Redes empresariales: Panorama mundial de los desafíos de seguridad de la actualidad

Puntos destacados del 11.º *Informe de seguridad de infraestructura mundial anual (WISR)* de Arbor Networks

Hallazgos clave

34 % Sufrió ataques DDoS, la mitad de los cuales excedió la capacidad de Internet total.

29 % Informó un aumento en la frecuencia de los ataques.

23 % Observó amenazas persistentes avanzadas (APT).

17 % Detectó infiltraciones maliciosas.

53 % Percibió que los firewall o los dispositivos IPS fallaron o contribuyeron a una interrupción durante un ataque.

38 % No cuenta con las herramientas para monitorear los dispositivos BYOD en la red, a pesar de un aumento de más del 100 % en incidentes de seguridad relacionados con BYOD.

57 % Está planificando implementar soluciones para acelerar la respuesta ante incidentes.

43 % Usa sistemas de mitigación de DDoS inteligentes (IDMS).

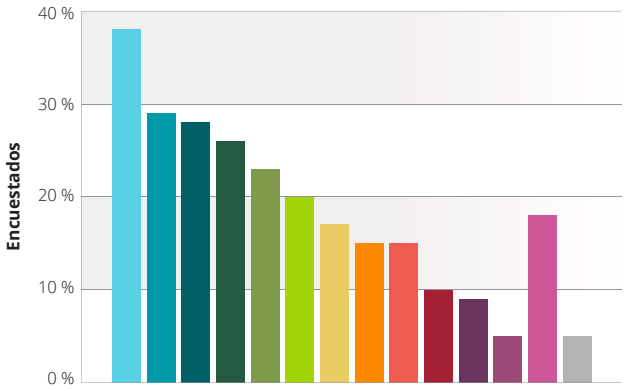
25 % Mitiga ataques DDoS en menos de 15 minutos.

El 11.º *Informe de seguridad de infraestructura mundial anual (WISR)* de Arbor Networks brinda un panorama actual acerca de las amenazas de seguridad en las redes y las técnicas para mitigarlas. El informe se basa en una encuesta realizada a 354 organizaciones que representan operadores de redes de empresas y proveedores de servicios de todo el mundo.
Cubre un período de 12 meses desde noviembre de 2014 hasta octubre de 2015. Este documento resume las respuestas de los operadores de redes de empresas acerca de los principales desafíos de seguridad que tuvieron que enfrentar en 2015 y aquellos que anticipan para el futuro próximo.

Amenazas y preocupaciones en torno a la seguridad

Los ataques DDoS continúan siendo la amenaza más común que enfrentan los encuestados de las empresas (ver Figura 1). La mitad de estos ataques DDoS excedió la capacidad del vínculo de Internet de las redes afectadas. La proporción de encuestados que observó infiltraciones maliciosas y amenazas persistentes avanzadas (APT) creció al 17 % y al 23 % respectivamente. Acerca de las amenazas para el próximo año, los ataques DDoS y las APT continúan siendo la mayor preocupación.

Principales amenazas de seguridad en redes



- **38 %** Congestión en la conectividad a Internet debido a un ataque DDoS
- **29 %** Congestión en la conectividad a Internet debido a un pico/crecimiento de tráfico real
- **28 %** Pérdida de datos accidental
- **26 %** Hosts saturados o comprometidos de otra manera en la red corporativa
- **23 %** Amenaza persistente avanzada (APT) en la red corporativa
- **20 %** Interrupción accidental grave de servicio
- **17 %** Infiltración maliciosa
- **15 %** Exposición a datos confidenciales pero no regulados
- **15 %** Robo
- **10 %** Exposición a datos regulados
- **9 %** Desfiguración de la Web
- **5 %** Exfiltración de datos o espionaje industrial
- **18 %** Ninguno de los anteriores
- **5 %** Otro

Fuente de la Figura 1: Arbor Networks, Inc.

ARBOR NETWORKS
The Security Division of NETSCOUT

Acerca de Arbor Networks

Arbor Networks, la división de ciber-seguridad de NETSCOUT, ayuda a proteger las redes empresariales y de proveedores de servicios más grandes del mundo de los ataques DDoS y de las amenazas avanzadas. Arbor es el proveedor líder a nivel mundial de protección contra DDoS en los segmentos del mercado corporativo, de comunicación y de telefonía móvil, según una investigación de Infonetics.

