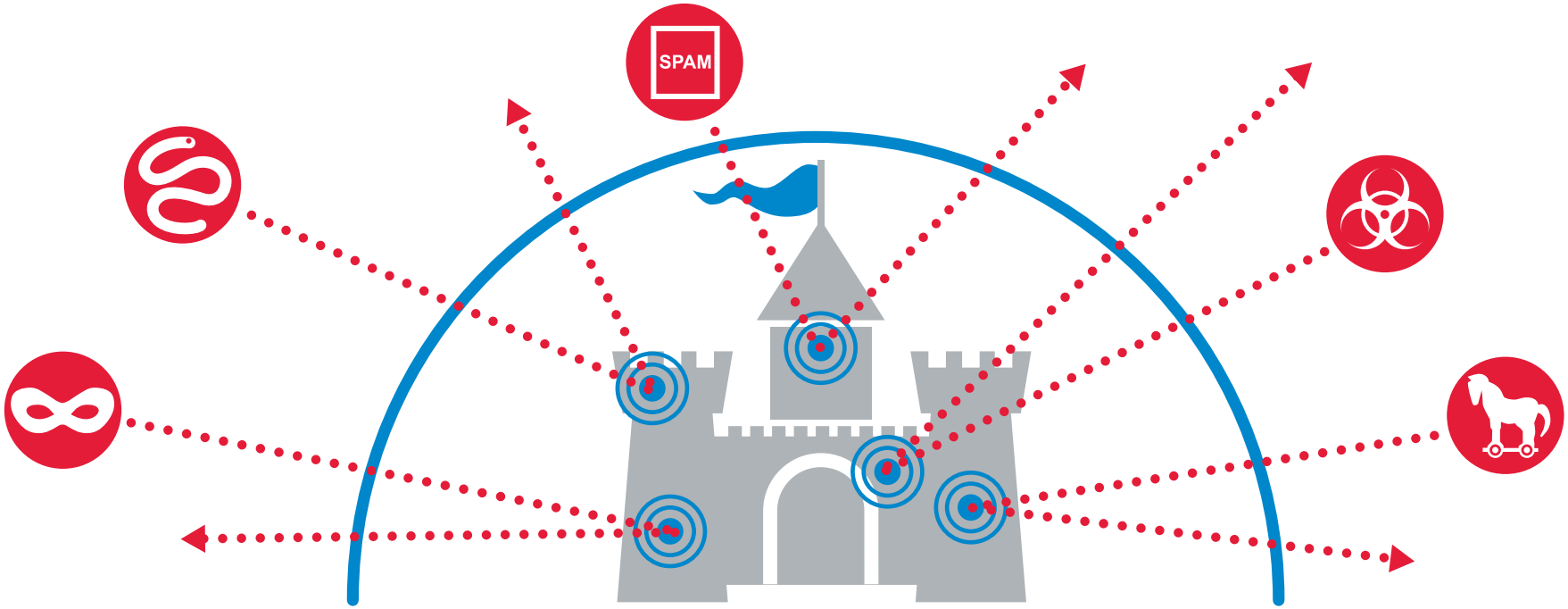
Tipos de ciberataques

y claves para prevenirlos

Introducción

Los ciberdelincuentes actuales emplean diversas técnicas complejas para evitar ser detectados mientras tratan de *colarse* en las redes corporativas con un fin: robar propiedad intelectual. Suelen cifrar las amenazas con complicados algoritmos para eludir su detección por parte de los sistemas de prevención de intrusiones. Una vez encontrada la vulnerabilidad del objetivo, los atacantes intentan descargar e instalar malware en el sistema expuesto. Es habitual que se sirvan de nuevas variantes evolucionadas del malware que las soluciones antivirus todavía no conocen.

