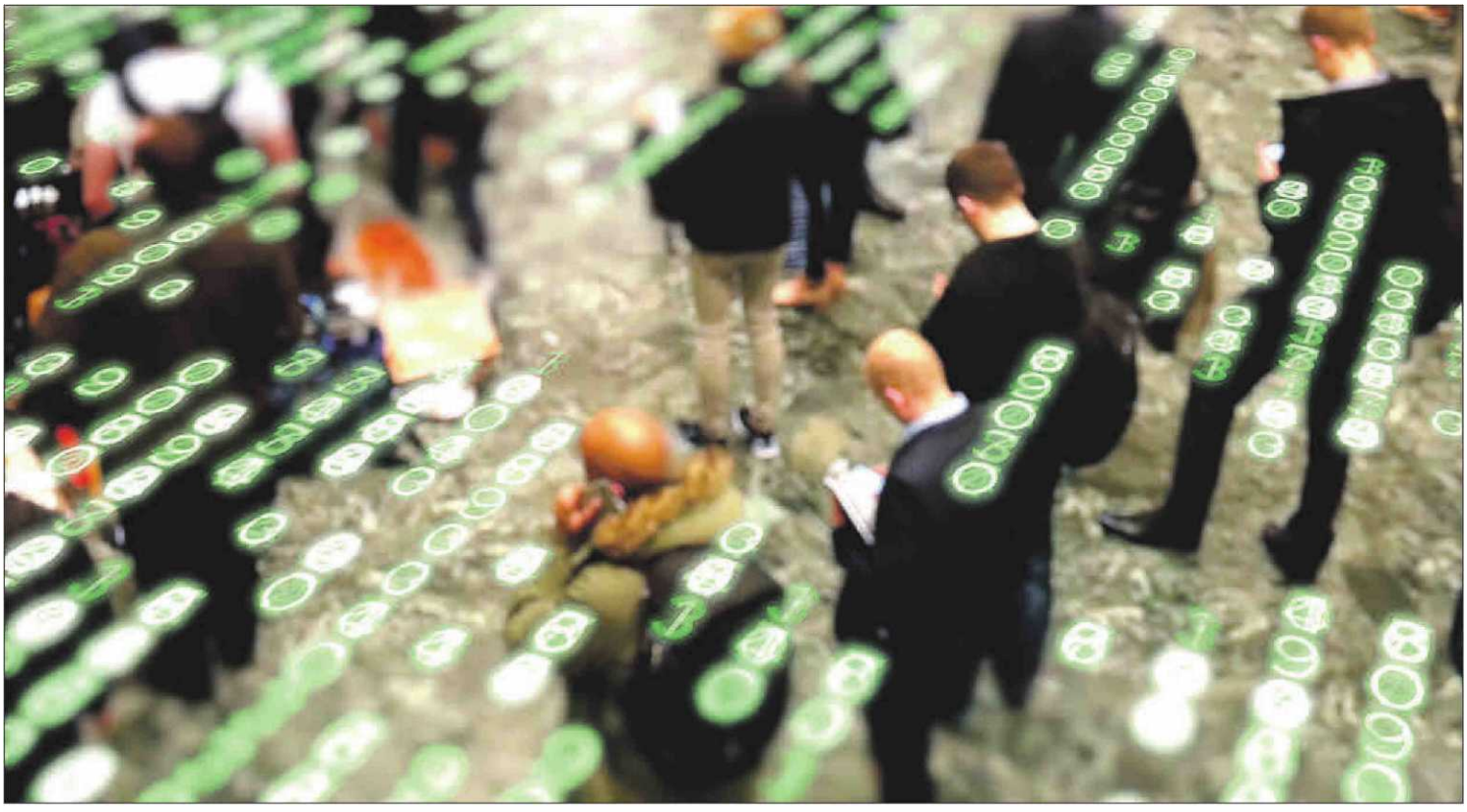
El Economista - 24.05.2017



ISTOCK

Gestión preventiva de amenazas, la mejor defensa contra ciberataques

Expertos de Indra opinan sobre cómo responder a campañas de 'malware'

elEconomista MADRID.

La mejor forma de afrontar un ciberataque es partir del supuesto de que ya podrías estar infectado. Esta es la premisa de la que parte el equipo de ciberseguridad de Minsait, la unidad de negocio de Indra que da respuesta a los retos de la transformación digital, para proteger a las empresas e instituciones a las que da servicio.

