La seguridad empieza en el borde de Internet:

Guía de seguridad para compradores de 2019

La seguridad es la base de la innovación empresarial digital.

Tal vez esta sea una afirmación atrevida, que no siempre ha sido aceptada como verdad. En un pasado no tan lejano, la seguridad digital se consideraba un centro de costes. Eso ha cambiado.

La seguridad es esencial para el éxito de cualquier empresa digital. Sin embargo, si hay una cosa con la que siempre puede contar es con que los ataques para vulnerar la seguridad son inevitables. Y no debe asombrar a nadie afirmar que estos ataques pueden tener consecuencias funestas que van más allá del tiempo de inactividad. Las filtraciones de seguridad merman la confianza y dañan la reputación.

En pocas palabras, no hay otra opción. Como director de Tecnologías de la Información, director de Seguridad o algún otro tipo de responsable de TI, tiene claro que su trabajo consiste en ser el agente central que pone de relieve las relaciones entre los riesgos empresariales y los digitales. Su responsabilidad es encontrar el talento y la tecnología necesarios para garantizar la protección de sus activos digitales.

Según Gartner, en 2020, el 100 % de las grandes empresas deberá informar a sus juntas directivas, al menos una vez al año, sobre los riesgos de ciberseguridad y tecnológicos a los que se enfrentan. Esto supera el 40 % detectado en 2018. Tanto si está al cargo de una empresa grande como de una pequeña, parte de su estrategia de seguridad, gestión de riesgos y cumplimiento de normativas continua será la de contar con la solución de seguridad más eficaz para su empresa.

Nos consta que esto es más fácil en la teoría que en la práctica. Para ayudarle, hemos elaborado esta guía con el objeto de que encuentre la solución adecuada para su empresa, de manera que pueda hacerla más resiliente y aumentar la confianza y los ingresos.

Como responsable de seguridad debe conocerse bien.

La pregunta definitiva: ¿cuál es la mejor solución para mitigar riesgos? Para responder a esta pregunta, primero debe responder a algunas otras: ¿Quiénes somos como empresa? ¿Cuáles son nuestros requisitos? ¿Cuáles son los resultados que esperamos conseguir como consecuencia de esta compra? Empiece por lo siguiente:

Evalúe sus riesgos.

Una evaluación rigurosa de los riesgos permite analizar con criterio la estrategia de seguridad actual de una organización. Para empezar, debe identificar las posibles amenazas a las que se enfrenta la organización, además de valorar cada una de ellas en función de la probabilidad de que se produzca, así como del posible impacto si lo hace.

Después de identificar las posibles amenazas, el siguiente paso consiste en identificar sus vulnerabilidades, como un servidor web que ejecute un sistema operativo no actualizado y con fallos de seguridad conocidos, o bien un ancho de banda de red insuficiente para absorber un ataque DDoS. Además, a medida que las empresas migran las aplicaciones a la nube, la forma en que los empleados acceden a ellas va cambiando. Ya no es viable proporcionar un acceso ilimitado según un modelo de seguridad anticuado, que se diseñó teniendo en mente la idea falsa de que el perímetro era impenetrable.

Es ahora cuando está empezando a centrar sus esfuerzos en áreas donde se solapan las amenazas y las vulnerabilidades. El siguiente paso es realizar un análisis de brechas. ¿Qué controles necesitamos, de los que aún no disponemos, para mitigar estas amenazas?

La seguridad no debe suponer un obstáculo para las operaciones empresariales, sino que debería facilitarlas.

Recordatorio: la experiencia del usuario y la seguridad no deben entrar en conflicto.

La seguridad no debe suponer un obstáculo para las operaciones empresariales, sino que debería facilitarlas. En la actualidad, existe tolerancia cero por parte de los usuarios ante una experiencia negativa. Tanto si su trabajo consiste en proteger a un retailer online como la distribución OTT en una organización, los usuarios finales esperan la perfección, sin tiempo de inactividad ni retrasos.

