ivanti

DATASHEET

Retos en la gestión de parches

Resultados de la encuesta y opiniones sobre el paso de las organizaciones al Everywhere Workplace

Introducción

Los entornos de trabajo actuales ya no se limitan a un espacio cerrado en el que los puestos de trabajo con ordenadores controlados por el área de IT son el centro de la productividad. Hoy en día, las empresas están más distribuidas que nunca, lo que da lugar a mayor probabilidad de ataques. En el Everywhere Workplace, los empleados se conectan mediante diferentes dispositivos para acceder a las redes, los datos y los servicios corporativos a medida que trabajan y colaboran desde nuevos y diferentes lugares, por lo que la aplicación de parches nunca ha sido tan compleja como en la actualidad.

Mientras tanto, los equipos de IT y de seguridad se esfuerzan por mantener bajo control el panorama del trabajo a distancia, que se amplía constantemente. Mantener el nuevo espacio de trabajo en línea seguro y actualizado con los últimos parches de seguridad es necesario, aunque cada vez es mayor el reto.

Los retos

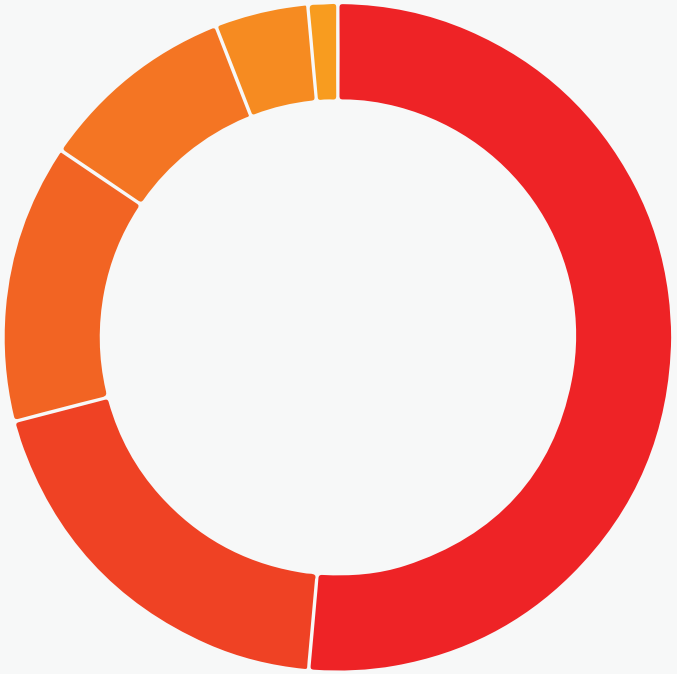
Un nuevo estudio de Ivanti ha revelado que el 71% de los profesionales de la informática y la seguridad consideran que la aplicación de parches es demasiado compleja y requiere mucho tiempo. A medida que los ciberatacantes maduran sus tácticas y convierten en armas las vulnerabilidades, especialmente las de ejecución remota de código, las empresas se enfrentan al riesgo de la superficie de ataque y a las formas de acelerar las acciones de parcheo y reparación.

Los profesionales de la informática y la seguridad apenas pueden responder con la suficiente rapidez; el 53 % de los encuestados aseguró que organizar y priorizar las vulnerabilidades les ocupa la mayor parte de su tiempo. La situación es alarmante, ya que cuanto más tiempo permanezcan las vulnerabilidades sin parchear, más expuesta estará una empresa al riesgo de sufrir un ataque o un ransomware. Sin embargo, no existe ninguna empresa con capacidad para parchear todos sus puntos de exposición, por lo que la priorización basada en el riesgo debe realizarse rápidamente para adelantarse a los ataques automatizados de los adversarios. Hoy en día, las vulnerabilidades sin parchear siguen siendo uno de los puntos de infiltración más comunes para los ataques de ransomware, los cuales han aumentado en frecuencia e impacto para empresas de todos los tamaños.

Los equipos de IT y seguridad también dedican gran parte de su tiempo a emitir resoluciones para parches fallidos (19 %), a probar parches (15 %) y a coordinarse con otros departamentos (10 %). La gran cantidad de retos a los que se enfrentan los equipos de seguridad a la hora de aplicar parches puede ser la razón por la que el 49 % de los encuestados cree que los actuales protocolos de gestión de parches de su empresa no consiguen mitigar el riesgo de forma eficaz.