Nuestras soluciones para amenazas avanzadas brindan visibilidad de red completa a través de una combinación de tecnología de NetFlow y de captura de paquetes, lo que permite la detección y mitigación rápida de malware e infiltraciones maliciosas. También ofrecemos análisis líder en el mercado para lograr respuesta ante incidentes, análisis de históricos, visualización y sistemas forenses dinámicos. Arbor se esmera en ser un "multiplicador de fuerza", al convertir en expertos a los equipos de seguridad y redes. Nuestra meta es brindar un panorama completo de las redes y un mayor contexto sobre seguridad para que los clientes puedan resolver los problemas de manera más rápida y reducir el riesgo para sus negocios.

El *Informe de seguridad de infraestructura mundial anual (WISR)* de Arbor se realiza anualmente y brinda un panorama inusual acerca de la evolución de las amenazas mundiales con base en una serie de encuestas respondidas por operadores de red de todo el mundo. Para obtener más información acerca de los servicios y productos de Arbor, visite nuestro sitio web arbornetworks.com. La investigación, el análisis y el panorama de Arbor, junto con los datos del sistema de inteligencia de amenazas mundial ATLAS® se pueden encontrar en el ATLAS Threat Portal.

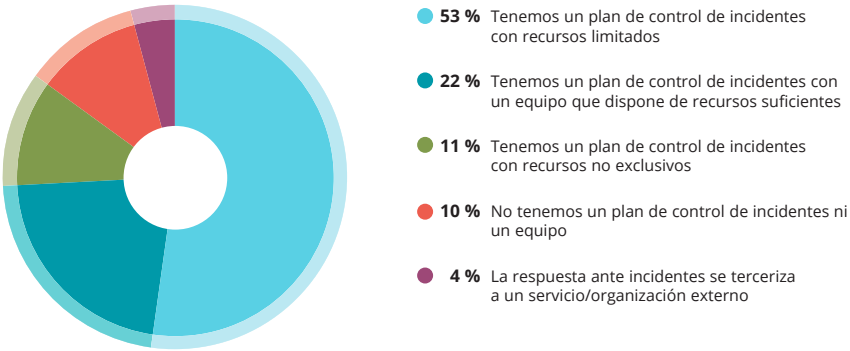
Detección, informe y corrección de amenazas

Menos del cinco por ciento de los encuestados dijo que resolver los incidentes llevó más de tres meses. Casi 85 por ciento cuenta con procesos de notificación internos o externos formales ante casos de infiltraciones. Los mecanismos más utilizados para acelerar la detección y la contención de amenazas son nuevas herramientas forenses, procesos de evaluación (triage) mejorados y la integración de inteligencia de amenazas en la función de respuesta ante incidentes.

Preparación para la respuesta ante incidentes

Tres cuartos de los encuestados tiene un plan de respuesta ante incidentes y al menos algunos recursos preparados, durante más de dos tercios del año pasado (ver Figura 2). Sin embargo, el 38 por ciento no planifica aumentar sus recursos internos para estar mejor preparado. Casi el 50 % contrató organizaciones externas para que los ayudaran con la respuesta ante incidentes, especialmente en el área de sistemas forenses de TI. Solo el seis por ciento no se preparó de ninguna manera para controlar un incidente, un porcentaje menor al diez por ciento observado el año pasado. El 57 % está considerando implementar soluciones que aceleren el proceso de respuesta ante incidentes, lo que la convierte en la estrategia más elegida para mejorar la preparación ante amenazas.

Postura con relación a la respuesta ante incidentes



Fuente de la Figura 2: Arbor Networks, Inc.

Detección de amenazas

Las herramientas más utilizadas para detectar amenazas son los firewalls, la gestión de eventos e información de seguridad (SIEM) y los analizadores de NetFlow. Sin embargo, el uso de herramientas forenses de análisis de paquetes y tecnologías sandbox ha aumentado de manera significativa, lo que indica una inversión constante en soluciones de distinta índole para la detección de amenazas. La detección automatizada continúa siendo el método más común para la detección de incidentes.

Capacitación en seguridad para los usuarios finales

El 70 % de los encuestados cree que su comunidad de usuarios está educada correctamente sobre temas básicos de seguridad. Es más, el 62 % actualiza las capacitaciones sobre seguridad de sus empleados y exige recertificaciones periódicas.

