EL FACTOR CONFIANZA

El rol de la ciberseguridad a la hora de mantener el impulso de una empresa

Resumen ejecutivo

En 2018, se redoblaron las apuestas de los ciberataques. Los titulares de las noticias siguieron mostrando incidentes de alto perfil relacionados con la seguridad de los datos, incluido el mayor ataque de denegación de servicio jamás registrado, con un volumen de 1,7 Tbps.1 En la Unión Europea, el Reglamento General de Protección de Datos (RGPD), que entró en vigencia el 25 de mayo de 2018, impone reglas estrictas en relación con la forma de recopilar, procesar y controlar la información de identificación personal (IIP). Además, criptomineros se infiltraron en diversas redes en busca de dinero fácil.

Entramos en una era de la "posconfianza" en la que las organizaciones y los individuos desconfían cada vez más de las promesas de seguridad. Cada vez que los consumidores interactúan con una marca, juzgan si confían lo suficiente en una empresa como para compartir su IIP con ella. Los ciberataques exitosos menoscaban la confianza que las empresas lucharon por establecer entre sus marcas y los clientes. Las ramificaciones ya no son responsabilidad exclusiva de los profesionales de la seguridad, sino que alcanzan incluso a los gerentes de primera línea.

Para ayudar a las organizaciones a entender mejor los complejos desafíos a los que se enfrentan en la lucha por proteger sus marcas, Radware publica anualmente un Informe Global de Seguridad de Aplicaciones y Seguridad de la Red. La octava edición del informe combina la investigación orgánica de Radware, datos de ataques reales y análisis de nuevas tendencias y tecnologías con los hallazgos de una encuesta global de la industria.

El informe destaca el impacto comercial y tecnológico de la ciberseguridad, incluidos los siguientes aspectos:

- Las lecciones aprendidas de los ataques recientes
- El verdadero costo cuantitativo y cualitativo de los ciberataques
- Un panorama general de las amenazas de red y de aplicaciones
- Información sobre las vulnerabilidades de las nuevas tecnologías
- Predicciones para 2019

PRINCIPALES HALLAZGOS

Equilibrar el cálculo de la relación costo-riesgo

Protegerse contra los ciberataques requiere una inversión considerable que se computa como un gasto operativo en el balance. Por naturaleza, las organizaciones buscan constantemente formas de conservar fondos. Sin embargo, la decisión de cuánto invertir en seguridad si se tiene en cuenta el riesgo de que los ciberataques penetren las defensas y afecten los negocios no es nada fácil.

Consideremos los siguientes datos esclarecedores revelados por la encuesta global de la industria 2018-2019 de Radware:

- En apenas un año, los costos iniciales atribuibles a los ciberataques aumentaron 52% hasta alcanzar 1,1 millones de dólares.
- Las organizaciones que consideraron el costo total de los ciberataques estimaron el monto en casi el doble que las empresas que no consideraron los costos.
- Dos de cada cinco empresas informaron experiencias negativas para los consumidores y pérdida de reputación luego de un ataque exitoso.
- 93% de los encuestados sufrieron un ciberataque durante los últimos 12 meses. Apenas 7% dijo no haber sufrido ningún ataque.
- Un tercio de las organizaciones sufrieron ciberataques semanalmente.
- El principal impacto de los ciberataques fue una perturbación del servicio, sufrida por casi la mitad de los encuestados. Los ataques que provocaron una interrupción total o parcial del servicio aumentaron 15% y afectaron la productividad.
- La ciberextorsión se mantuvo en primer lugar entre las motivaciones de los hackers y explicó el 51% de los ataques.

[1]https://security.radware.com/ddos-threats-attacks/threat-advisories-attack-reports/memcache-ddos-as-a-service/

Nuevos vectores de ataque

Para causar una denegación de servicio, los atacantes emplean técnicas eficientes como ráfagas, amplificación, cifrado o ***botnets*** de Internet de las Cosas (IoT). Además, dirigen sus ataques a la capa de aplicación para maximizar el daño.