Sin embargo, a menudo, al proteger la red, las experiencias de los usuarios se ven afectadas de forma negativa. Existe la vieja creencia de que, en un nivel básico, la experiencia del usuario y la seguridad entran en conflicto. Pero esto no tiene por qué ser así.

Es cierto que algunas soluciones de seguridad perturban la experiencia del usuario. Otras posibles trabas incluyen procesos de seguridad que interrumpen innecesariamente las aplicaciones o que dificultan la labor de los desarrolladores. Algunos proveedores de seguridad incluso impiden a los equipos internos elegir un proveedor de servicios en la nube en el que implementar sus aplicaciones. Pero, de nuevo, esto no tiene por qué ser así.

Su próximo proveedor de seguridad debe cumplir estos cuatro requisitos fundamentales.

Después de responder a las anteriores preguntas y tener claros cuáles son sus objetivos, es el momento de centrar su atención en los posibles proveedores. Para ello, céntrese primero en los siguientes elementos fundamentales que debe ofrecer cualquier plataforma de seguridad de calidad:

Plataforma: el valor de una plataforma de seguridad depende de usted y de las necesidades de su empresa. Hágase estas preguntas al determinar los elementos fundamentales que una plataforma debe proporcionarle: ¿Qué significa la plataforma de seguridad para usted como responsable de seguridad? ¿Qué funciones le ofrece? ¿Le permite avanzar más rápido? ¿Cómo garantiza la seguridad de sus activos? ¿Es fácil (o difícil) de gestionar?

Servicio y asistencia: su próximo proveedor debe contar con expertos en seguridad altamente cualificados que proporcionen análisis de amenazas y una estrategia personalizada. Para muchas organizaciones, la protección contra las amenazas de seguridad diversas y en constante evolución exige algo más que simple tecnología. Teniendo en cuenta que se enfrenta a objetivos empresariales contrapuestos y a un presupuesto de TI limitado, puede que no disponga del tiempo, los recursos o el personal experto necesarios para proporcionar la mejor seguridad posible para sus sitios, aplicaciones y API. Los servicios de seguridad gestionados pueden ayudar a reducir el tiempo de respuesta y, al mismo tiempo, aumentar la calidad de la mitigación gracias al uso de una estrategia conjunta entre usted y el proveedor.

Cumplimiento de normativas: asegúrese de que cualquier proveedor en el que esté pensando cumpla todas las normativas correspondientes para su sector, incluido el Reglamento General de Protección de Datos (RGPD) de la Unión Europea, las Normas de seguridad de datos del sector de las tarjetas de pago (PCI DSS), la Ley de Transferencia y Responsabilidad de Seguros Médicos de 1996 (HIPAA), el Programa Federal de Gestión de Autorizaciones y Riesgo (FedRAMP), la norma ISO 27002 y los Controles de Organizaciones de Servicio (SOC) 2, entre otros.

Por último, ¿su solución le permite marcar todas las casillas en la lista?: hay ciertas funciones que cualquier proveedor de seguridad debe dominar y abordar para cumplir con sus exigencias. A continuación, se muestran los elementos básicos que debe tener en cuenta a la hora de enfrentarse al proceso de selección de proveedores.

- ❑ Mitigación de DDoS
- ❑ Seguridad de aplicaciones
- ❑ Seguridad de API
- ❑ Prevención de phishing
- ❑ Protección ante Credential Stuffing
- ❑ Detección de bots
- ❑ Acceso seguro a las aplicaciones
- ❑ Protección contra malware

Una solución de seguridad debe proteger a sus empleados y aplicaciones, además de ofrecer protección contra bots y el fraude.

¿Cuáles son las ventajas generales que debe ofrecer cualquier solución?

