9 PRINCIPALES TENDENCIAS DE SEGURIDAD Y RIESGO EN 2020 SEGÚN GARTNER

La rápida migración a la computación en la nube, los requisitos de cumplimiento normativo y la evolución de las amenazas siguen siendo los principales desafíos.

Responder a la complejidad de los efectos que trajo aparejado el COVID-19 sigue siendo el mayor desafío para la mayoría de las organizaciones de términos de seguridad en 2020.

“La pandemia, y los cambios resultantes en el mundo empresarial, aceleraron la digitalización de los procesos empresariales, la movilidad de las terminales y la expansión de la computación en la nube en la mayoría de las organizaciones, revelando el pensamiento y las tecnologías heredadas”, afirma Peter Firstbrook, vicepresidente de análisis de Gartner.

El COVID-19 reorientó a los equipos de seguridad en el valor de las herramientas operativas y de seguridad entregadas en la nube que no requieren una conexión LAN para funcionar, revisando las políticas y herramientas de acceso remoto, la migración a los centros de datos en la nube y las aplicaciones SaaS, y asegurando nuevos esfuerzos de digitalización para minimizar interacciones de persona a persona.

Gartner ha identificado nueve tendencias principales anuales que son la respuesta de las organizaciones líderes a estas tendencias externas a largo plazo.

Estas tendencias destacan cambios estratégicos en el ecosistema de seguridad que aún no son ampliamente reconocidos, pero se espera que tengan un impacto amplio en la industria y un potencial significativo de disrupción.

• 9 TENDENCIAS SEGÚN GARTNER

TENDENCIA N. ° 1: Surgen capacidades extendidas de detección y respuesta para mejorar la precisión y la productividad

Están surgiendo soluciones de detección y respuesta extendidas (XDR) que recopilan y correlacionan automáticamente datos de múltiples productos de seguridad para mejorar la

detección de amenazas y proporcionar una capacidad de respuesta a incidentes. Por ejemplo, un ataque que provocó alertas en el correo electrónico, el punto final y la red se puede combinar en un solo incidente. Los objetivos principales de una solución XDR son aumentar la precisión de detección y mejorar la eficiencia y productividad de las operaciones de seguridad.

"La centralización y normalización de datos también ayuda a mejorar la detección al combinar señales más suaves de más componentes para detectar eventos que de otro modo podrían ignorarse", dice Firstbrook.

TENDENCIA N. ° 2: Surge la automatización de procesos de seguridad para eliminar las tareas repetitivas

La escasez de profesionales de la seguridad capacitados y la disponibilidad de la automatización dentro de las herramientas de seguridad han impulsado el uso de una mayor automatización de los procesos de seguridad. Esta tecnología automatiza las tareas de operaciones de seguridad centradas en la computadora basándose en reglas y plantillas predefinidas.

Las tareas de seguridad automatizadas se pueden realizar mucho más rápido, de forma escalable y con menos errores. Sin embargo, hay rendimientos decrecientes por construir y mantener la automatización. Los líderes de SRM deben invertir en proyectos de automatización que ayuden a eliminar las tareas repetitivas que consumen mucho tiempo, dejando más tiempo para centrarse en funciones de seguridad más críticas.

TENDENCIA N. ° 3: La Inteligencia Artificial crea nuevas responsabilidades de seguridad para proteger las iniciativas empresariales digitales

La inteligencia artificial, y especialmente el aprendizaje automático (ML), continúa automatizando y aumentando la toma de decisiones humanas en un amplio conjunto de casos de uso en seguridad y negocios digitales. Sin embargo, estas tecnologías requieren experiencia en seguridad para abordar tres desafíos clave: proteger los sistemas comerciales digitales impulsados por IA, aprovechar la IA con productos de seguridad empaquetados para mejorar la defensa de la seguridad y anticipar el uso nefasto de la IA por parte de los atacantes.

TENDENCIA N. ° 4: Los jefes de seguridad (CSO) de nivel empresarial emergen para unir múltiples silos orientados a la seguridad

En 2019, los incidentes, las amenazas y las divulgaciones de vulnerabilidades fuera de los sistemas de TI empresariales tradicionales aumentaron y empujaron a las organizaciones líderes a repensar la seguridad en el mundo físico y cibernético. Las amenazas emergentes, como los

ataques de ransomware en los procesos comerciales, los posibles ataques de siegeware en los sistemas de gestión de edificios, la suplantación de GPS y las continuas vulnerabilidades del sistema OT / IOT se extienden por el mundo ciberfísico. Las organizaciones centradas principalmente en esfuerzos centrados en la seguridad de la información no están equipadas para hacer frente al efecto de las fallas de seguridad en la seguridad física.