Los profesionales de la informática y la seguridad afirmaron que gastan la mayor parte de su tiempo al mes en las siguientes actividades:

- **53%** - Organizar y priorizar las vulnerabilidades
- **19%** - Resolución de problemas por parches fallidos
- **15%** - Parches de prueba
- **10%** - Coordinación con otros departamentos
- **3%** - Cumplimiento
- **1%** - Mantenimiento de registros



Las causas

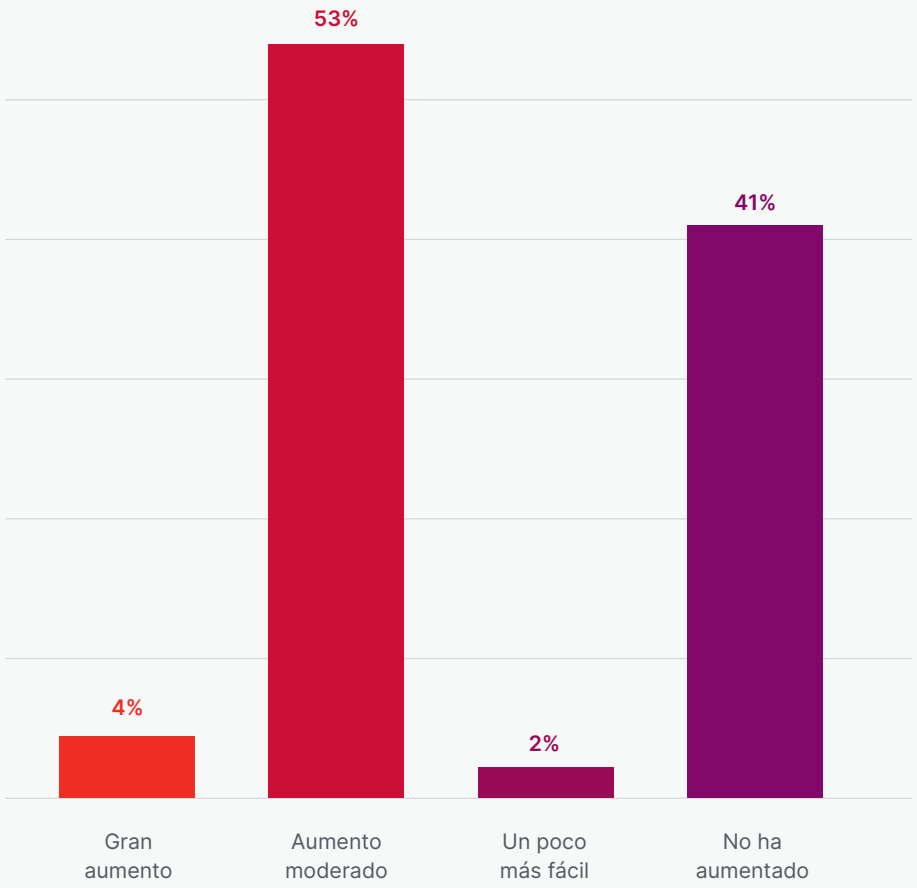
La mayoría (57 %) de los encuestados considera que la transición global hacia un espacio de trabajo descentralizado ha hecho más compleja la gestión de parches. La escala de la gestión de parches también ha aumentado con el alto número de endpoints disponibles para los usuarios y los sistemas críticos para el negocio que los soportan, desde Windows a macOS, Linux a los servidores de Windows, y más.

Además, algunos sistemas informáticos son difíciles de parchear porque provocan interrupciones. Un alarmante 61 % de los profesionales de la informática y la seguridad afirmaron que reciben peticiones de los propietarios de las líneas de negocio para posponer las ventanas de mantenimiento 1 vez al trimestre. Otro 28 % afirma que recibe este tipo de solicitudes 1 vez al mes.

Al mismo tiempo, la velocidad de armamento de las vulnerabilidades sigue aumentando, especialmente para aquellas con capacidad de permitir la ejecución remota de código (RCE). Es la tormenta perfecta de la escasa visibilidad debido al teletrabajo y al work from anywhere y al crecimiento de los actores de amenazas que encuentran y utilizan rápidamente las vulnerabilidades explotables.

Además, muchas empresas carecen de la experiencia en seguridad o del tiempo necesario para permitir que sus recursos recopilen información sobre amenazas y asignen las amenazas de explotación activa con las vulnerabilidades abiertas en su organización para lograr un contexto de amenazas basado en el riesgo. La escasez de personal IT ha reducido la capacidad de mitigar los problemas de seguridad administración y gestión para muchas empresas. Y para estas empresas, los ciberataques, en particular el ransomware, son los más devastadores.

¿En qué medida el trabajo a distancia ha aumentado la complejidad y la escala de la de parches en su empresa?



El entorno de las amenazas

A medida que los equipos de IT luchan por lidiar con una mayor superficie de ataque, los hackers informáticos perfeccionan sus tácticas y vigilan los puntos en los que las empresas presentan riesgos de exposición a la vulnerabilidad. Buscan el equilibrio entre la perseverancia y la paciencia con el uso sofisticado de exploits, herramientas y tecnología emergente. Su principal objetivo es perturbar, robar y actuar para obtener ganancias monetarias explotando los negocios de las empresas.

Otra encuesta de Ivanti revela que el 63 % de los encuestados afirma que sus empresas han sufrido un ataque de ransomware en el último año. Y el 89 % de los encuestados señaló que los portátiles, los ordenadores de escritorio y los dispositivos móviles eran los dispositivos más buscados.

