WatchGuard

La Vulnerabilidad y la Administración de Parches

watchguard.com

Índice:

WatchGuard

La importancia de la administración de parches en las organizaciones

Los parches de software tienden a ser un problema para los administradores de TI. La priorización y la implementación de estos parches es una tarea que requiere de mucho tiempo, no solo para ellos, sino también para los usuarios. Las computadoras y los servidores deben reiniciarse con frecuencia, lo que lleva a interrupciones en el trabajo. Debido a esto, a veces las actualizaciones se posponen y se ignoran los parches recomendados. Sin embargo, lo que parece una acción inocente podría terminar teniendo serias consecuencias para las organizaciones.

Asimismo, los administradores de TI pueden tener serias dificultades para asegurarse de que todos los sistemas de su red tengan los parches necesarios instalados. Los parches y las actualizaciones de software son críticas cuando se trata de garantizar que una organización cuenta con una posición sólida de seguridad cibernética, ya que impiden que el software y los sistemas sean vulnerables a las amenazas de seguridad.

WatchGuard®

Vulnerabilidades en cifras

En 2020, profesionales, investigadores y proveedores de seguridad reportaron un total de 18.103 vulnerabilidades, con un promedio de 50 vulnerabilidades y exposiciones comunes (CVE) por día.[1] Según estas cifras, tal vez no debería sorprendernos que sea extremadamente difícil para las organizaciones con recursos de TI limitados mantener y proteger su infraestructura.

La administración de parches es una tarea que puede requerir una gran cantidad de tiempo y recursos y con frecuencia es difícil obtener un panorama general de sus activos y aplicaciones, priorizar los parches e incluso tener la capacidad de implementar parches con rapidez en programas y sistemas críticos. Las empresas deben poder administrar los parches con la mayor eficiencia posible, ya que de lo contrario podrían provocar un enorme impacto negativo en su productividad, así como en su seguridad cibernética.

24,1%[2] de las vulnerabilidades pertenecen a cinco empresas: Software in the Public Interest (SPI), SUSE, Oracle, IBM y Microsoft. Las aplicaciones de terceros que más se utilizan son el principal objetivo de los hackers. Según el índice de Vulnerabilidades y Exposiciones Comunes (CVE)[3], las aplicaciones como Java, Adobe, Google Chrome, Mozilla Firefox y OpenOffice, entre otras, poseen el número más alto de vulnerabilidades. Por lo tanto, no es suficiente solo implementar parches en los sistemas operativos.

Otro factor a considerar es el aumento en el número de atacantes con las habilidades necesarias para descubrir vulnerabilidades con mayor rapidez. Una vez que las encuentran, implementan programas que automatizan el uso de estas nuevas vulnerabilidades, las cuales se distribuyen de manera generalizada, a veces incluso de forma viral. El resultado de esta combinación de amenazas, vulnerabilidades y consecuencias implica un riesgo significativo para las empresas. Sin embargo, aunque pueda parecer sorprendente, no son las vulnerabilidades no detectadas las que plantean el mayor peligro.

Fuentes:
1. SCMagazine - Vulnerabilities hit record high in 2020, topping 18,000 (Las vulnerabilidades alcanzan un récord de 18.000 en 2020)
2. Alerta de ciberseguridad – TechRepublic
3. attack.mitre.org – MITRE

Vulnerabilidades conocidas, vulnerabilidades de alto riesgo

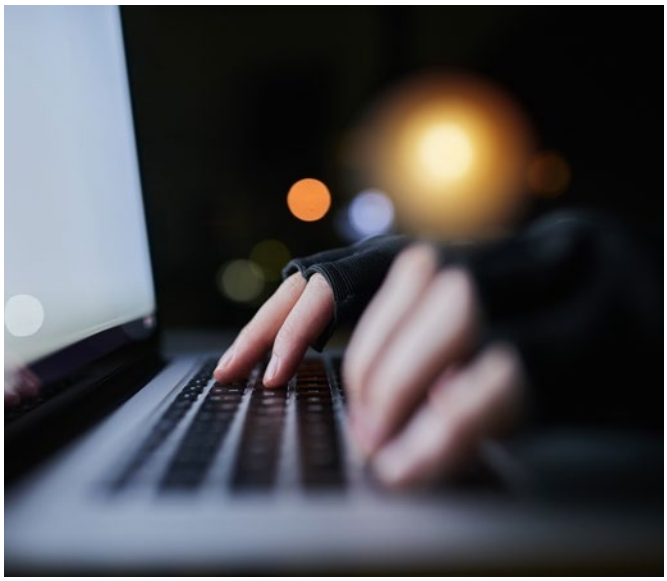
En la actualidad, el aprovechamiento de vulnerabilidades es aún la principal causa de la mayoría de las vulneraciones de seguridad. Los casos más notorios, como WannaCry, Petya y BlueKeep, que provocaron estragos a nivel mundial, todavía hoy siguen presentes en nuestra memoria. Solo un pequeño número de ataques ocurren como resultado de verdaderas vulnerabilidades desconocidas (ataques de día cero), debido a que la mayoría es ocasionada por vulnerabilidades conocidas.