- Los ataques de capa de aplicación fueron los que más daño causaron. Dos tercios de los encuestados sufrieron ataques de capa de aplicación. Un tercio de los encuestados prevén que las vulnerabilidades de las aplicaciones serán un gran problema en 2019, particularmente en los entornos en la nube. Más de la mitad de los encuestados modificaron y actualizaron sus aplicaciones mensualmente, mientras que el resto hizo actualizaciones con mayor frecuencia. Estas actualizaciones constantes justifican la automatización de la seguridad.
- La cantidad de ataques que causaron una interrupción total del servicio aumentaron 15% y una de cada seis organizaciones informó haber sufrido un ataque de 1 Tbps.
- Los hackers encontraron nuevas tácticas para derribar redes y centros de datos: Los ataques de desbordamiento HTTPS aumentaron 20%; los ataques DNS y los ataques de ráfaga aumentaron 15%; y los ataques con ***bots*** aumentaron 10%.
- Un tercio de las empresas informaron sufrir ataques cuyos motivos no pudieron identificar.

Prepararse para lo que viene

Las empresas indican que entienden la seriedad de los cambios en el panorama de amenazas y toman pasos para proteger sus activos digitales, pero la gravedad de las amenazas de seguridad tiene un peso importante.

- Casi la mitad de los encuestados no se sentían debidamente preparados para defenderse contra todo tipo de ataques a pesar de tener soluciones de seguridad implementadas.
- 86% de las empresas exploraron soluciones de aprendizaje automático e inteligencia artificial (IA) durante los últimos 12 meses. Casi la mitad dijeron que la motivación para explorar estas soluciones era disminuir el tiempo de respuesta a los ataques. Radware observó un aumento de 44% en quienes utilizan ***blockchain*** para sus actividades.
- Las empresas siguieron diversificando las operaciones de red entre múltiples proveedores de servicios en la nube. Dos de cada cinco organizaciones utilizan soluciones híbridas de ciberseguridad que combinan protección local con protección en la nube.
- 45% de las organizaciones de EMEA dijeron no estar bien preparadas para cumplir con el RGPD.

El éxito es la única opción

El costo de los ciberataques es demasiado alto como para permitirse errores en la mitigación de ataques. La confianza del consumidor se destruye en instantes y hay un costo considerable para la reputación de la marca, así como costos asociados con la recuperación de clientes. El RGPD y otras normativas gubernamentales pueden llevar a la bancarrota a las empresas que no cumplen con sus exigencias.

Es esencial que las organizaciones incorporen la ciberseguridad a sus planes de crecimiento a largo plazo. La protección de los activos digitales ya no se puede delegar exclusivamente al Departamento de Informática. En cambio, la planificación de seguridad se debe incorporar directamente a las nuevas ofertas de productos y servicios, la seguridad, los planes de desarrollo y las nuevas iniciativas empresariales. El director ejecutivo y los demás ejecutivos deben ponerse al frente a la hora de invertir para resguardar la experiencia de los clientes.

La perspectiva gerencial

Los directores ejecutivos son los nuevos "directores de confianza"

La ciberseguridad se torna un tema muy personal para los ejecutivos en quienes recae el liderazgo de los niveles más altos de una empresa. Para construir y mantener una relación sólida con los clientes, los directores ejecutivos deben convertirse también en "directores de confianza". Dado que un único ciberataque puede aniquilar años de trabajo en la creación de una estrategia de marca, ya no basta con asignar la estrategia de seguridad al director de Seguridad Informática. Hay demasiado en juego.

Por ejemplo, consideremos el destino de los directores ejecutivos de empresas que sufrieron violaciones de alto perfil de la seguridad de los datos, como Equifax, Yahoo, Moller-Maersk y Anthem Healthcare. Todo el trabajo que las organizaciones dedicaron a fortalecer el valor de sus marcas se evaporó en cuanto los clientes perdieron confianza en ellas a causa de los ataques. En poco tiempo, los directores ejecutivos de estas empresas tuvieron que retirarse "por cuestiones personales".

Garantizar la ciberseguridad es una parte integral de los modelos de negocios de las empresas y los directores ejecutivos deben verificar los esfuerzos y financiar medidas de protección. Los directores ejecutivos que delegan la estrategia de seguridad sin supervisión lo hacen a su propio riesgo.