Según el director de Operaciones de Ciberseguridad de esta unidad, Alberto López, hay algunas medidas que ayudan a hacer frente un incidente de *ransomware*. La primera de ellas pasa por disponer de herramientas que ofrezcan visibilidad de lo que está ocurriendo en la red y que permitan llevar a cabo acciones de contención y aislamiento, que eviten la propagación del *malware* o virus en caso de contagio. Para ello, se emplean técnicas de monitorización del tráfico y de segmentación dinámica de red que dan luz verde o bloquean ciertas actividades en función de las distintas situaciones posibles.

No importa si los sistemas parecen estar funcionando sin problemas. Lo urgente es rastrear posibles virus y amenazas dentro de la Red. "Las empresas pueden tardar una media de 60 días, más de tres meses, en descubrir que han sido víctimas de un ataque", explica López.

El *software* malicioso *WannaCry* –que, desde que empezase su ataque, ha llegado a infectar a más de 230.000 equipos de casi 200 países diferentes– cifra y *secuestra* archivos para pedir un rescate y su presencia se detecta de forma inmediata una vez se ha activado, pero otro tipo de *malware* utiliza la estrategia contraria: pasar inadvertidos para robar información o alterar el funcionamiento de los equipos sin que el usuario lo perciba. Estas amenazas *silenciosas* provocan pérdidas de más de 360.000 millones de euros al año en todo el mundo.

Otra de las medidas para hacer frente a un ataque de *ransomware*, según los expertos de Minsait, es defender los sistemas y redes corporativas frente a las principales vías de infección: el correo electrónico, la navegación en Internet o las conexiones con redes de terceros.

Asimismo, Minsait utiliza técnicas de *hunting o caza de ciberataques* para rastrear la red en busca de comportamientos inusuales y disponer de registros que, llegado el caso, permitan reconstruir cómo se ha producido un incidente.

"Estas medidas deben englobarse dentro de un marco de buen gobierno de la empresa que, además de aspectos tecnológicos y técnicos, contemple otros elementos como protocolos de actuación, aspectos legales o de comunicación, entre otros" comenta López, destacando además que no se trata de implantar elementos concretos o aislados, como puede ser un antivirus o un sistema de *back up*, sino de incorporar la ciberseguridad como proceso crítico en todos los ámbitos de actividad de la empresa.

Atajar una situación de crisis

Durante el último ataque vivido, la red de centros avanzados de ciberseguridad (i-CSOC) de Minsait en Europa y Latinoamérica ha estado a pleno rendimiento: ha monitorizado las redes y sistemas de distintas empresas e instituciones y ha aplicado técnicas de *reversing* para estudiar el *malware WannaCry* y determinar cómo funciona y cómo se propaga.

También ha informado a sus clientes y emitido recomendaciones, apoyándose en la red de contactos que mantiene con los principales proveedores de soluciones de ciberseguridad del mundo.

Respecto a si todas las empresas pueden acceder a las tecnologías y servicios necesarios para protegerse, desde Minsait explican que están ofreciendo la ciberseguridad como servicio, de modo que cualquier compañía, ya sea grande, mediana o pequeña, pueda beneficiarse de las herramientas más avanzadas, pagando solo por el uso que hace de ellas.

Así, López explica que el objetivo de esta unidad de negocio es "proporcionar un esquema de trabajo que facilite a cualquier tipo de organización mecanismos avanzados para minimizar el número de ataques exitosos e identificar de forma temprana aquellos que hayan vulnerado las medidas desplegadas, minimizando su impacto".

La importancia de los simulacros y la formación para saber actuar

Una de las lecciones que deja 'WannaCry' es que ninguna empresa está libre de sufrir un ataque. Por eso en Minsait ven imprescindible que toda compañía disponga de un plan de gestión de crisis, que identifique qué personas intervendrán, cuál será su rol y cómo se tomarán las decisiones. También hay que fijar una política de comunicación interna y externa. Para probar la validez de estos planes es necesario realizar simulacros que pongan en juego las medidas implantadas con 'fuego real'. López explica que "en Minsait, a través de nuestro servicio 'Threat Assessment' lanzamos de manera permanente campañas de 'ransomware' y otro tipo de ataques contra un entorno controlado que desplegamos en nuestro cliente. Evaluamos la eficacia de procedimientos y controles y analizamos en tiempo real si los ataques se bloquean con éxito". Asimismo, en Minsait trabajan en formar a los profesionales para que conozcan los riesgos y sepan cómo actuar para asegurar la continuidad del negocio.