Ciberseguridad: 5 consejos sencillos para proteger tu servidor contra hackers

Prácticas recomendadas de endurecimiento de servidores para Windows y Linux

Willem L. Middelkoop
Mar. 10, 2018

Esta semana uno de mis clientes fue hackeado y me pidió asistencia de emergencia para ayudar a asegurar la infraestructura de su servidor. Era un servidor web que ejecutaba sitios web de WordPress en Apache (con PHP/MySQL), incluyendo algunas tiendas online con datos de clientes. Este hackeo podría haberse evitado fácilmente con las siguientes mejores prácticas, ¿está *su* servidor seguro?

El centro de datos es donde reside tu servidor. Aunque pueda ser físicamente seguro, ¡también deberías comprobar su software!

1) Instala menos software

La seguridad cibernética es bastante difícil, deberías hacértelo más fácil instalando menos software. Menos programas, servicios y plugins significan menos cosas de las que preocuparse. En terminología de seguridad cibernética, esto se llama reducir el vector de ataque.

Reduce tu vector de ataque:

- **comenzando con un sistema base mínimo**: no comiences con un sistema operativo completo e inflado, comienza con lo mínimo posible y realiza un seguimiento de las cosas que agregas
- **instala solo lo que absolutamente necesitas**: instala herramientas, plugins, complementos y programas que realmente - realmente - necesitas. Sé duro y decidido: ¡menos es más!
- **comprueba las dependencias de las cosas que instalas**: si instalas algo, asegúrate de verificar las dependencias; el software a menudo requiere otro software (que no necesariamente quieres)

2) Cierra todos los puertos de red, filtra los que no puedas bloquear

Los firewalls se utilizan para filtrar el tráfico de red y están disponibles como software de sistema estándar en la mayoría de los sistemas operativos. Limita las aperturas que los hackers tienen a tu servidor.

La configuración del firewall debe:

- **adoptar una política predeterminada de bloqueo:** la mayoría de los sistemas operativos permiten todo de forma predeterminada. Dale la vuelta a esto y bloquea todo excepto el tipo de tráfico que esperas y necesitas.
- **comprobar la entrada y la salida:** filtra el tráfico de red entrante y saliente. Esto hace que sea mucho más difícil para los hackers entrar (y salir, en el desafortunado caso de un ataque exitoso).
- **filtrar los puertos abiertos:** asegura los puertos de red abiertos filtrando el tráfico según la fuente (dirección IP) y/o el estado, solo permite el tráfico desde donde esperas que provenga.

3) Oculta toda la información de la versión

El software que ejecuta tu servidor tiene versiones, a menudo un número que indica la fecha exacta en que se creó. Los hackers pueden usar esta información de la versión para buscar problemas de seguridad conocidos, vulnerabilidades y debilidades.

Deja de ayudar a los hackers eliminando la información de la versión de:

- **servidores web:** Apache, NGINX, Microsoft Internet Information Services, etc. Comprueba tu servidor analizando las cabeceras HTTP.
- **servidores de correo:** Postfix, Exim, Dovecot, Sendmail, etc. A menudo, estos servidores comunican su versión en un "banner de saludo", que se muestra directamente después de establecer una conexión mediante SMTP, IMAP, POP3.
- **lenguajes web:** PHP, .NET, Java, etc. A veces, estos frameworks y lenguajes de scripting agregan su propia cabecera HTTP ("x-powered-by") con información de la versión.
- **WordPress:** plugins, temas, formularios, galerías, tiendas web, etc. La información de la versión a menudo se incluye en la salida HTML o en los nombres de archivo de CSS, JavaScript e imágenes.
- **servidores de archivos:** FTP, SFTP, WebDav, etc. Estos servidores comunican su información de versión en su saludo, que se muestra directamente al conectarse, a menudo antes de la autenticación.
- **SSH:** ¿Sabías que OpenSSH comunica la información de la versión del sistema operativo de forma predeterminada?

4) Usa autenticación de certificado/clave en lugar de contraseñas

Si se permiten los inicios de sesión basados en contraseña, los hackers pueden intentar acceder repetidamente al servidor. Con la potencia informática moderna, es fácil autom-

atizar estas adivinanzas probando combinación tras combinación hasta que se encuentra la contraseña correcta (fuerza bruta).