Monitoreo de los dispositivos BYOD

El 13 % de los encuestados observó incidentes de seguridad relacionados con los dispositivos personales de los empleados (BYOD), más del doble del año pasado. Aún así, cerca del 40 % aún no ha implementado herramientas para monitorear los dispositivos BYOD en su red. Si bien ha aumentado la implementación de límites de acceso para los dispositivos personales de los empleados en las empresas, el uso de administración de dispositivos móviles (MDM) disminuyó un diez por ciento. Podría deberse a un problema de costos, pero necesita resolverse ya que la política de BYOD se continuará implementando.

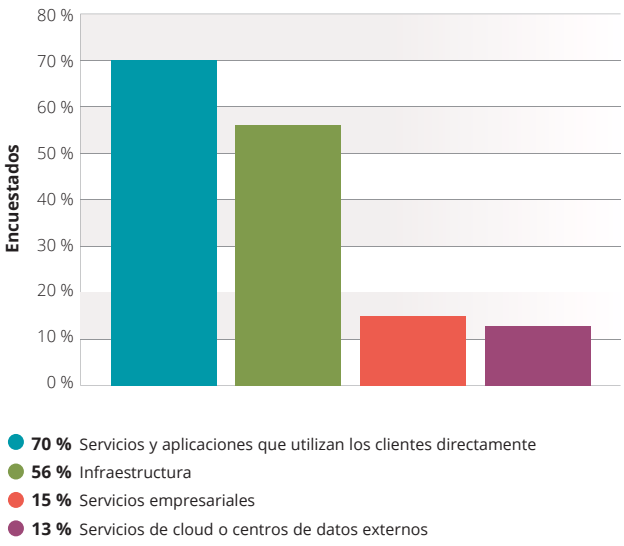
Frecuencia de ataques DDoS

El 34 % de los encuestados sufrió ataques DDoS el año pasado. Sin embargo, este porcentaje varía por área. Para los bancos y los gobiernos, los porcentajes son mayores, 45 % y 43 % respectivamente. Más de un cuarto de los encuestados observó un aumento en la frecuencia de los incidentes. De todos los encuestados empresariales que sufrieron ataques, más de un cuarto tuvo más de 10 ataques por mes.

Duración y objetivos de los ataques DDoS

El 70 % de los encuestados sufrió ataques que afectaron servicios y aplicaciones que utilizan sus clientes (ver Figura 3). Más de la mitad observó ataques que afectaron la infraestructura, como routers, balanceadores de carga, firewalls y el ancho de banda. Más de la mitad también percibió que los firewall o los dispositivos IPS fallaron o contribuyeron a una interrupción durante un ataque, más del 35 % observado el año pasado. La mayoría de los encuestados (88 %) informó la ocurrencia de ataques que duraban menos de un día. Cerca del 60 % indicó que el ataque más prolongado finalizó en siete horas o menos.

Objetivos de los ataques DDoS



Fuente de la Figura 3: Arbor Networks, Inc.

Tipos de ataques DDoS

El 58 % de los ataques DDoS informados fueron volumétricos, mientras que el 24 % afectó la capa de aplicaciones. Esto refuerza la necesidad de una defensa por capas. El principal objetivo de los ataques a nivel de aplicaciones fueron los servicios web. Más del 80 % observó ataques a HTTP, y más de la mitad contra HTTPS y DNS. Cerca de la mitad observó ataques volumétricos que afectaron servicios web cifrados (UDP/TCP puerto 443). Además, el 37 % sufrió ataques que afectaron el servicio cifrado en la capa de aplicaciones y el 42 % observó ataques que afectaron el protocolo SSL/TLS.

Ataques multivectoriales

Los ataques DDoS multivectoriales combinan varias técnicas de ataque al mismo tiempo, que tienen el mismo objetivo: aumentar tanto las posibilidades de éxito del ataque como la complejidad para mitigarlo. Este año, el 43 % de los encuestados padecieron ataques DDoS multivectoriales en las redes empresariales.

