tu firewall se vuelva a encender, así como diversas funciones de monitoreo y mensajes o alertas para prevenir ataques o incidentes con tu servidor.

11) Capacitación continua y normatividad.

La capacitación continua no solo beneficia a los profesionales de la seguridad de la información, sino también a todos los empleados que interactúan con servidores virtuales. Los usuarios finales pueden ser la primera línea de defensa contra amenazas como el phishing y el malware. La capacitación regular sobre seguridad informática puede ayudar a crear una cultura de seguridad en la organización y reducir el riesgo de ataques exitosos.

Además de la capacitación, las auditorías periódicas son esenciales para evaluar la seguridad de los servidores virtuales. Las auditorías permiten identificar vulnerabilidades, configuraciones incorrectas o prácticas de seguridad deficientes que podrían ser explotadas por atacantes. Al llevar a cabo auditorías regularmente, las organizaciones pueden detectar y corregir problemas antes de que se conviertan en amenazas reales.

Las auditorías no solo ayudan a prevenir ataques, sino que también mejoran la capacidad de una organización para recuperarse de ellos. Al identificar debilidades y tomar medidas correctivas, una organización puede fortalecer su infraestructura y estar mejor preparada para enfrentar incidentes de seguridad. Esto reduce el tiempo de inactividad y el impacto en el negocio en caso de un ataque exitoso.