

LA MITAD DE LAS EMPRESAS EUROPEAS SON VULNERABLES A ATAQUES INFORMÁTICOS.

Un estudio de McAfee revela la existencia del elevado grado de desprotección de las empresas desde que se produce un ataque hasta que aplican el parche adecuado.

En España la mitad de las empresas no priorizan las áreas críticas, prioritarias a la hora de aplicar parches frente a una vulnerabilidad.

McAfee, Inc. (NYSE: MFE), líder en soluciones de Prevención de Intrusiones y de Gestión de Riesgos, ha anunciado los resultados de un estudio realizado que revela el grado de desprotección de las compañías a la hora de gestionar parches de seguridad. Casi la mitad (el 45%) de las empresas encuestadas afirmaron que su infraestructura informática nunca está protegida al 100% frente a las vulnerabilidades.

El estudio de McAfee, dirigido por Ipsos Research, se realizó sobre una muestra de 600 ejecutivos TI europeos pertenecientes a compañías de más de 250 empleados. Su objetivo era analizar la dinámica de respuesta de las empresas ante el anuncio de una vulnerabilidad en su sistema. Las conclusiones del estudio revelan que:

- ° Más de un cuarto de los encuestados (27%) respondieron que les lleva 48 horas o más proteger totalmente su infraestructura desde el momento en que se publica un parche y el momento en que la infraestructura informática está totalmente protegida con respecto a esta vulnerabilidad. Uno de cada cinco (19%) afirmó que tardan hasta una semana o más.
- ° Más de un tercio (36%) de las empresas encuestadas en Europa no sabe cuántos parches han aplicado en sus empresas a lo largo de 6 meses.
- ° El 58% de los profesionales TI encuestados reconocieron no saber cuánto le está costando a su empresa la aplicación de parches.
- ° Uno de cada cinco profesionales TI declaró invertir una hora o más al día en la investigación de vulnerabilidades y parches.
- ° El 45% de los encuestados reconocieron no priorizar que áreas de la empresa se consideran prioritarias para parchearlas primero. En España esta cifra asciende al 50%.

En el entorno actual, donde las amenazas TI son cada vez más rápidas y perfeccionadas, la complejidad del proceso de gestión de parches es una preocupación importante para muchas grandes organizaciones. El tiempo que transcurre entre la descarga de un parche y su plena aplicación deja a la compañía vulnerable a infracciones de seguridad, caídas masivas, pérdida de productividad y, en último término, a la pérdida de la confianza de los clientes.

Un proceso que consume tiempo

El desarrollo de parches es un proceso complicado, especialmente para las grandes organizaciones, donde puede requerir incluso días de investigación, pruebas y aplicación para cada parche. El estudio de McAfee revela que el 20% de los encuestados dedica una hora o más al día a la gestión de vulnerabilidades. En Italia, casi un tercio (31%) de los encuestados invierte este tiempo al día en investigar vulnerabilidades, frente al 24% de Alemania. En Europa, uno de cada diez profesionales informáticos dedica 240 horas al año a investigar vulnerabilidades, lo que equivale a 5 semanas de

trabajo dedicadas por entero a esta actividad.

Una ventana de vulnerabilidad en continua expansión

El tiempo empleado en implementar parches deja a las empresas abiertas a la recepción de ataques. En Europa, más de un cuarto de los encuestados admitieron que la ventana desde que se publica un parche hasta que la infraestructura informática está totalmente protegida es de 48 horas o más. Una de cada diez (19%) empresas europeas, afirmó que tardan hasta una semana en aplicar los parches. Donde más tiempo dura la ventana de vulnerabilidad es en Francia, donde más de un cuarto (27%) de los encuestados tardan más de una semana en proteger a su empresa de una vulnerabilidad.

El coste de la gestión de parches

Sorprendentemente, el estudio revela el desconocimiento de muchos de los profesionales TI con respecto al número de parches que aplican y el coste que esto supone para sus empresas. El número de parches que se aplican es tan elevado que más de un tercio (36%) de las empresas encuestadas en Europa no sabe cuántos se han aplicado en sus empresas en un período de 6 meses, y el 58% reconoció no saber cuánto le está costando a su empresa este proceso. Asimismo, IDC prevé que el mercado Europeo de gestión de parches alcanzará los 88 millones de dólares en 2010[1].

Lo que está claro, en cualquier caso, es que la mayoría de los profesionales encuestados opinan que necesitarán dedicar más recursos a la gestión de parches en el futuro. Más de la mitad (54%) estarían dispuestos a invertir más en este área, un dato que en el caso de las empresas de Alemania alcanza el 68% liderando los planes de aumentar sus recursos en este ámbito.

Priorizando la protección

En el entorno actual las empresas necesitan instaurar sistemas de gestión de parches que reflejen la realidad de unos recursos informáticos limitados y de unas amenazas cada vez más perfeccionadas. En la raíz de este planteamiento debe hallarse la identificación de los activos que son esenciales para el negocio y la priorización de los recursos para proteger en primer lugar a dichos activos. El estudio de McAfee revela una tendencia creciente en la adopción de esta práctica. El 45% de los encuestados prioriza aquellas áreas de negocio donde los parches se aplican en primer lugar. Sin embargo, la investigación aún señala la existencia de un importante porcentaje de empresas que no asigna prioridades a efectos de la aplicación de parches, como es el caso de España, donde la mitad de las empresas encuestadas (50%) no lleva a cabo esta práctica de priorización de áreas.

Para obtener una adecuada protección, las empresas deberían combinar el proceso de priorizar la gestión de parches con soluciones de bloqueo proactivo, protegiendo así a las redes frente a las amenazas conocidas como a las desconocidas, lo que daría a las empresas un tiempo extra para la investigación y la aplicación de parches.

Cumplimiento de las normativas

La gestión de parches es también crítica para las empresas ya que pueden impactar en el cumplimiento de una serie de normas gubernamentales como la Sarbannes Oxley, la HIPPA o la MiFID. De acuerdo a estas legislaciones, el hecho de no aplicar el parche más reciente para proteger a los sistemas podría representar una infracción de la ley y tener serias implicaciones. En Europa la mayoría de las organizaciones han dado los pasos necesarios para cumplir la normativa de la administración. El 82% de los encuestados en la investigación de McAfee confían en que su política de gestión de parches la cumple.

El feedback que nos llega de las grandes compañías no deja lugar a dudas la gestión de parches es una seria preocupación para ellas , afirma John Parker, Director de la Línea de Productos de

McAfee para la Prevención de Intrusiones en la región de EMEA. Las organizaciones son vulnerables a los ataques TI porque estamos sumidos en una dinámica cada vez más rápida de desarrollo y aplicación de parches. En este entorno cambiante, la única solución para mitigar este riesgo y dar tranquilidad a los ejecutivos en el área de seguridad, es combinar el proceso de priorizar la gestión de parches con soluciones proactivas de prevención de intrusiones.

Nota a los editores

La investigación fue dirigida por Ipsos Research entre 600 profesionales TI de Reino Unido, Francia, Alemania, Italia, España y Holanda en noviembre de 2005.

McAfee, Inc.

www.mcafee.com/es

Fecha artículo: 2006-04-26 09:31:13 - url artículo: <http://www.internautas.org/html/743.html>

Logos y marcas propiedad de sus respectivos autores.

Los comentarios son propiedad y responsabilidad de cada autor.

© 1998-2009 Asociación de Internautas - <http://www.internautas.org>

Inscrita en el Registro Nacional de Asociaciones con el número 164343 - e-mail: asociacion@internautas.org