FORTINET

REPORTE

Los cuatro desafíos de ciberseguridad más críticos de nuestra generación

Tendencias de la industria

La transformación que la mayoría de las redes está experimentando actualmente es mucho más grande e impactante de lo que la mayoría de las personas reconoce. Los dispositivos IoT, la computación en la nube y el rápido desarrollo de aplicaciones empresariales, han acelerado la recopilación y distribución de Big Data. Los centros de datos encargados de extraer esos datos para impulsar aún más la agilidad y la capacidad de respuesta del negocio están sumando inteligencia artificial y aprendizaje automático para hacerlo posible. El resultado es hipervelocidad, hiperconectividad e hiperescala, todos creciendo a una tasa exponencial.

Todo esto sienta las bases para cosas como automóviles inteligentes, edificios inteligentes, ciudades inteligentes e infraestructuras inteligentes, incluidos el transporte inteligente, las redes eléctricas y la manufactura. El crecimiento de dispositivos móviles más rápidos e inteligentes y los nuevos modelos de computación en el borde, impulsados por 5G acelerarán todo esto aún más y con mayor rapidez, a medida que miles de millones de nuevos entornos de borde se agregan e interconectan a través de una red global de redes, tanto públicas como privadas.

En este nuevo entorno, los humanos simplemente no pueden moverse lo suficientemente rápido como para agregar seguridad como una ocurrencia tardía, especialmente cuando las redes son a menudo ad hoc y cada vez más temporales. Si pretendemos proteger los datos, la información personal y las infraestructuras críticas contra ciberdelincuentes en un entorno en constante cambio, la ciberseguridad debe ser una característica fundamental de cada producto y sistema desde el momento en que se concibe, lo que le permitirá interoperar, expandirse y contraerse automáticamente, así como crecer en tiempo real.

Para alcanzar este grado de profunda integración de la seguridad, algo absolutamente esencial para lograr y mantener una sociedad y una economía verdaderamente digitales, los líderes de negocios deben prestar atención a cuatro desafíos fundamentales:

1. Compartir información en tiempo real

Los ataques pueden penetrar en un dispositivo o red en un abrir y cerrar de ojos, explotando incluso brechas de seguridad temporales debido a sistemas de seguridad no integrados que luchan por ponerse al día con los cambios dinámicos en las conexiones de red y en la infraestructura. En el mundo actual, donde todo es bajo demanda, la velocidad es fundamental para una estrategia efectiva de ciberseguridad. Y para hacer que el desafío sea más difícil, también se cifra un porcentaje cada vez mayor del creciente volumen del tráfico de Internet.

La velocidad es crítica y depende de su profunda integración en los dispositivos y sistemas que se protegen. Pero la velocidad por sí sola no es suficiente. También se necesita visibilidad, y eso requiere acceso a información sobre amenazas en tiempo casi real. Compartir inteligencia de amenazas entre dispositivos en la misma red es esencial, pero incluso eso no es suficiente. El intercambio de información también tiene que ocurrir entre organizaciones y entidades que tradicionalmente han sido aisladas.

Los ciberdelincuentes de hoy no reconocen las fronteras políticas o geográficas y nuestra nueva economía digital está tan profundamente interconectada por la tecnología, que la ciberseguridad y la seguridad global se han convertido en la misma cosa. El resultado es que ninguna organización, pública o privada, puede tener una visión completa de todo el panorama cibernético y defenderse activamente contra las amenazas cibernéticas a menos que todos compartamos activamente la inteligencia de amenazas.

2. Colaborar de manera amplia y profunda

La colaboración permite a los buenos crear una mente colectiva, aprender rápidamente, expandiendo constantemente nuestra competencia y capacidad. Si las organizaciones o los estados no aprenden unos de otros, los mismos ataques derribarán innecesariamente innumerables entidades.

Esta colaboración debe ser amplia y profunda. Amplia porque todos participan en una conversación común sobre ciberseguridad y en cómo abordar a nuestros enemigos comunes. Y profunda porque la conversación sola no es suficiente. Necesitamos trabajar juntos para profundizar nuestro conocimiento colectivo colaborando en el intercambio de inteligencia sobre amenazas, colaborando en la educación y colaborando en la próxima generación de tecnologías de ciberseguridad aumentadas por el aprendizaje automático y la inteligencia artificial.