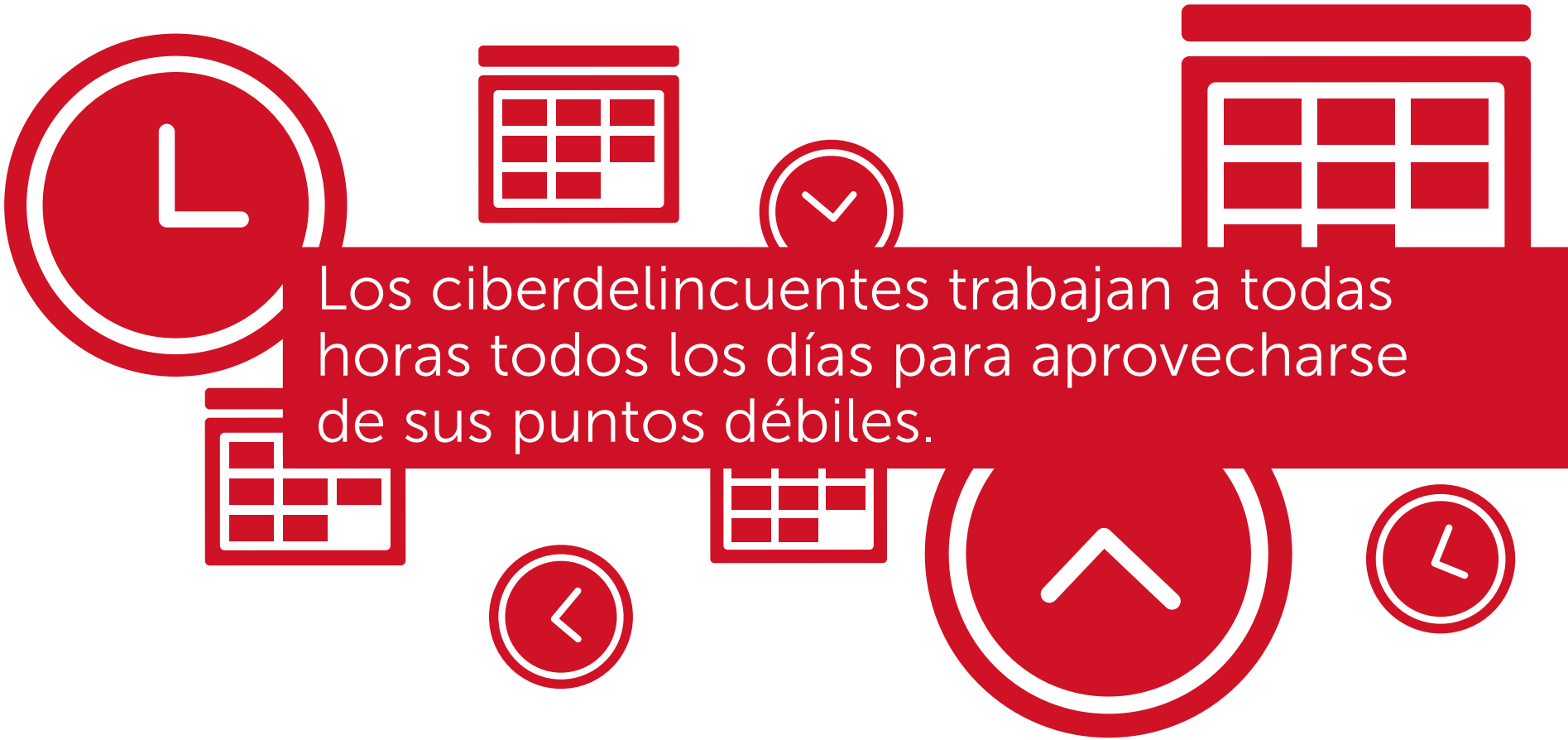
Este libro electrónico recoge las estrategias y las herramientas utilizadas por los ciberdelincuentes para infiltrarse en su red, así como las claves que le ayudarán a detener sus avances.



Estrategia de ciberataque n.° 1

Bombardear incesantemente las redes con malware

Muchos proveedores de firewalls de nueva generación (NGFW) ofrecen algún tipo de tecnología antimalware basada en red dentro de un enfoque de seguridad de varios niveles. Sin embargo, la mayoría de estos sistemas tienen un límite: de 5000 a 30 000 firmas de malware que residen en la memoria integrada del sistema del NGFW. El problema de este enfoque radica en que un gran número de ellos reciben nuevas actualizaciones de protección contra malware una vez al día. Esta frecuencia es insuficiente y deja las redes expuestas a toda una serie de ataques continuados que evolucionan constantemente.