Autenticación segura mediante:

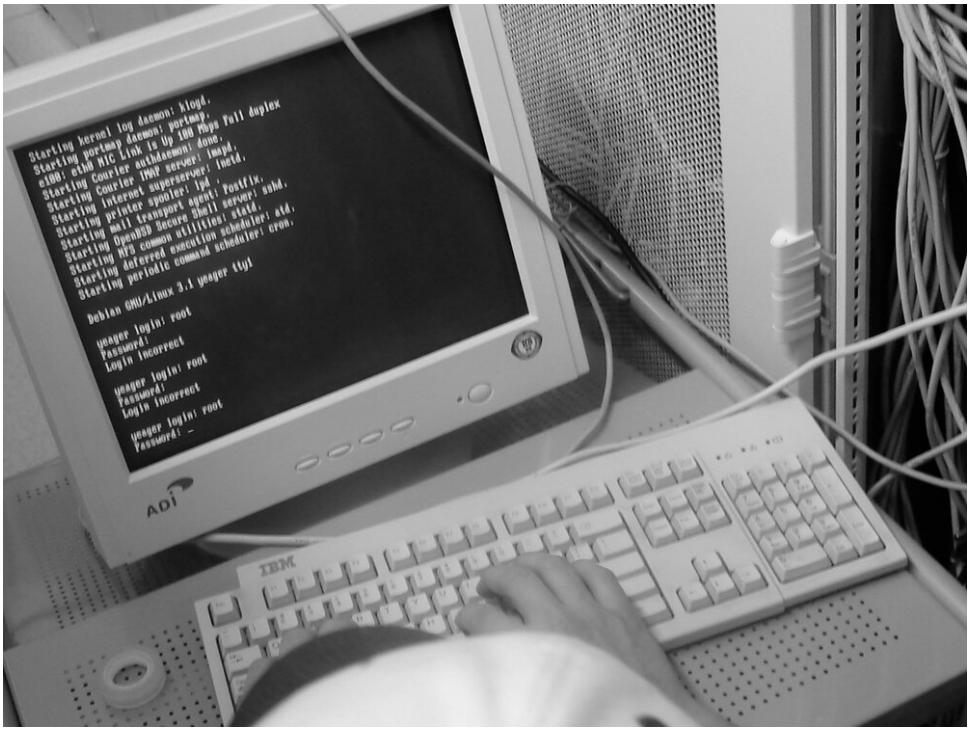
- **uso de autenticación de clave SSH:** una clave SSH es mucho más larga que una contraseña normal y contiene caracteres diferentes a las letras y números legibles ordinarios. Esto da como resultado más combinaciones posibles, lo que hace exponencialmente más difícil para los hackers encontrar la clave correcta.
- **limitar la tasa de autenticación:** ralentiza artificialmente la comprobación de la contraseña/clave, reduciendo la velocidad de las adivinanzas automatizadas.
- **bloquear las adivinanzas automatizadas:** excluye las direcciones IP si no han podido iniciar sesión correctamente.

5) Comprueba y actualiza regularmente

La mayoría de los hackeos están automatizados en estos días, los bots escanean constantemente cada servidor y sitio web en busca de oportunidades de explotación. No es una cuestión de *SI* te encontrarán, sino de *CUÁNDO*.

Cuida tu servidor:

- **comprobando sus registros:** los problemas potenciales a menudo se hacen visibles antes de que ocurran cosas realmente malas. Comprueba los registros del servidor en busca de errores y anomalías; a menudo son signos tempranos de problemas.
- **busca actualizaciones:** ya sea utilizando el software en tu servidor o consultando el sitio web del proveedor/software.
- **actualiza regularmente:** no esperes hasta que sea demasiado tarde, instala las actualizaciones lo antes posible (¡pero *después* de haberlas probado!)



Comprueba tu servidor regularmente, o encuentra a alguien que lo haga por ti.

Conclusión

Si implementas estas medidas, puedes mejorar enormemente la seguridad cibernética de tu servidor. Proteger tu servidor significa una mayor seguridad para tu negocio, tu organización y los datos de tus clientes.

Ningún consultor de seguridad (cuerdo) te ofrecerá garantías, dados los recursos y la determinación suficientes, los hackeos siempre serán posibles. Prepárate haciendo copias de seguridad y encriptando tus datos.

Espero que estos consejos te ayuden, si necesitas ayuda adicional, puedes encontrar mi información de contacto aquí o consultar mis servicios de seguridad cibernética.