Una solución de seguridad debe proporcionar a su organización tres ventajas generales: **escalabilidad, visibilidad e inteligencia**, todo ello a la vez que protege a sus empleados y aplicaciones, y ofrece protección contra los bots y el fraude. Una solución nueva debería facilitarle la adopción de un modelo Zero Trust para proteger a sus empleados, garantizar los ingresos y las experiencias de los clientes frente a los bots y el fraude y, tal vez lo que es más importante, proteger las aplicaciones y las API, que son las piedras angulares de la experiencia digital moderna.

Escalabilidad: a medida que los ataques aumentan tanto en tamaño como en velocidad, es fundamental que cualquier solución en la que esté pensando pueda adaptarse al ritmo de las amenazas en constante evolución. En 2018, un ataque DDoS de 1,3 Tbps, basado en la reflexión de Memcached, amenazó con desencadenar el caos. Este ataque sin precedentes tuvo un tamaño superior al doble del importante ataque de la botnet Mirai de 2017.

Vivimos en un mundo en el que el tráfico malicioso de bots seguirá alcanzando niveles sin precedentes. Los hackers actuales utilizan bots para iniciar análisis previos al ataque, aprovechar cualquier vulnerabilidad y ejecutar diversos ataques, como inyección de código, DDoS y ataques para adivinar las contraseñas, contra propiedades web. Estos bots también cometen fraudes mediante Credential Stuffing, realizando y cancelando de forma reiterada compras, reteniendo o usando inventario, realizando scraping de sitios, robando información y alojando muchas otras actividades no deseadas. En el peor de los casos, un bot malintencionado puede provocar interrupciones en la aplicación y la API, lo que puede ocasionar pérdidas de ingresos.

El mejor método para acabar con las enormes cantidades de tráfico no deseado consiste en eliminar el tráfico en el *borde de Internet*, antes de que llegue a los sitios web. Sin embargo, el hecho de que el tráfico legítimo de bots sea una parte necesaria de Internet complica aún más la cuestión. Contar con protección contra bots maliciosos y la capacidad de gestionar el tráfico de bots legítimos es un atributo fundamental en cualquier solución que se plantee adquirir.

También existe el problema de **la escala para gestionar las aplicaciones corporativas.** Asimismo, mantener y dar soporte a aplicaciones altamente distribuidas es cada vez más difícil y, además, las expectativas de los usuarios cada vez son mayores. Las aplicaciones están en todas partes y en todo momento. Se encuentran dispersas por una plantilla que trabaja en sitios muy remotos, en algunos casos, en regiones de todo el mundo.

Es más, las aplicaciones se diseñan y ensamblan cada vez más a partir de fuentes dispares: marcos, scripts, diversas fuentes de contenido y ejecución de código en tiempo real que se produce desde multitud de ubicaciones. Es por ello por lo que necesita una solución que pueda adaptarse a ese contexto.

Visibilidad: si no tiene visibilidad de los ataques, no puede obtener información útil sobre cómo proteger mejor a sus clientes en tiempo real y mitigar las amenazas en el futuro. Las plataformas de seguridad más sólidas interactúan con miles de millones de dispositivos y cientos de millones de direcciones IP al día, y experimentan miles de millones de ataques DDoS al año. La solución que elija debe tener este tipo de alcance para ofrecerle visibilidad del panorama de amenazas existente.

Una de las quejas habituales tras infracciones graves es que los hackers fueron capaces de trabajar sin ser detectados durante X meses y que, una vez que los malos de la película estaban dentro, podían moverse a sus anchas por la red. Busque una solución que pueda proporcionarle una combinación de funciones de registro y control de acceso a aplicaciones más detalladas, con protección contra amenazas basada en sistema de nombres de dominio (DNS). Con ello obtendrá más visibilidad y reducirá el tiempo de detección de las infracciones.

