Opinión

Eutimio Fernández,
MIEMBRO DEL GRUPO DE SEGURIDAD AUTELSI.
DIRECTOR DE SEGURIDAD EN CISCO ESPAÑA.

Ciber-seguridad y transformación digital

Hoy en día nadie duda del proceso de transformación digital en el que estamos inmersos las personas, las administraciones públicas y las empresas.

En muchos casos transformación y en otros muchos aceleración digital, donde tendencias tecnológicas como Internet de las Cosas, Cloud, Movilidad, Big Data & Analytics, necesitan de una capa de seguridad cada día más sofisticada.

Según el Informe Anual de Seguridad de Cisco, sólo el 45% de las organizaciones confían en su estrategia para hacer frente a unos ciberataques cada vez más organizados y persistentes, mientras el 92% de los dispositivos de Internet albergan vulnerabilidades conocidas y el 36% de los equipos ya no cuentan con soporte o están descatalogados.

A su vez, la ciberdelincuencia se ha profesionalizado, constituyendo todo un "sector económico" que genera unos beneficios anuales estimados de entre 450.000 millones y un billón de dólares (aproximadamente entre el 1 y el 2% del PIB mundial o entre el 50 y 100% del PIB español).

En España, el Instituto Nacional de Ciberseguridad (INCIBE) calcula que las empresas españolas perdieron 14.000 millones de euros en 2014 por ciberataques que se han incrementado un 200% hasta noviembre de 2015 (39.985 incidentes) frente al año anterior.

Palanca para la innovación y el crecimiento

Los CEOs y responsables de TI están enormemente preocupados por esta situación, ya que la seguridad no es sólo un mecanismo de protección sino también un facilitador de la transformación digital, y por tanto de innovación y crecimiento.

El 64% de los directivos consultados por Cisco en su informe anual consideran que la ciber-seguridad constituye un pilar esencial para su digitalización, y siete de cada diez afirman que la preocupación por las amenazas está frenando su innovación y por tanto limitando sus nuevas oportunidades de negocio.

A este escenario hay que añadir el déficit de profesionales en ciberseguridad (2 millones en 2019 a escala global) y la creciente complejidad: las redes se componen de múltiples elementos objetivo del malware, incluyendo dispositivos, terminales, aplicaciones y cada vez más objetos conectados bajo el concepto de Internet de las Cosas, como ejemplo los 210 millones de conexiones M2M previstas para 2020 en España, el 62% del total de conexiones.

La red como sensor

Conocer con claridad la actividad de los objetos conectados, las aplicaciones, los usuarios y los dispositivos que hacen uso de la infraestructura es crítico para poder aplicar las políticas correctas de prevención, remedio y análisis, en la estrategia de protección, ya que no podemos proteger lo que no conocemos.

Y la red, que es el elemento estratégico fundamental que está en todas partes de cualquier organización, que como su sistema nervioso, puede utilizarse como un gran sensor para obtener una completa visibilidad de los flujos, amenazas, malware y violaciones de las políticas de seguridad.

De hecho, debido a la sofisticación y a la escasa visibilidad, el tiempo medio que el malware permanece en los sistemas corporativos sin ser detectado se sitúa actualmente entre los 100 y 200 días. Sólo con una visibilidad completa de la red, una inteligencia global que nos permita detectar amenazas de día cero y una gestión unificada de todas las soluciones de seguridad, bajo una arquitectura coordinada y proactiva es posible reducir este tiempo a menos de 24 horas, con la consiguiente reducción del riesgo.

En definitiva, para que la ciberseguridad constituya un impulsor y no suponga un freno a la transformación digital, las organizaciones deben adoptar una nueva estrategia de seguridad integrada, centrada en las amenazas y con la visibilidad necesaria para detectar y detener el malware antes, durante y después de los ataques. ✦