Descargar el *Informe de seguridad de infraestructura mundial anual (WISR)* 2015 completo

Desde su creación hace 11 años, el *Informe de seguridad de infraestructura mundial anual (WISR)* de Arbor se ha basado en datos de encuestas obtenidos de aquellas personas involucradas directamente con la seguridad operativa diaria. Los más de 350 operadores de red que participaron en el informe de este año representan un amplio espectro de ubicaciones geográficas y enfoques de negocio, lo que brinda un panorama mundial real de la seguridad de infraestructura desde una perspectiva operativa. Nuestro informe 2015 muestra las tendencias clave con relación a las amenazas de seguridad que enfrentan cuatro sectores principales: proveedores de servicios, empresas, centros de datos y operadores de redes móviles. También presenta las tecnologías que utiliza cada uno de estos sectores para identificar y mitigar las amenazas de seguridad.

Para descargar una copia gratuita de este informe, arbornetworks.com/report

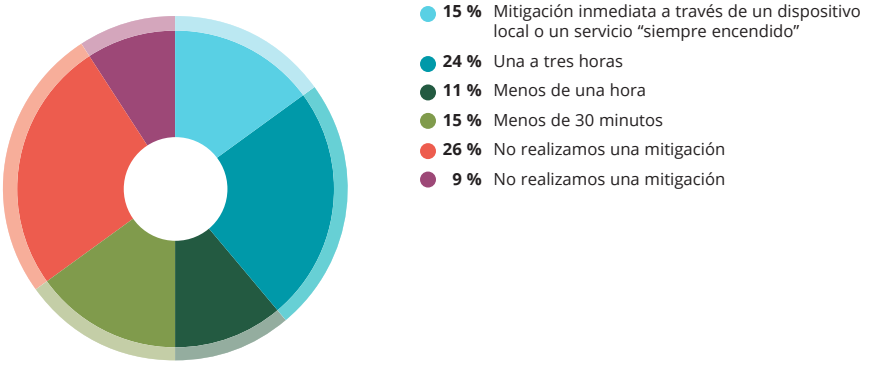
Técnicas de mitigación de ataques DDoS

Entre los encuestados de este año, los firewalls continúan siendo la técnica de mitigación de DDoS más común. Pero su uso ha disminuido notablemente del 72 % del año pasado al 53 % de este año. Es una señal positiva, ya que los firewalls son susceptibles a los ataques DDoS por saturación de estado, como lo prueba el 53 % de los encuestados empresariales que observó fallas de sus firewalls debido a ataques DDoS durante el período cubierto por la encuesta. Una observación alentadora es que el 43 % ahora usa sistemas de mitigación de DDoS inteligentes (IDMS), comparado al tercio del año pasado. Sin embargo, solo el 23 % cuenta con una estrategia de mitigación de DDoS por capas, que es la mejor práctica en la actualidad.

Tiempo de mitigación de un ataque DDoS

Con una mejora significativa con relación al año pasado, casi el doble del porcentaje de los encuestados puede mitigar inmediatamente un ataque a través del servicio o dispositivo "siempre encendido" (ver Figura 4). Además, un poco más de un cuarto puede mitigar el ataque en menos de 15 minutos. Sin embargo, casi el mismo porcentaje de encuestados mide su tiempo de respuesta en horas, no minutos. A medida que las empresas se vuelven más dependientes de Internet y los períodos de inactividad se tornan más costosos, es cada vez más importante reducir el tiempo de mitigación de los ataques.

Tiempo de mitigación de un ataque DDoS



Fuente de la Figura 4: Arbor Networks, Inc.

Costo e impacto en los negocios de los ataques DDoS

Cuando se les pide a los encuestados que identifiquen los impactos en los negocios que resultan de los ataques DDoS, estos mencionan gastos operativos (64 %), daño a la marca/reputación (36 %), pérdida de ingresos (30 %) y pérdida de clientes (17 %). Cerca de dos tercios de los encuestados estima que el impacto asociado con la pérdida de conectividad a Internet es de más de USD 500/minuto, y algunos indican un gasto mucho mayor.

ARBOR NETWORKS
The Security Division of NETSCOUT

Sede Corporativa
76 Blanchard Road
Burlington, MA 01803 EE. UU.
Llamada gratuita en
EE. UU.: +1 866 212 7267
Tel.: +1 781 362 4300

Ventas en Norteamérica
Llamada gratuita: +1 855 773 9200

Europa
Tel.: +44 207 127 8147

Asia Pacífico
Tel.: +65 68096226

www.arbornetworks.com

SR/WISR/ENTEPRISE/EN/0216-LETTER