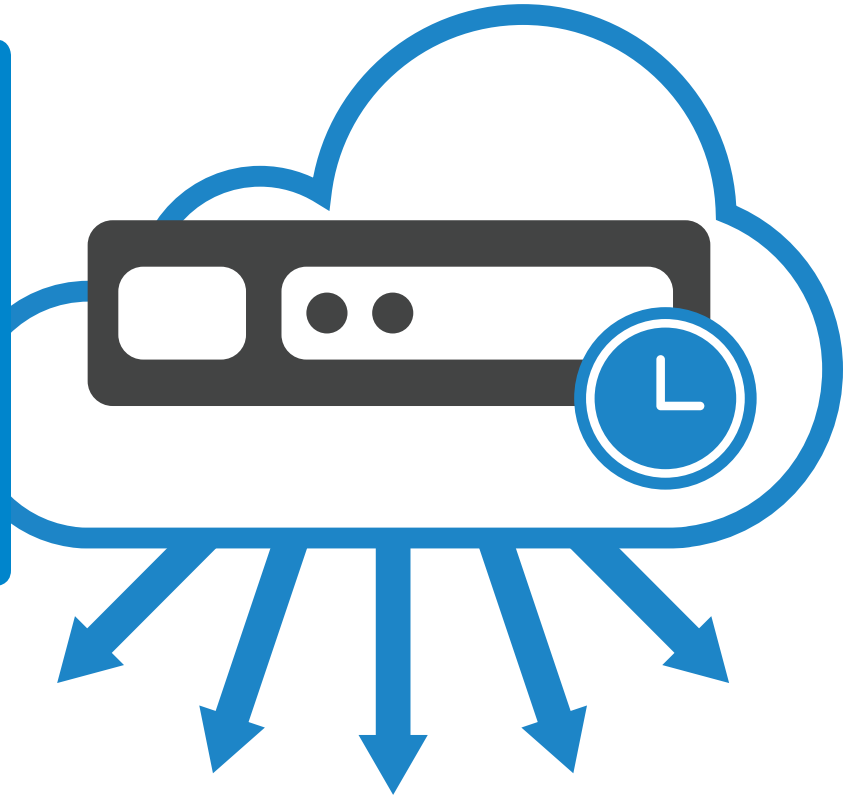


Contraataque n.° 1

Proteja la red cada minuto del día todo el año

Cada hora se desarrollan cientos de nuevas variantes de malware. Por eso, las organizaciones necesitan una protección en tiempo real actualizada al minuto que les blinde ante las últimas amenazas. Un firewall solo es eficaz si se actualiza continuamente, las 24 horas del día, los 7 días de la semana. Además, como el número de variantes y de tipos de malware es tan alto, la memoria disponible de cualquier firewall siempre es inferior a la necesaria. Los firewalls deberían utilizar la cloud para contar con las máximas opciones de visualización del malware y de sus variantes e identificarlas mejor.

Procúrese un firewall que aproveche las potentes capacidades de la cloud para aplicar contramedidas de bloqueo de las últimas amenazas en tiempo real.



Estrategia de ciberataque n.° 2

Infectar las redes con diferentes tipos de malware

Los ciberdelincuentes utilizan diferentes tipos de malware para atacar las redes. Los cinco más comunes son los virus, los gusanos, los troyanos, el spyware y el adware.

Los virus informáticos, en los inicios, se propagaban a través de los disquetes que se compartían. Conforme la tecnología ha evolucionado, los métodos de distribución también se han ido adaptando. En la actualidad, los virus se transmiten a través de los archivos compartidos, de las descargas web y de los archivos adjuntos de los mensajes de correo electrónico.

Los gusanos informáticos existen desde finales de los años ochenta, pero no se extendieron hasta que las infraestructuras de red de las organizaciones se generalizaron. A diferencia de los virus informáticos, los gusanos pueden reptar por las redes sin mediar interacción humana.

Los troyanos se han diseñado específicamente para extraer información confidencial de la red. Muchos tipos de troyanos se hacen con el control del sistema infectado y abren una puerta trasera por la que el atacante accede más tarde. Los troyanos se utilizan a menudo en la creación de redes de robots informáticos.

El spyware no es, en sí, un elemento malicioso, pero puede causar graves trastornos, ya que suele infectar los navegadores web e inutilizarlos casi por completo. Algunas veces, el spyware aparenta ser una aplicación genuina que reporta al usuario ciertas ventajas al poder utilizarla como tal, pero, a su vez, registra secretamente el comportamiento y los patrones de uso.

El adware, por lo general, se utiliza para distribuir anuncios publicitarios que ofrecen alguna clase de beneficio económico al atacante. La víctima infectada por adware, al intentar acceder a Internet, recibe un continuo bombardeo de ventanas emergentes, de barras de herramientas y de otras formas de publicidad.