El último año, los hackers aprovecharon vulnerabilidades conocidas y corregidas para atacar sistemas sin parches. Muchas de estas vulnerabilidades se habían dado a conocer en los dos años anteriores.[4] Por el contrario, las vulnerabilidades de día cero explican cerca del 0,4% de las vulnerabilidades de la década pasada.

Es importante recordar que los hackers también tienen acceso a vulnerabilidades públicas para perpetrar sus ataques, las cuales no dudan en aprovechar, sabiendo con claridad que la mayoría de las empresas no implementan parches en sus sistemas. De hecho, el 80% de los ataques exitosos aprovecha vulnerabilidades para las que existen parches conocidos que no se han implementado.

A la luz de estos hechos, es claro que las empresas deben concentrar sus esfuerzos en controlar y mitigar las vulnerabilidades conocidas que se aprovechan una y otra vez. Son estas vulnerabilidades las que implican un riesgo mayor y más real que otros tipos de amenazas.

El tiempo que transcurre entre el descubrimiento de una vulnerabilidad y el momento que se ejecutael ataque se ha reducido de manera considerable, lo que obliga a las empresas a trabajar contra reloj para implementar parches antes de que los criminales cibernéticos puedan poner en peligro a sus sistemas mediante el uso de una serie de vectores de ataque.



El 57% de las víctimas de ataques cibernéticos sostiene que aplicar un parche hubiera impedido el ataque. El 34% comenta que sabía sobre la vulnerabilidad antes de que ocurrieran los ataques cibernéticos.[5]

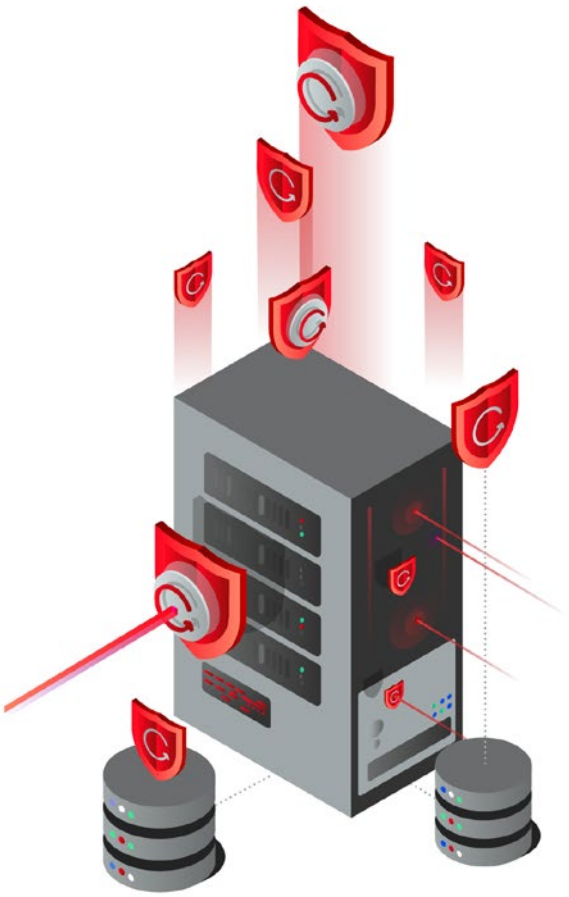
Fuentes:
4. Agencia de Ciberseguridad y Seguridad de Infraestructuras – CISA
5. Costo y consecuencias de las brechas en la respuesta a las vulnerabilidades – Ponemon

WatchGuard

Administración de parches

A/ ¿QUÉ IMPLICA LA ADMINISTRACIÓN DE PARCHES?

