RESPUESTA DEL GOBIERNO

(184) PREGUNTA ESCRITA CONGRESO

184/14793 **06/07/2017** **41611**

AUTOR/A: GALOVART CARRERA, María Dolores (GS); MEIJÓN COUSELO, Guillermo Antonio (GS)

RESPUESTA:

El pasado 12 de mayo a las 9:25 de la mañana se empezaron a producir infecciones en sistemas y redes informáticos de varias empresas españolas, así como de otros países, por un virus informático conocido como Wannacry que realiza un cifrado de los archivos de los ordenadores que infecta, solicitando a continuación al afectado, mediante un mensaje en la pantalla del ordenador, un rescate de entre 300 dólares y 600 dólares en BitCoins para poder descifrarlos y, por tanto, poder recuperarlos. Este tipo de virus se clasifican como "Ransomware".

La primera empresa que se tiene constancia que sufrió la infección contactó a las 11:15 de la mañana con el equipo técnico del CERT de Seguridad e Industria (CERTSI), operado conjuntamente por el Instituto Nacional de Ciberseguridad (INCIBE) del Ministerio de Energía, Turismo y Agenda Digital y el Centro Nacional de Protección de Infraestructuras Críticas (CNPIC) del Ministerio del Interior, informando del problema e iniciando la colaboración para su contención, mitigación y recuperación.

Teniendo en cuenta la información analizada por el CERTSI hasta el momento, España actualmente ocuparía la posición 20 del ranking por países en número de infecciones acumuladas desde que se inició el ciberataque, cifrado en más de 180 países afectados, más de 360.000 infecciones.

Las empresas españolas estratégicas afectadas fueron una decena y pertenecen a diferentes sectores, entre ellos las Tecnologías de la Información y de la Comunicación (TIC), Energía, Sistema Financiero y Sector Público, pero en ninguna de estas empresas llegó a afectar a ningún sistema o red que dé soporte a servicios esenciales, a diferencia de otros países en los que se produjo un impacto en el Sector Financiero, Transporte o Salud.

No se tiene constancia por parte de INCIBE de la posible afectación a Ministerios y otras Administraciones Públicas españolas. Según la información disponible por INCIBE no se ha afectado a ningún servicio informático, redes o sistemas sensibles o críticos.

En cuanto al Protocolo específico en el ámbito del Ministerio de Energía, Turismo y Agenda Digital, se informa que el citado Ministerio cuenta con una Subsecretaría Técnica responsable de la seguridad del propio Departamento. Adicionalmente cuenta con INCIBE, cuyo dispositivo se activó como en el resto de ciberataques que se reciben diariamente. INCIBE dispone de mecanismos detectivos y preventivos mediante los cuales notifica a distintos agentes que pueden estar siendo blancos de un incidente de ciberseguridad o un ciberataque. Estos mecanismos incluyen servicios en modo 24x7 para atender y mitigar los impactos de estas amenazas. Adicionalmente, en situaciones especiales en los que se detecta o recibe notificación por algún agente de que está siendo afectado por un incidente se activa dicho Protocolo con un dispositivo especial que permite disponer de más recursos para atender el incidente, coordinarse con terceros agentes, aumentar las capacidades para el análisis de las amenazas, emisión de informes, notificaciones a posibles víctimas del ciberataque, atención a medios de comunicación, etc. Dichos dispositivos han funcionado tal y como están establecidos.

Por otra parte, se informa que el Consejo de Seguridad Nacional convocó tras el incidente cibernético una reunión extraordinaria en la cual los diferentes agentes que tomaron parte en el soporte, resolución y mitigación del ciberataque expusieron las diferentes acciones que llevaron a cabo durante la situación de crisis. En dicha reunión se debatieron los distintos puntos de mejora expuestos, entre los cuales se encuentra los procedimientos de coordinación, y la compartición de información relativa a los ciberataques.

Se han identificado diversas lecciones aprendidas derivadas del ataque, a fin de poder luchar contra este tipo de amenazas, entre las que destacan la necesidad de una mayor coordinación en el plano internacional y europeo y la necesidad de realizar un mayor esfuerzo por extender la cultura de ciberseguridad a todos los niveles que incluya más información y mejor comunicación sobre estas amenazas.

Finalmente, cabe señalar que la cuantía del impacto recibido por el ciberataque depende principalmente del tiempo de indisponibilidad de los sistemas y redes afectados, del tiempo de mitigación, del tiempo de recuperación de los procesos de negocio o actividades críticas, en definitiva, de la vuelta a la normalidad de la operativa de una organización, entidad o compañía afectada por el ciberataque. Por tanto, se indica que el cálculo de estos impactos y su monetización, si bien es una tarea factible y asequible en cuanto a su análisis y elaboración, son sólo conocidos por las empresas afectadas.

Madrid, 31 de octubre de 2017