Los hackers están siempre al acecho de las vulnerabilidades y los equipos de IT y de seguridad se esfuerzan por priorizar sus esfuerzos de gestión de parches para poder resolver rápidamente la exposición al riesgo de vulnerabilidad.

El ataque del ransomware de tipo WannaCry, que encriptó unos 200.000 ordenadores en 150 países, sigue siendo un ejemplo, incluso después de cuatro años, de las graves repercusiones que pueden producirse cuando no se aplican rápidamente los parches. El parche para la vulnerabilidad explotada existía desde varios meses antes del ataque inicial, pero muchas organizaciones no lo aplicaron. Y hasta la fecha, dos tercios de las empresas aún no han parcheado sus sistemas. Sin embargo, las empresas de todo el mundo siguen siendo víctimas de los ataques del ransomware de tipo WannaCry; de enero a marzo de 2021 se produjo un aumento del 53% en el número de organizaciones afectadas por el ransomware WannaCry.

Crear un contexto de confianza para la gestión de la seguridad y los riesgos

El panorama laboral en expansión y la transformación digital continuarán. Ahora bien, es necesario que haya una forma de ampliar el contexto Zero Trust para la seguridad y la gestión de riesgos.

Implantar un marco Zero Trust es primordial para proteger los datos sensibles de la empresa de accesos no autorizados y de ataques cibernéticos. En su versión más sencilla, Zero Trust proporciona a las organizaciones una evaluación continua de los dispositivos de sus empleados, de los endpoints, los activos y las redes de los que depende la empresa.

En mayo de 2021, el presidente Biden firmó una Orden Ejecutiva que establece que las agencias federales deben desarrollar planes para implementar una estrategia de seguridad Zero Trust. La seguridad Zero Trust también es una prioridad para los profesionales de IT y ciberseguridad: según un estudio reciente realizado por Ivanti, el 98 % de los profesionales norteamericanos de IT y seguridad manifestaron que sus prácticas de seguridad se alinearán más con la estrategia Zero Trust durante el próximo año.

El contexto Zero Trust examinará el aspecto del riesgo para los dispositivos, los endpoints y los activos que se utilizan en el Everywhere Workplace. Se prevé que entender qué nivel de riesgo de vulnerabilidad es aceptable y qué parches deben aplicarse para cumplir los requisitos de confianza establecidos por la empresa aumentará el valor de la gestión de parches basada en el riesgo.

Los principales líderes de la industria, los profesionales y las empresas de análisis recomiendan un enfoque basado en el riesgo para identificar y priorizar los puntos débiles de la vulnerabilidad y acelerar la eficacia de la reparación. La Casa Blanca publicó recientemente un memorando en el que anima a las empresas a utilizar una estrategia de evaluación basada en el Zero Trust para impulsar la gestión de parches y reforzar la ciberseguridad contra los ataques de ransomware. Además, Gartner incluyó la gestión de la vulnerabilidad basada en el riesgo como uno de los principales proyectos de seguridad en los que los profesionales de la seguridad y la gestión de riesgos deberían centrarse en 2021 para impulsar el valor empresarial y reducir el riesgo.

Conclusión

Si bien la productividad ha aumentado en el Everywhere Workplace, las amenazas también se han disparado. En este ecosistema disperso, los empleados utilizan varios dispositivos para acceder a los datos, las redes y las aplicaciones de la empresa para seguir trabajando desde cualquier lugar y en cualquier momento. Estos puestos de trabajo descentralizados son más propensos a sufrir amenazas importantes por parte de los ciberatacantes, que están aprovechando el cambio repentino a un espacio de trabajo sin perímetro y o lo utlizan como conducto para infiltrarse en las empresas.

El Everywhere Workplace exige un enfoque de la seguridad y la gestión de riesgos que evalúe continuamente el contexto actual para establecer la confianza que se basa en un análisis activo basado en el riesgo. Gracias al acceso a la mejor inteligencia sobre vulnerabilidades y parches que incluye explotaciones de vulnerabilidades activas en la naturaleza, vulnerabilidades con vínculos con el ransomware, datos de sentimiento sobre la fiabilidad de los parches, Ivanti está ampliando las herramientas que los equipos de IT y de seguridad pueden desplegar sin problemas y mejorando la eficacia de la seguridad y la gestión de riesgos de su organización.

Para más información, lea nuestro blog e inscríbase en la serie de seminarios web Ivanti Patch Tuesday Y escuche el podcast de Ivanti Insights, "La siguiente evolución de la gestión de parches: No intente parchearlo todo".

ivanti

ivanti.com
1 800 982 2130
sales@ivanti.com

1. i. Smarter with Gartner, Gartner Top 10 Security Projects for 2020-2021, February 22, 2021
2. ii. GARTNER is a registered trademark and service mark of Gartner, Inc. and/or its affiliates in the U.S. and internationally and is used herein with permission. All rights reserved.