Es el proceso por el cual las empresas, o más específicamente sus departamentos de TI, descargan e instalan parches (cambios en el código o los datos) con la intención de actualizar, optimizar o proteger el software, las computadoras, los servidores y los sistemas. El objetivo es garantizar que estos componentes funcionen de manera adecuada o mitigar las vulnerabilidades de seguridad. Aunque pueda parecer una tarea simple, a la mayoría de las empresas les cuesta identificar qué actualizaciones de parches críticas deben instalar primero. Por lo tanto, priorizar los parches es clave para los administradores. De hecho, según Ponemon, el tiempo promedio que demoran las empresas en implementar parches en las aplicaciones o sistemas es de 97 días.[6] Sin embargo, el tiempo promedio de demora en detectar un ataque cibernético una vez que se implementa un parche para una vulnerabilidad de seguridad crítica es de 43 días,[7] lo que significa que existe una brecha de riesgo promedio de 59 días.



Fuentes:
6. Estado de riesgo de seguridad de endpoints 2020 – Ponemon
7. Costo y consecuencias de las brechas en la respuesta a las vulnerabilidades – Ponemon

B/ ¿QUÉ TIPOS DE PARCHES EXISTEN?

Existen diferentes tipos de parches, cada uno de ellos desarrollado para un propósito específico: para corregir un error o vulnerabilidad específica. Estos son solo algunos ejemplos: Revisión, parches de servicio, versiones de mantenimiento, parches de Monkey, etc.

En este documento nosconcentraremos en los dos tipos que consideramos los más importantes, ya que su objetivo es corregir vulnerabilidades de seguridad críticas que por lo general son las más utilizadas por los atacantes y que por lo tanto son las más importantes para las empresas y los expertos en seguridad.

- **Los parches de seguridad afectan tanto a los sistemas operativos como al software de terceros:** Un parche de seguridad es un cambio que se realiza en una aplicación o programa para corregir errores o defectos que provocan vulnerabilidades. Implementar este tipo de parches evita que puedan utilizarse las vulnerabilidades o bien elimina o mitiga la capacidad que tienen las amenazas de aprovechar la vulnerabilidad de un activo. La administración de parches es parte de la administración de vulnerabilidades: la práctica cíclica de identificar, clasificar, corregir y mitigar vulnerabilidades (riesgos de seguridad).

- **Paquete de Servicios (SP) o Paquete de Funcionalidades (FP):** Estos son parches importantes formados por una recopilación de actualizaciones, correcciones o mejoras de funcionalidades para un elemento de software. Suelen resolver varios problemas pendientes y por lo general incluyen todos los parches, las revisiones, los parches de mantenimiento y seguridad lanzados antes del paquete de servicios.

C) ¿CUÁL ES EL PROPÓSITO DE LOS PARCHES?

Los parches están diseñados para reparar una vulnerabilidad o brecha de seguridad identificada después del lanzamiento de una aplicación o un elemento de software.

El software sin parches puede dejar expuestos a todos los endpoints a vulneraciones, al dar a los hackers una gran oportunidad de lanzar ataques eficaces. Los parches de software son un componente crítico de las operaciones para los administradores y los expertos en seguridad.

En la industria de la tecnología, y en especial en la industria del software, es frecuente que, una vez lanzada la aplicación, esta deba corregirse o incluso modificarse. Por este motivo, es buena idea desarrollar un proceso similar al del ciclo de vida del software, en el que se establecen diferentes fases para permitir el análisis, la evaluación y la aplicación regular de parches para resolver cualquier problema que pueda surgir.

Ciclo de Vida de Administración de Parches

La administración de parches puede ser la herramienta más efectiva para proteger a su empresa contra vulnerabilidades y la menos costosa de mantener si se la implementa de manera eficiente. En esta sección, explicaremos cómo establecer un procedimiento de administración de parches de rutina, con el objetivo de integrarlo a las operaciones estándarde su empresa. En este ciclo o procedimiento, existen seis fases.[8]

Aplicabilidad:

Los parches publicados no siempre son válidos para todos los dispositivos. Esto significa que es importante controlar si una actualización específica es apropiada para los activos de su proceso.

Adquisición:

Obtener el archivo de actualización de una fuente oficial, así como controlar que el parche sea legítimo, no siempre es sencillo. El uso de hashes no es frecuente para parches relacionados con sistemas de control.

Identificación de activos y software base:

La identificación de activos y del software base instalado en ellos, así como su nivel de parches, es una tarea compleja, pero mejora tanto la seguridad como la operatividad. Contar con esta base le permite realizar cambios al sistema sin riesgos y volver a un estado funcional previo conocido en caso de que haya un problema al instalar una actualización o un parche.

