

➔ RESUMEN EJECUTIVO

A lo largo de 2017, los titulares de los grandes medios de comunicación anunciaron ciberataques y amenazas de seguridad que incluyeron la posible interferencia en las elecciones presidenciales de los Estados Unidos, brotes de malware a nivel mundial y la filtración de datos de Equifax. Estos eventos de alto perfil y muchos otros instaron a todo tipo de partes, desde gobiernos nacionales y empresas internacionales hasta individuos que compran soluciones antimalware para dispositivos personales, a aumentar su inversión en ciberdefensa. Sin embargo, el aumento de la inversión viene de la mano de un aumento en las amenazas, las intrusiones y las vulnerabilidades.

Entender esta dinámica compleja y desafiante es precisamente el objetivo detrás del *Informe global de seguridad de las aplicaciones y seguridad de red* de Radware. Este informe reúne hallazgos de una encuesta global de la industria, la investigación orgánica de Radware, datos de ataques reales e historias de clientes para dar un panorama de la situación actual y qué pueden hacer los profesionales de seguridad al respecto.

Toda la comunidad de la seguridad informática puede sacar provecho de este informe, que resalta la investigación y el conocimiento de Radware sobre:

- ▶ el panorama de amenazas: el quién, el qué y el porqué de los atacantes;
- ▶ el impacto potencial sobre su empresa, incluidos los costos asociados con los diferentes ciberataques;
- ▶ cuán preparada está cada industria;
- ▶ las experiencias de las organizaciones de su industria;
- ▶ las nuevas amenazas y cómo protegerse contra ellas;
- ▶ predicciones para el 2018.

➔ AL LÍMITE

Actualmente, la principal motivación detrás de los ciberataques es el cibercrimen. Los atacantes buscan un rédito económico y se sienten alentados por la prosperidad de las criptodivisas. Al mismo tiempo, los ataques se tornan más dirigidos. Un enemigo decidido invierte en reconocimiento, ingeniería social y herramientas específicas para conocer mejor su objetivo.



El malware, los bots y las amenazas basadas en ingeniería social resultaron los vectores de ataque más comunes. Sin embargo, las organizaciones no deben temer únicamente a lo que está frente a ellas, sino también a lo que se esconde detrás de la esquina, como las botnets de IoT, los ataques de denegación permanente de servicios (DDoS), los ataques basados en SSL y las inyecciones sofisticadas de malware. Para prepararse, las organizaciones pueden interiorizarse de nuevas tecnologías tales como la IoT, las cadenas de bloques (*blockchain*) y la computación sin servidores o de “función como servicio” (FaaS).

Los reglamentos todavía juegan un papel importante a la hora de elevar los estándares de seguridad, gracias a que proporcionan lineamientos y normas para cada industria o región. Aunque muchas organizaciones se esfuerzan por cumplir con las normas de seguridad y privacidad, no parecen dar igual importancia al cumplimiento y las certificaciones a la hora de evaluar soluciones de seguridad. Resulta que ciertas organizaciones no conocen bien las certificaciones existentes y casi un tercio nunca pregunta a los proveedores sobre ellas.

Los ciberataques masivos de 2017 tuvieron éxito simplemente debido a vulnerabilidades no atendidas. Ese es un error humano pequeño y común que puede tener consecuencias devastadoras. El aprendizaje automático y la inteligencia artificial (IA) pueden parecer la solución lógica. Veinte por ciento de las organizaciones ya confían en dichas soluciones y otro 28% piensa implementarlas en 2018. Sin embargo, estas soluciones no son infalibles. Solo piense en los riesgos del envenenamiento de la IA, en cómo los sistemas automáticos se pueden frustrar y en cómo estos sistemas pueden fallar (p. ej., Microsoft Tay y los *chatbots* de Facebook).

Si combinamos todo, está claro que nos enfrentamos a una falencia importante. Los seres humanos estamos al límite de nuestra capacidad colectiva de mantener el control. Sin embargo, la IA y el aprendizaje automático todavía no han alcanzado un nivel de madurez suficiente y es fácil engañarlos.

