Infraestructuras críticas: un desafío mayor aún para la seguridad

Félix Muñoz
Director de Seguridad del Grupo Entelgy

Transportes, energía, sistemas financieros, telecomunicaciones… Hablar de infraestructuras críticas es hacerlo de todos aquellos servicios indispensables en el día a día de cualquier sociedad. ¿Se imaginan una ciudad, un país entero, sin luz? ¿Un ataque a nivel nacional a los sistemas de agua potable? ¿Un fallo global en todos los cajeros automáticos al mismo tiempo? Sin duda, sólo imaginarlo provoca escalofríos. Esa es, precisamente, la razón de que se consideren a todos estos sectores, y más concretamente a las instalaciones, redes y procesos de trabajo que los sustentan, como infraestructuras críticas o estratégicas.

Las infraestructuras críticas, por su trascendencia, deben tener asegurada su disponibilidad y funcionamiento correcto en todo momento. Y su seguridad debe contemplarse de forma global, abarcando las dimensiones física y virtual. Pero, además, no se puede, ni debe, olvidar las ciberamenazas, cada vez más presentes y con consecuencias especialmente negativas.

Y es que Internet ha supuesto un riesgo añadido a las ya sensibles infraestructuras críticas. A uno de los problemas de base que presentan –los dispositivos y las tecnologías usadas para gestionar los sistemas de control no fueron diseñados en su día para ser conectados a redes remotas o públicas–, se suma ahora su conexión a la Red.

Antes, los sistemas de control estaban aislados o con acceso muy restringido. Actualmente, están conectados a Internet y, consecuentemente, a las miles de ciberamenazas y ciberataques que la Red esconde y que representan un peligro con una probabilidad mucho más alta que el asalto físico y con un menor riesgo para el ciberdelincuente, tal y como apunta Francisco Martínez, secretario de Estado de Seguridad de España.

Iniciativas legislativas

Sin duda, esta nueva dimensión requiere medidas de control incluso gubernamentales. Por ello, en los últimos años han sido varias las iniciativas legislativas que han surgido en todo el mundo para tratar de asegurar, de algún modo, la disponibilidad y correcto funcionamiento de las infraestructuras críticas.

En el caso de España, la Ley 08/2011 establece una definición oficial de infraestructuras críticas: "Las infraestructuras estratégicas cuyo funcionamiento es indispensable y no permite soluciones alternativas, por lo que su perturbación o destrucción tendría un grave impacto sobre los servicios esenciales". Esta misma norma establece medidas para la protección de las infraestructuras críticas: el operador designado como crítico deberá elaborar un Plan de Seguridad del Operador (PSO) y un Plan de Protección Específico (PPE) por cada una de las infraestructuras críticas que posea o gestione. Hasta la fecha, se han nombrado 93 operadores críticos y se han identificado más de 300 infraestructuras críticas de sectores como el energético, el de la industria nuclear, el financiero, el del transporte y el del agua.

En Latinoamérica, un continente clave para Entelgy, muchos de sus Estados cuentan ya con avances notables en lo relativo a una estrategia y marco legal nacional de ciberseguri-

dad y ciberdefensa para la protección de las infraestructuras críticas, estando en desarrollo el resto de ellos. En este sentido, los trabajos que se están realizando en la región deben apoyarse en experiencias previas internacionales registradas en Europa, EEUU y países pioneros en la materia.

Los obstáculos que nos podemos encontrar son los mismos que se han experimentado en otros países. Pero con el asesoramiento y la información adecuados se pueden lograr los objetivos de forma acertada en base a las lecciones aprendidas. Además, contamos con una ventaja estratégica adicional: el grado de concienciación actual en Latinoamérica es muy alto.

Al respecto, 14 países latinoamericanos cuentan ya con equipos de respuesta a incidentes de seguridad informática (CSIRT, por sus siglas en inglés), entre los que se encuentran el ArCERT argentino –que, posteriormente, daría lugar al ICIC–, el CLCERT chileno, el CTIR Gov brasileño, el CTIRGT guatemalteco, el CERTUy uruguayo, el VenCERT venezolano, el PerCERT peruano y el ColCERT colombiano.

La protección, un reto

El aumento de ataques contra infraestructuras críticas es una realidad. El cambio a sistemas propietarios, abiertos e interconectados de los sistemas que controlan estas infraestructuras ha disparado las amenazas y los riesgos. En España, los ciberataques a infraestructuras críticas han pasado de 17 a 134 en sólo tres años. Y en 2016, según el Ministerio del Interior, serán 300. Estos ataques se dirigen a sectores estratégicos como el energético, el del agua, el financiero o el alimentario, que, en caso de fallo, generarían un auténtico caos en la sociedad.

Y los datos no son mucho mejores en Latinoamérica, donde, recientemente, la Organización de los Estados Americanos (OEA) publicaba un informe en el que alertaba del, cada vez mayor, riesgo informático al que se enfrentan las infraestructuras críticas de la región. El estudio tomaba como base una encuesta a la que contestaron 575 organismos públicos y privados relacionados con las comunicaciones, la banca, las manufacturas, la energía y la seguridad.

De manera anónima, y sin aportar detalles que comprometan su seguridad, el 60 por ciento de los participantes revelaba que ha sufrido intentos de robar sus datos, principalmente, a través del conocido como *phising*, el ataque más habitual, un engaño para que la víctima permita el acceso de *software* maligno a su equipo –como los falsos *e-mails* de bancos o Correos–.

Pero, además, el informe pone de manifiesto que están en ascenso otras variedades más inquietantes: el 40 por ciento de los encuestados afirma que ha habido intentos de inutilizar sus ordenadores, el 44 por ciento ha registrado ataques para borrar sus archivos y el 54 por ciento ha detectado intención de manipular sus sistemas.

Estamos ante un complicado escenario en el que InnoTec, la empresa de ciberseguridad del Grupo Entelgy, ofrece una solución para la provisión y gestión centralizada de seguridad, mediante acceso remoto seguro, gracias a sus alianzas con empresas líderes del sector.

Con clientes de Latinoamérica de primer nivel, como Grupo Aval, ATH, Porvenir, IBM, el Banco de la República, ACH, Alkosto, Old Mutual o la Universidad de La Sabana, el enfoque de InnoTec para la protección de sistemas críticos contempla cinco niveles:

- **Identificación:** Descubrimiento e inventariado automatizados de dispositivos.
- **Protección:** Entrega y despliegue automatizados de parches y actualizaciones.
- **Detección:** Recolección y gestión de registros de seguridad junto a análisis de incidentes.
- **Respuesta:** Acceso remoto seguro dispositivo a dispositivo.
- **Recuperación:** *Backup* y restauración.

Un enfoque global que tiene en cuenta nuevas necesidades más allá de la clásica tríada de confidencialidad, integridad y disponibilidad. Una propuesta inteligente y con una mirada lateral en la que ponerse en el lugar del atacante, analizando nuevas formas de proteger nuestros activos, dificultando no sólo penetrar en la infraestructura, sino evitando que el atacante se mueva horizontalmente por la misma para encontrar nuevos vectores de ataque y persistencia. En definitiva, la seguridad entendida como un todo en el que la inteligencia es la clave. ■