Validación:

El objetivo de la validación es garantizar que la actualización notenga un impacto negativo en el proceso. Para validar el parche o actualización, se deben utilizar los activos de prueba y se deben seguir las fases de implementación. La validación tiene el fin de verificar qué consecuencias podría tener la actualización, lo que podría incluir cambios en las políticas de firewall, cambios de configuración, etc.

Disponibilidad:

La lista actual de parches se debe revisar en base al inventario de activos y software, con la identificación de aquellos parches que afectan a cada activo.

Implementación:

Se debe crear un paquete de implementación en el proceso de validación. El paquete debe contener los archivos de actualización y las instrucciones de instalación, así como una lista de activos donde debe realizarse la implementación.

WatchGuard

Fuentes:
8. Administración de parches en sistemas de control – INCIBE-CERT

Mantenga las vulnerabilidades conocidas lejos de la infraestructura de TI con WatchGuard Patch Management

WatchGuard Patch Management es una solución que simplifica el complejo ciclo de vida de administración de parches para los sistemas operativos y el software de terceros. En consecuencia, se reduce la superficie de ataque y se fortalece la capacidad de prevenir y contener los incidentes provocados por las vulnerabilidades del sistema.

La solución está integrada a las soluciones de seguridad de endpoints de Seguridad de WatchGuard, lo que significa que no requiere de nuevos agentes o consolas de administración. Ofrece visibilidad centralizada en tiempo real del estado de las vulnerabilidades, los parches, las actualizaciones pendientes y los programas de software no compatibles o en fin de ciclo de vida (EOL) en computadoras y servidores, tanto dentro como fuera de la red corporativa. Sus herramientas de administración le permiten automatizar la detección, la programación, la instalación y la supervisión de los parches y actualizaciones críticas que su organización necesita, todo en tiempo real y en un formato simple e intuitivo.

Los principales beneficios y funcionalidades de WatchGuard Patch Management

- Capacidad de auditoría, supervisión y priorización de actualizaciones para los sistemas operativos y las aplicaciones. Le permite ver el estado de los parches y las actualizaciones pendientes para el sistema y cientos de aplicaciones de terceros e incluso le permite revertir parches.
- Evita incidentes al reducir de manera sistemática la superficie de ataque que provocan las vulnerabilidades. La administración de parches y actualizaciones le permite adelantarse a los ataques de vulnerabilidades.
- Contiene y mitiga ataques que aprovechan vulnerabilidades, con la implementación inmediata de actualizaciones críticas desde la consola en la nube. La consola correlaciona detecciones con vulnerabilidades y de este modo minimiza el tiempo de respuesta, contención y corrección, mediante la implementación de las actualizaciones necesarias desde la consola. Además, le permite aislar las computadoras afectadas de la red y contiene tanto los ataques reales como los potenciales.
- Reduce los costos operativos, ya que no requiere implementaciones o actualizaciones de agentes en los endpoints, lo que simplifica la administración sin sobrecargar las computadoras o los servidores. Minimiza el esfuerzo de actualizaciones remotas desde la consola en la nube. Visibilidad inmediata y automática de vulnerabilidades, actualizaciones y aplicaciones en fin de ciclo de vida.

WatchGuard

La administración de parches es un proceso que debe realizarse de manera regular y debe ser lo más completo posible para ser efectivo. No obstante, esto no significa que todos los sistemas deben tratarse de la misma manera; todas las empresas deben priorizar sus activos y garantizar que se proteja a los más importantes primero.

De todos modos, es importante asegurarse de que los parches se implementen en todos los equipos y no solo en aquellos que sean más valiosos o importantes para la empresa. Además, los parches no solo requieren un esfuerzo por parte de los administradores del sistema, sino que también pueden requerir el soporte de la empresa que debe acordar una ventana de mantenimiento específica.

Protección de Ataques

Arquitectura Adaptable de Seguridad

WatchGuard

Descubra cómo WatchGuard Patch Management puede ayudarlo a simplificar la administración de vulnerabilidades mediante la optimización del proceso de actualizaciones y parches de seguridad.

Para obtener más información visite nuestro sitio web

WatchGuard

VENTAS EN NORTEAMÉRICA 1.800.734.9905 VENTAS INTERNACIONALES 1.206.613.0895 SITIO WEB www.watchguard.com