Los ciberdelincuentes utilizan diferentes tipos de malware para cogerle desprevenido.

Contraataque n.° 2

Asegúrese de proteger la red contra todos los tipos de malware

Todos los firewalls deberían mantener a las organizaciones a salvo de virus, gusanos, troyanos, spyware y adware. Para lograrlo, lo mejor es integrar estas medidas de protección en un enfoque de baja latencia aplicable en un solo paso. Busque características como las siguientes:

- **Protección contra malware basada en red** para impedir que los atacantes descarguen o transmitan el malware a un sistema vulnerable.
- **Actualizaciones continuas y en el momento oportuno** para proteger las redes permanentemente de los millones de nuevas variantes de malware que se crean, en el mismo instante en que se descubren.
- **Servicio de prevención de intrusiones (IPS)** para evitar que los atacantes se aprovechen de las vulnerabilidades de la red.

Asegurarse de que cualquiera que disponga de acceso a su red cuenta con un software de protección antivirus le ofrecerá un nivel adicional de protección contra malware en la red. Si las organizaciones combinan un antivirus de PC de aplicación forzosa con los firewalls de red, podrán bloquear muchas de las herramientas que utilizan los ciberdelincuentes para poner en peligro la red.

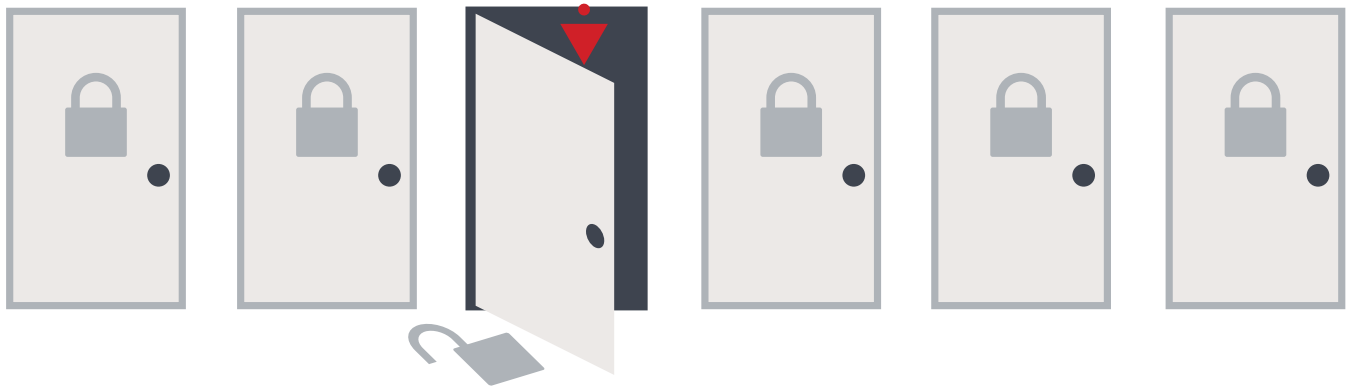
Para anticiparse a las amenazas, opte por implantar varios niveles de protección contra malware.

Estrategia de ciberataque n.° 3

Encontrar y atacar las redes más débiles

Aunque muchos proveedores de firewalls afirman ofrecer una excelente protección antiamenazas, son muy pocos los que han podido demostrar la eficacia de sus soluciones. Las organizaciones que utilizan firewalls de inferior calidad quizá crean que sus redes están protegidas, pero la realidad es que los delincuentes más hábiles pueden burlar el sistema de prevención de intrusiones con complicados algoritmos que eluden la detección y suponen un riesgo para el sistema.

Como algunos firewalls ofrecen protección a costa del rendimiento, las organizaciones que los usan pueden caer en la tentación de desactivarlos o de limitar las medidas de seguridad para conseguir el alto rendimiento de red que se demanda. Esta es una práctica arriesgada y debe evitarse.