➔ OTROS HALLAZGOS Y ASPECTOS DESTACADOS



La extorsión motivó la mitad de los ataques

Al dispararse el valor del Bitcoin, también se dispararon los ataques de extorsión. Las organizaciones indicaron el cobro de un rescate como la motivación detrás de la mitad de todos los ataques. Esto la convierte en la principal motivación, por encima de las amenazas internas, el hacktivismo y la competencia, entre otras. A nivel internacional, 42% de las empresas fueron víctimas de ataques extorsivos, lo cual representa un aumento de 40% respecto de 2016.



Principal inquietud: filtración de datos

La filtración de datos y la pérdida de información resultaron la principal inquietud relacionada con la seguridad, siendo identificada por 28% de las organizaciones a nivel mundial. Otra inquietud importante fue la degradación o interrupción en el servicio, identificada por 23% de las organizaciones.



Los ataques DDoS ganan popularidad y se enfocan en la capa de aplicación

La prevalencia de los ataques DDoS aumentó 10% y afectó a casi dos de cada cinco empresas. Una de cada seis sufrió un ataque de una botnet de IoT y 68% de los ataques provocaron una degradación o interrupción completa del servicio. Ambas situaciones tienen costos asociados. En 2017, también se observó un aumento de la cantidad de ataques de capa de aplicación frente a la cantidad de ataques de capa de red.



El 80% no rastrea los costos

Ochenta por ciento de las organizaciones no calculan el costo de los ciberataques. Uno de cada tres no cuenta con un plan de respuesta a emergencias a pesar de que los ciberataques se han convertido en algo casi cotidiano. Otro dato alarmante es que, en uno de cada cuatro ataques, un cliente abandona la organización atacada o la demanda.



La seguridad todavía está “nublada”

Las organizaciones identificaron los errores en la configuración de seguridad (26%) y las vulnerabilidades en las aplicaciones (23%) como los principales riesgos en los entornos en la nube. También informaron que 51% de las aplicaciones en la nube sufren cambios semanalmente (un aumento de 16% en comparación con 2016). Los cambios frecuentes presentan un desafío de visibilidad y control para los profesionales de la seguridad, particularmente cuando un cuarto de las aplicaciones son críticas para las operaciones.

El desafío de seguridad más frecuente al migrar aplicaciones a la nube es el control, la gerencia y la falta de visibilidad, identificados por el 46% de las organizaciones. Les siguen la falta de experiencia y conocimientos prácticos, y la complejidad en el manejo de las políticas de seguridad. Un dato interesante es que el 51% de los usuarios de nubes públicas confían en los servicios de seguridad de los proveedores de servicios en la nube y los incorporan a los paquetes que contratan, incluso si los proveedores no son empresas enfocadas en la seguridad.



¿Un potencial bloqueado?

Las cadenas de bloques (*blockchain*) son un tema tecnológico en auge. Sin embargo, 36% de los encuestados admiten que no entienden los mecanismos detrás de esta tecnología, y solo 10% creen que las cadenas de bloques mejorarán la seguridad informática.



El sector de Educación no tiene buenas calificaciones

El sector de Educación es el menos preparado para enfrentarse a diferentes tipos de ciberataques. Este es el segundo año consecutivo en el que el sector se ubica en el último puesto en esta categoría.



El 72% no están preparados para el RGPD

Casi tres cuartos de las organizaciones (72%) dicen no estar bien preparadas para el Reglamento General de Protección de Datos (RGPD) de la UE. Dieciséis por ciento de los encuestados ni siquiera sabe qué es el RGPD.

Los equipos de seguridad pueden usar los hallazgos y datos del *Informe global de seguridad de las aplicaciones y seguridad de red* que Radware publica cada año para analizar el panorama de amenazas y diseñar estrategias de seguridad para proteger a sus empresas. Dado que los ciberatacantes cambian constantemente de blanco, Radware también alienta a las organizaciones a mantenerse un paso delante con la ayuda de su centro de recursos de seguridad, [DDoSWarriors.com](https://www.radware.com).