Se proyecta que el costo estimado del daño causado por cibercriminales, malware y violaciones de datos alcanzará los $ 6 trillones de dórales para 2021. Para potenciar el liderazgo para enfrentar estos desafíos, los expertos tecnológicos y los tomadores de decisiones de alto nivel en los sectores público y privado deben trabajar juntos.

Más del 92% del malware se entrega a través de correo electrónico. Con las políticas y campañas de concienciación adecuadas, así como la diligencia en la práctica, podríamos eliminar más del 90% del malware simplemente enseñando nuevas habilidades que superen los comportamientos arraigados.

3. Crear y promover una visión de ciberseguridad integrada

Para que el intercambio de información y la colaboración sean efectivos, todos debemos tener una visión y un compromiso singulares para construir una estrategia de seguridad informática verdaderamente integrada. Esta visión para la ciberseguridad integrada debe ser amplia e inclusiva, anticipando las próximas acciones de los ciberdelincuentes en lugar de solo reaccionar ante ellas.

Esto debe ser un esfuerzo global, donde la educación y capacitación en ciberseguridad se convierta en parte del desarrollo educativo de todos. Nos enfrentamos a una creciente brecha de habilidades de ciberseguridad que amenaza la existencia misma de nuestra incipiente economía digital y necesitamos una estrategia que abarque a las organizaciones públicas y privadas para educar a las personas a ser más conscientes de los riesgos de operar en un mundo digital, al tiempo que protegemos a las futuras generaciones de profesionales de ciberseguridad que tanto necesitamos. Sin estos esfuerzos, no tendremos suficientes soldados experimentados para luchar en esta guerra.

4. Promover la plataforma tecnológica

Para la mayor parte de la infraestructura digital del mundo, la ciberseguridad nunca fue parte del diseño. Esto debe cambiar y se empieza por entender los desafíos subyacentes.

Primero, la ciberseguridad requiere enormes cantidades de potencia informática, a menudo más que cualquier otro sistema en red. De ahora en adelante, la mayoría de los productos, dispositivos e infraestructura deben tener esta potencia informática adicional diseñada. Además, las funciones de ciberseguridad dentro de los dispositivos deben caber en una plataforma integrada que distribuya las cargas de trabajo en las capas de un sistema.

Después, la red debe tener capacidad de autodefensa y no depender por completo de dispositivos de seguridad especialmente diseñados. Esta estrategia de red basada en la seguridad cambia muchos de los supuestos tradicionales de la red. En lugar de buscar solo la ruta más rápida, la red basada en la seguridad toma en cuenta el riesgo de cada ruta y mueve el tráfico por la ruta segura más rápida. Para que esto funcione, todos los dispositivos de red necesitan compartir información sobre la velocidad y el riesgo de cada ruta de red.

Se debe brindar una seguridad sólida en toda la red distribuida, combinada con baja latencia y alto rendimiento, especialmente con la implementación de redes 5G. Esto solo puede suceder cuando la seguridad está integrada en cada dispositivo, lo que les permite detectar, correlacionar y colaborar automáticamente con otros dispositivos para crear y mantener una red de seguridad en entornos dinámicos que están en constante cambio.

Y finalmente, necesitamos invertir en aprendizaje automático e inteligencia artificial para aumentar nuestra capacidad de correlacionar todos estos datos, detectar anomalías y amenazas, responder en tiempo real y compartir nueva inteligencia en un repositorio común para que todos estén más seguros.

Avanzar hacia un mundo protegido

Independientemente de la industria, el mercado vertical y la geografía, los líderes de negocios, la industria y el gobierno tienen la responsabilidad de guiar a sus organizaciones hacia un mundo más seguro. En un clima permeado por la falta de confianza y la escasa cooperación, los únicos ganadores son los cibercriminales.

Solo a través de una verdadera integración, en todos los dispositivos, redes públicas y privadas, industrias y fronteras nacionales y geográficas, la seguridad cibernética puede crear un mundo verdaderamente protegido.