Además, una solución de seguridad debe ofrecer visibilidad después de un ataque y proporcionar asistencia en tiempo real. Un centro de operaciones de seguridad debe funcionar como un único punto de contacto para la asistencia ante ataques y la respuesta a incidentes, en tiempo real, contra una amplia variedad de amenazas. Por eso, debería ayudarle a no limitarse a los paneles generales tras sufrir un ataque y a adquirir una visibilidad exhaustiva para realizar análisis forenses y de las causas de fondo con posterioridad al ataque.

Es posible que desee averiguar si una posible plataforma le permite gestionar varias soluciones a través de un único portal unificado que permita ver los ataques y el control de las políticas. También debe permitir integrar la solución en su herramienta de gestión de eventos e información de seguridad (SIEM) actual para tener una percepción y visibilidad más claras de todas sus soluciones de seguridad.

Inteligencia: junto con capacidad de red, su próxima solución debe proporcionar la experiencia que exige la creciente amenaza de ataques DDoS volumétricos. Una solución sobresaliente debe ser capaz de proporcionar mitigación de DDoS en cero segundos a través de un centro de operaciones de seguridad, con expertos del sector que proporcionen servicios de supervisión, barrido y mitigación de DDoS siempre activos.

La protección de sus aplicaciones, las API y los usuarios están relacionados con algo más que con la capacidad: exige inteligencia frente a amenazas. La inteligencia artificial y el aprendizaje automático desempeñan un papel fundamental a la hora de ofrecer una inteligencia capaz de mejorar su estrategia de seguridad. Busque plataformas con visibilidad de Internet de gran alcance, gran escala y distribución global, junto con funciones de ciencia de datos de vanguardia.

Un proveedor que cumpla estos requisitos debe ser capaz de ofrecer protección adaptable para el acceso y frente a las amenazas, así como inteligencia exhaustiva ante amenazas, mediante el uso de motores de aprendizaje automático que cuenten con la información adecuada. Tanto personas como algoritmos deben realizar análisis estadísticos, de tendencias y de patrones de datos estructurados y no estructurados, con el objeto de identificar y mitigar los nuevos vectores de ataque antes que nadie.

Cuando se implementa la seguridad en el borde de Internet, los activos quedan protegidos en una ubicación más cercana al propio ataque, y también se acerca la experiencia digital a los usuarios.

Ocho cosas que su solución de seguridad debe hacer por su organización.

Hasta ahora, hemos proporcionado un marco introductorio para iniciar el proceso de selección de plataformas de seguridad, así como las áreas críticas en las que centrarse mientras continúa con la investigación. Ahora, pasemos a lo esencial. ¿Qué aspectos clave debe cubrir su próxima solución de seguridad?

Garantizar que su empresa siga funcionando: el rendimiento es fundamental, pero la disponibilidad es esencial. El tiempo de inactividad y las interrupciones tienen un efecto negativo en los ingresos, la productividad y la reputación: la verdadera esencia de su empresa. La seguridad es, sencillamente, innegociable cuando hablamos de empresas digitales y de innovación. Su próxima solución de seguridad debe permitir una mitigación rápida y precisa, y ser capaz de identificar y detener las amenazas. Punto.

Proteger sus aplicaciones y API: las API son los componentes básicos de las aplicaciones modernas y el tejido conjuntivo entre las empresas que impulsan experiencias de usuario modernas y óptimas. Las organizaciones necesitan cientos de API, lo que amplía la superficie de ataque más allá de los límites tradicionales. Cada API es un posible punto de fallo en cuanto a seguridad, estabilidad y escalabilidad. La respuesta es un firewall de aplicaciones web (WAF) basado en la nube que proporcione una capa de seguridad entre las implementaciones en la nube y los consumidores que desean acceder a los datos, protegiendo los sitios web y las API contra ataques dirigidos oportunistas y persistentes.