Como resultado, las organizaciones líderes que implementan sistemas ciberfísicos están implementando CSO a nivel empresarial para reunir múltiples silos orientados a la seguridad, tanto con fines defensivos como, en algunos casos, como habilitadores comerciales. El CSO puede agregar seguridad de TI, seguridad OT, seguridad física, seguridad de la cadena de suministro, seguridad de gestión de productos y programas de salud, seguridad y medio ambiente en una organización centralizada y un modelo de gobierno.

TENDENCIA Nº 5: La privacidad se está convirtiendo en una disciplina propia

Ya no es “solo una parte del” cumplimiento, legal o de auditoría, la privacidad se está convirtiendo en una disciplina propia cada vez más influyente y definida, que afecta a casi todos los aspectos de una organización.

Como disciplina independiente de rápido crecimiento, la privacidad debe estar más integrada en toda la organización. Específicamente, la disciplina de privacidad codirige la estrategia corporativa y, como tal, debe alinearse estrechamente con seguridad, TI / OT / IoT, adquisiciones, recursos humanos, legal, gobierno y más.

TENDENCIA N. ° 6: Los nuevos equipos de "confianza y seguridad digitales" se centran en mantener la integridad de todas las interacciones donde el consumidor se encuentra con la marca

Los consumidores interactúan con las marcas a través de una variedad cada vez mayor de puntos de contacto, desde las redes sociales hasta el comercio minorista. Lo seguro que se siente el consumidor dentro de ese punto de contacto es un diferenciador comercial. La seguridad de estos puntos de contacto a menudo la gestionan grupos discretos, con unidades de negocio específicas que se centran en las áreas que ejecutan. Sin embargo, las empresas se están moviendo cada vez más hacia equipos de seguridad y confianza multifuncionales para supervisar todas las interacciones, lo que garantiza un nivel estándar de seguridad en cada espacio donde los consumidores interactúan con la empresa.

TENDENCIA N. ° 7: La seguridad de la red se transforma del enfoque en modelos de dispositivos basados en LAN a SASE

Los servicios de seguridad entregados en la nube se están volviendo cada vez más populares con la evolución de la tecnología de oficina remota. La tecnología Secure Access Service Edge (SASE) permite a las organizaciones proteger mejor a los trabajadores móviles y las aplicaciones en la nube al enrutar el tráfico a través de una pila de seguridad basada en la nube, en lugar de hacer retroceder el tráfico para que fluya a través de un sistema de seguridad físico en un centro de datos.

TENDENCIA N. ° 8: Un enfoque de ciclo de vida completo para la protección de los requisitos dinámicos de las aplicaciones nativas de la nube

Muchas organizaciones utilizan el mismo producto de seguridad en los puntos finales orientados al usuario final que para las cargas de trabajo del servidor, una técnica que a menudo continúa durante las migraciones de "elevación y cambio" a la nube. Pero las aplicaciones nativas de la nube requieren diferentes reglas y técnicas, lo que lleva al desarrollo de la protección de cargas de trabajo en la nube (CWPP). Pero a medida que las aplicaciones se vuelven cada vez más dinámicas, las opciones de seguridad también deben cambiar. La combinación de CWPP con la gestión emergente de la postura de seguridad en la nube (CSPM) representa toda la evolución de las necesidades de seguridad.

TENDENCIA N. ° 9: La tecnología de acceso a la red de confianza cero comienza a reemplazar las VPN

La pandemia de COVID ha puesto de relieve muchos de los problemas con las VPN tradicionales. El acceso a la red emergente de confianza cero (ZTNA) permite a las empresas controlar el acceso remoto a aplicaciones específicas. Esta es una opción más segura, ya que "oculta" las aplicaciones de Internet: ZTNA solo se comunica con el proveedor de servicios ZTNA y solo se puede acceder a él a través del servicio en la nube del proveedor ZTNA.

Esto reduce el riesgo de que un atacante aproveche la conexión VPN para atacar otras aplicaciones. La adopción de ZTNA a gran escala requiere que las empresas tengan un mapeo preciso de qué usuarios necesitan acceso a qué aplicaciones, lo que ralentizará la adopción.

Obtenido de: https://www.gartner.com/smarterwithgartner/gartner-top-9-security-and-risk-trends-for-2020/?utm_campaign=EVT_GB_2020_SWG_NL_NL5&utm_medium=email&utm_source=Eloqua&cm_mmc=Eloqua-_-Email-_-LM_EVT_GB_2020_SWG_NL_NL5-_-0000