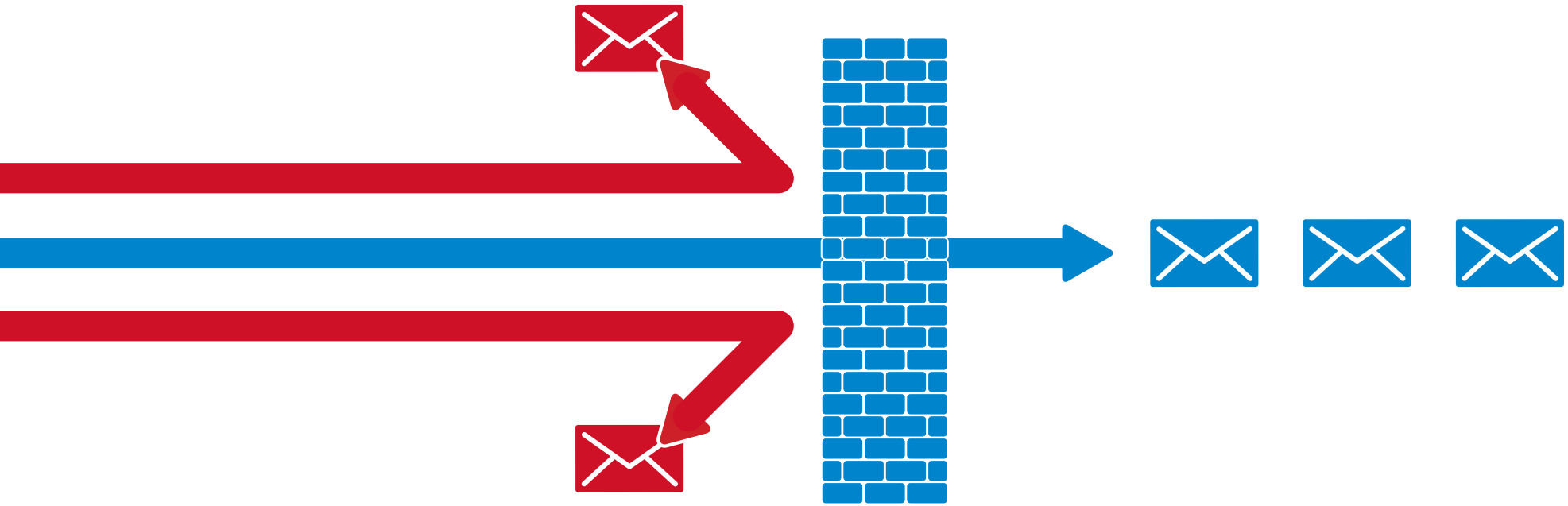


Los ciberdelincuentes escogen a sus víctimas en función de los puntos débiles que descubren en la red.

Contraataque n.° 3

Elija un firewall de alto rendimiento con férrea protección antiamenazas

Busque un firewall con protección contra malware basada en la red probada y certificada por la asociación independiente ICSA Labs. Además, plantéese la elección de un diseño multinúcleo capaz de analizar archivos de cualquier tamaño y tipo para que reaccione sin problemas ante los cambiantes flujos de tráfico. Todos los firewalls necesitan un motor que proteja las redes de los ataques internos y externos sin sacrificar rendimiento.



Estrategia de ciberataque n.° 4

Transformarse con frecuencia y atacar a escala global

Muchos ciberdelincuentes logran sus propósitos porque no cesan de reinventar nuevo malware ni de compartirlo con otros atacantes por todo el mundo. Esto significa que surgen nuevas amenazas cada hora en todos los continentes.

La mayoría de estos ciberdelincuentes utilizan tácticas de ataque relámpago: realizan la incursión, saquean todo lo que pueden y se marchan antes de que nadie pueda dar la voz de alarma. Luego repiten el ataque en otro sitio.

Cada hora surgen nuevas amenazas en todos los continentes.

Contraataque n.° 4

Elija un firewall que le proteja de las amenazas globales

Reaccionar rápidamente a las amenazas es esencial para disfrutar de protección. Si quiere implementar contramedidas en el firewall que le protejan de las amenazas emergentes de la forma más rápida posible, recurra a un proveedor de firewalls con un equipo interno de expertos en métodos para contrarrestar los ataques. Asimismo, ese equipo debe ampliar el alcance de sus actuaciones a partir de una colaboración lo más extensa posible con la comunidad de seguridad.

Ningún appliance de firewall puede bloquear los millones de tipos de malware que existen. Las firmas de amenazas más antiguas y menos usadas pueden eliminarse del firewall local y le dejan expuesto a los ataques. Una solución de amplio espectro puede evitar este problema al utilizar un catálogo de malware completo basado en cloud que amplifica el análisis del firewall local.

