Los Equipos de Respuesta de Incidencias Informáticas y su decisiva importancia para la seguridad de las organizaciones

Análisis Flash ESYS | Raquel Jorge Ricart – octubre 2022

En el CyberLunch de octubre organizado por la Fundación ESYS, los expertos Juan Carlos Gómez Castillo, director global de seguridad digital en Telefónica, y Pedro Hernández Liarte, gerente del CSIRTglobal de Telefónica, han abordado el papel determinante y los retos a los que se enfrenan los conocidos como Equipos de Respuesta de Incidencias Informáticas (CSIRT).

Los CSIRT son plataformas que se han convertido en herramientas claves y estratégicas para hacer frente a los ciberataques, las vulnerabilidades cibernéticas y otras amenazas que puedan afectar a ciertos productos, procesos o personas dentro de una organización. También tienen una incidencia muy relevante en la supervivencia de cualquier institución, y en el propio bienestar de las personas que dependen de los servicios que una organización provee, como es el caso de infraestructuras críticas (electricidad, agua) que reciben un ciberataque.

Hacia un cambio de mentalidad en la gestión de incidentes informáticos

Los CSIRT han existido desde hace muchos años, pero el incremento de ciberataques, la sofisticación de estos y el impacto que puede tener a nivel social, económico y reputacional han hecho que **sea necesario cambiar de mentalidad en las corporaciones a la hora de gestionar los incidentes informáticos** en dos sentidos.

Durante la conversación con los expertos se ha podido constatar que, en primer lugar, es necesario tener en mente que siempre vamos a poder estar comprometidos por un ciberataque o vulnerabilidad. De ahí que sea fundamental trabajar en la detección y respuesta continua y no solo en la gestión reactiva antes dichos incidentes. En segundo lugar, Gómez y Hernández han puntualizado que ya no hablamos de dos tipos de empresas (las que ya han sido atacadas y las que van a ser atacadas), sino de las que sí se protegen y aquellas que no lo hacen.

Entendiendo los mecanismos de coordinación de los CSIRT

Cuando ocurre un incidente informático, es tan importante hacer frente al mismo a través del ciclo de vida de respuesta a este incidente (recopilación de datos y fuentes, análisis y respuesta), como ser capaces de **asegurar una efectiva coordinación entre los actores involucrados.**

Lo primero que han dejado claro los expertos invitados es que los CSIRT no trabajan solos, sino que hay diferentes equipos que hacen frente a las tres fases en la gestión de la ciberseguridad: anticipación, detección y respuestas.

Tipo de equipo	Fase de gestión de la ciberseguridad en que participa
SOC (Security Operations Centre)	Monitoreo de la seguridad
CSIRT	Gestión de incidentes
Threat Hunting	Gestión de un evento de seguridad
Ciberinteligencia	Adquisición y análisis de inteligencia, que transmiten al equipo de Threat Hunting o al CSIRT según el tipo de información.
Red Team	Anticipación y detección de potenciales vulnerabilidades, testeando las debilidades del propio sistema de la organización, simulando ser un atacante externo.

No solamente se trabaja caso por caso ante una incidencia, gestión de seguridad y vulnerabilidad, sino que también existen otras áreas de colaboración, a través de **ciberejercicio**s internos (organizados por la propia empresa) y externos (tanto nacionales como europeos e internacionales).

Los retos y oportunidades de los CSIRT

Otra de las claves apuntada durante la conversación de ese CyberLunch es que cuando ocurre un incidente estos equipos asumen no solo el rol más técnico, sino que deben dar traslado y comunicar adecuadamente el ciberincidente que se haya producido. D. Si afectan a un servicio esencial y tiene peligrosidad alta, se comunica al INCIBE-CERT.; si el incidente afecta a los datos personales, se comunica a nivel interno a los distintos departamentos de la empresa (desde Recursos Humanos, Comité de Crisis, Seguros, o Comunicación y Relaciones Públicas, entre otros) y se transmite a la Agencia Española de Protección de Datos (AEPD). Otros retos que hay que afrontar en la gestión de estos centros CSIRT son la atracción y retención de **talento**; la disponibilidad de un **inventario de activos** completo, diverso y actualizado; la **compartición de información;** y el **excesivo volumen** de datos, alertas y consolas de seguridad.

Una de las principales conclusiones de este encuentro entre la comunidad de la Fundación ESYS con Carlos Gómez y Pedro Hernández ha sido que **los CSIRT, o Equipos de Respuesta de Incidencias Informáticas, se presentan como un elemento no solo estratégico, sino además crítico y esencial**, para garantizar la seguridad integral, la supervivencia de las organizaciones, así como su bienestar económico y social.