Lograr un entorno Zero Trust: necesita una plataforma de seguridad que proporcione un marco que solo entregue aplicaciones y datos a usuarios autenticados y autorizados, permita la inspección y el registro en línea del tráfico, evite malware y filtraciones basadas en DNS, proteja a los usuarios finales frente a ataques de phishing, pueda identificar y bloquear el tráfico de bots, se conecte a aplicaciones SaaS modernas, así como a aplicaciones heredadas del centro de datos, se integre perfectamente con un WAF para mitigar los ataques en la capa de aplicaciones, y proporcione acceso a aplicaciones sin cliente, pero garantizando que estas sean rápidas y fiables. En resumen, necesita una plataforma que se adapte expresamente a su empresa y aplique solo las interacciones permitidas entre sus datos y sus usuarios.

Proporcionar seguridad en el borde de Internet: cuando se implementa la seguridad en el borde de Internet, los activos quedan protegidos en una ubicación más cercana al propio ataque, y también se acerca la experiencia digital a los usuarios. Básicamente, está implementando un panel único, una extensión de su infraestructura, que se encuentra entre usted (sus usuarios, sus experiencias digitales) y la naturaleza en constante cambio del entorno digital actual. En cierto sentido, se trata de una cuestión de topología física. En un momento en el que los usuarios esperan una experiencia digital fluida "a la carta", llevar las interacciones al borde de Internet, más cerca del origen de los datos, no solo facilita una mejor experiencia, sino que ofrece la mejor ubicación para situar mecanismos de protección entre la empresa y los usuarios y consumidores de experiencias digitales, que se encuentran dispersos geográficamente.

Ganar la partida a las amenazas avanzadas: algunas amenazas están diseñadas específicamente para esquivar las herramientas de seguridad. Su nueva plataforma de seguridad debe ser capaz de estar un paso por delante y ser más inteligente que estas amenazas avanzadas. Es fundamental que cualquier proveedor de seguridad respalde su tecnología con expertos en seguridad que investiguen los últimos métodos que utilizan los agentes maliciosos. Las soluciones de seguridad deben aprovechar la tecnología y la experiencia humana para mantenerse al día o incluso anticiparse al siguiente ataque de día cero.

Agilizar sus controles de seguridad: su próxima solución de seguridad debería permitirle ser más ágil y aprovechar la automatización y los scripts (orquestación). Nuestra premisa es que la seguridad digital es la base de la innovación empresarial y, por lo tanto, del crecimiento. Busque una solución que le permita obtener valor más rápidamente ayudándole a ser más eficiente durante la transformación digital.

Proporcionar asistencia ininterrumpida: puede que no baste con que su organización confíe exclusivamente en las herramientas anti DDoS automatizadas o en las reservas de banda ancha para la detección de ataques DDoS y su protección. Es probable que desee beneficiarse de acceso al personal de mitigación experto las 24 horas del día, los 7 días de la semana, los 365 días del año. Un centro de operaciones de seguridad siempre activo con presencia en todo el mundo para responder a los ataques en cualquier momento y lugar, junto con centros de barrido distribuidos por todo el mundo, garantiza una estrategia de seguridad más sólida capaz de desviar incluso los ataques más sofisticados y de mayor envergadura. La combinación de personas y tecnología puede marcar la diferencia entre la mediocridad y la excelencia. Decida si su empresa necesita servicios gestionados.

Proteger su marca e infundir confianza al cliente: en esencia, la confianza es el alma de su negocio. Y es lo que está en juego cuando su trabajo consiste en proteger su empresa y mitigar los riesgos.

Los responsables de la seguridad deben ayudar a equipar a sus empresas digitales con la mentalidad, los recursos y la planificación necesarios para recuperarse de interrupciones inevitables. Los fallos en cualquier parte del ecosistema pueden tener un efecto en cascada y perjudicial en la empresa. Dado que la seguridad ya no es simplemente un centro de costes, tiene la oportunidad de fomentar la transformación digital, aumentar los ingresos y afianzarse a sí mismo y a su equipo como base de la empresa y la innovación.