Por último, otro síntoma que permite detectar la actividad sospechosa es el tráfico procedente de lugares en los que no opera comercialmente. Mientras que un firewall simple puede identificar y bloquear las amenazas por zona geográfica, un firewall sofisticado incorporará capacidades de filtrado de redes de robots informáticos que consiguen reducir la exposición a las amenazas globales conocidas mediante el bloqueo del tráfico procedente de dominios peligrosos o de las conexiones establecidas en ambas direcciones con una ubicación concreta.

Para bloquear las amenazas globales más recientes, invierta en una solución de seguridad de alcance global.

Conclusión

Los ciberataques aumentan exponencialmente, pero existen defensas eficaces. Cuando se plantee evaluar las diferentes soluciones de contraataque disponibles, si quiere encontrar la idónea para su entorno de red, descargue la documentación técnica "Claves para intensificar la seguridad de la red" e infórmese a fondo.

© 2015 Dell, Inc. Todos los derechos reservados. Este documento contiene información registrada protegida por derechos de autor. No se permite la reproducción total o parcial de este documento, ni su transmisión en cualquier forma o por cualquier medio, sea este electrónico, mecánico, por fotocopia, por grabación u otros métodos, con ningún objetivo, sin el premiso previo y por escrito de Dell, Inc. ("Dell").

Dell, Dell Software, los productos y el logotipo de Dell Software, tal y como se identifican en el presente documento, son marcas registradas de Dell, Inc. en los Estados Unidos o en otros países. El resto de las marcas y las marcas registradas son propiedad de sus respectivos titulares.

La información contenida en este documento se facilita en relación con los productos Dell. Este documento no le otorga ninguna licencia, expresa o implícita, por exclusión ni de ningún otro modo, sobre cualquier derecho de propiedad intelectual o en relación con la venta de productos Dell. A EXCEPCIÓN DE LO PREVISTO EN LAS CONDICIONES DE DELL SEGÚN SE ESPECIFICA EN EL ACUERDO DE LICENCIA DE ESTE PRODUCTO, DELL NO ASUME NINGUNA RESPONSABILIDAD Y NIEGA CUALQUIER GARANTÍA EXPLÍCITA, IMPLÍCITA O RECONOCIDA EXPRESAMENTE POR LA LEY CON RESPECTO A SUS PRODUCTOS, INCLUIDAS, SIN LIMITARSE A ELLAS, LAS GARANTÍAS IMPLÍCITAS DE COMERCIALIZACIÓN, IDONEIDAD PARA UN FIN DETERMINADO Y DE NO INFRACCIÓN. EN NINGÚN CASO DELL SERÁ RESPONSABLE DE LOS DAÑOS DIRECTOS, INDIRECTOS, CONSECUENTES, PUNITIVOS, ESPECIALES O INCIDENTALES (INCLUIDOS, ENTRE OTROS, LOS DAÑOS POR PÉRDIDA DE BENEFICIOS, INTERRUPCIÓN DE LA ACTIVIDAD EMPRESARIAL O PÉRDIDA DE INFORMACIÓN) QUE SE DERIVEN DEL USO O DE LA IMPOSIBILIDAD DE USO DE ESTE DOCUMENTO, AUNQUE SE HAYA ADVERTIDO A DELL DE LA POSIBILIDAD DE DICHOS DAÑOS. Dell no efectúa manifestación ni declaración de garantía alguna en cuanto a la exactitud o la integridad del contenido de este documento y se reserva el derecho de realizar modificaciones de las especificaciones y las descripciones de los productos en cualquier momento sin previo aviso. Dell no se compromete a actualizar la información contenida en este documento.

Acerca de Dell Software

Dell Software ayuda a los clientes a desarrollar un mayor potencial a través del poder de la tecnología. Para ello, ofrece soluciones ampliables, asequibles y fáciles de usar que simplifican la tecnología informática y mitigan los riesgos. El catálogo de Dell Software cubre las necesidades del cliente en cinco áreas clave: administración de centros de datos y gestión de clouds, administración de la información, gestión de trabajadores móviles, seguridad y protección de datos. Este software, combinado con el hardware y los servicios Dell, genera un nivel sin precedentes de eficiencia y productividad para acelerar la obtención de resultados empresariales. www.dellsoftware.com.

Si tiene alguna duda sobre el posible uso que puede hacer de este material, póngase en contacto con nosotros:

Dell Software
5 Polaris Way
Aliso Viejo, CA 92656 (Estados Unidos)
www.Dell.com
Consulte nuestro sitio web para obtener información sobre las oficinas regionales e internacionales.

Ebook-TypesOfCyberAttacks-GM-US-25949