650 empleados a casa y millones de euros en el aire: un nuevo ciberataque sacude al CSIC

Dos años después del devastador ciberataque sufrido por el CSIC, un centro adscrito a este organismo vuelve a caer. Un ’hackeo’ ha inutilizado los sistemas del INIA, que ha enviado a casa a sus más de 650 investigadores y administrativos

"No tenemos internet, no podemos acceder a ningún documento almacenado en red, nos tenemos que traer nuestro propio ordenador y conectarnos al 5G del móvil. Por no poder, no podemos ni imprimir. **Trabajar así es imposible**". Esta es la situación que viven desde hace dos semanas los más de 650 empleados del mayor organismo público de investigación agraria y alimentaria del país, el INIA (Instituto Nacional de Investigación y Tecnología Agraria y Alimentaria), adscrito al Consejo Superior de Investigaciones Científicas (CSIC) y dependiente del Ministerio de Ciencia, Tecnología e Innovación.

El pasado **12 de noviembre, prácticamente todos los sistemas internos del INIA dejaron de funcionar**. Lo que primero se atribuyó a una "avería", luego resultó ser un grave ciberataque del que no parece que vaya a haber una rápida recuperación. "Nos dicen que va para largo", explica resignado a este diario un investigador del centro.

Cuando llegaron a su oficina hace dos semanas, cientos de empleados del INIA se encontraron con una sorpresa: **no funcionaba nada**. Internet, aplicaciones corporativas, teléfonos... Cientos de proyectos de investigación, de repente, quedaban paralizados ante la imposibilidad de continuar el trabajo. "Nos enviaron un email y nos dijeron que era una avería y se solucionaría en un par de días", explica a El Confidencial un empleado. No ocurrió. Cuatro días después, el sábado 16 por la mañana, los empleados recibieron otro email. En este ya se reconocía que **el INIA había sido víctima de un ciberataque**. Pedían a todo aquel que pudiera que trabajase desde casa hasta nueva orden.

En ese mensaje, al que ha tenido acceso El Confidencial, se ordenaba "**no utilizar memorias USB o pendrive, discos duros, ninguna unidad externa de almacenamiento** y tampoco trabajar con ordenadores sin antivirus o con antivirus gratuitos. Así mismo, no se deberá conectar ninguna VPN externa", señalaba el email, dando pistas indirectas de cómo se podría haber producido el ataque.

Todo apunta a que el vector de entrada pudo haber sido un USB infectado. Eso habría desencadenado un ataque de ransomware, a través del cual se habrían secuestrado diversos sistemas del INIA. Se desconoce, sin embargo, el alcance exacto del ciberataque. **¿Se ha pedido rescate? ¿Ha habido robo de datos?** Si es así, ¿qué datos en concreto? ¿Hay datos personales afectados? **¿Se ha accedido a información científica sensible de investigaciones en curso?**

Este diario ha contactado con el CSIC para esclarecer estas y otras cuestiones. Al cierre de este artículo, **la única información recibida ha sido la siguiente:** "La respuesta se está gestionando a través del COCS (Centro de Operaciones de Ciberseguridad) de la Administración General del Estado". El COCS es un organismo dependiente de la Secretaría de Estado de Digitalización e Inteligencia Artificial (SEDIA), creado en 2022. **Ha costado 51 millones de euros**. Indra y Telefónica fueron los adjudicatarios del contrato (sin concurso público) para su implantación.

El INIA es uno de los mayores centros del CSIC. En él se realizan **investigaciones estratégicas centradas en los ámbitos medioambientales y agrícolas**. Allí también fue donde se probaron las vacunas españolas contra la COVID-19 o donde se creó el primer cordero modificado genéticamente en España. Además, se hacen trabajos clave para evitar la desaparición de los animales en peligro de extinción.

El Confidencial ha contactado con media docena de empleados del INIA que aseguran no haber recibido tampoco más detalles sobre lo ocurrido. "**Estamos un poco abandonados**. Nos han dicho que tienen que revisar uno a uno los ordenadores, así que podríamos estar parados varias semanas, incluso meses. Eso significa perder un montón de recursos, investigaciones paralizadas, tener que dar explicaciones a socios europeos... Si esto fuera una empresa privada, supondría la quiebra. Pero como esto es un centro científico público, nadie se entera", explica uno de los investigadores consultados, que pide mantener el anonimato.

El ciberataque pone en riesgo millones de euros en proyectos con empresas y centros de investigación de medio mundo. Con un presupuesto anual que ronda los 80 millones de euros, el INIA es el centro de referencia en nuestro país para la investigación en materia agrícola, ganadera, alimentaria, forestal y medioambiental. El pasado octubre, por ejemplo, la Fundación Bill & Melinda Gates le otorgó 4,5 millones de euros para el desarrollo de cereales más resistentes y productivos que se nutran con el nitrógeno del aire. El proyecto, formado por un consorcio internacional de centros de Europa, EEUU y Argentina, liderado por el investigador español Luis Rubio, es uno de los que puede verse afectado por el ciberataque, tanto en retrasos como en un posible robo de información.

"Estamos ante un incidente que debería catalogarse de seguridad nacional. Hablamos de un centro adscrito al CSIC que maneja muchas patentes y propiedad intelectual sobre innovaciones que podrían interesar a otros estados y ciberdelincuentes. En España el CSIC sufrió un hackeo masivo en el 2022. Debía haber servido de aviso, pero no se ha hecho prácticamente nada", explica a este diario otro investigador del INIA consultado.

El 16 de julio de 2022, el grupo de ciberdelincuentes **Vice Society** logró colarse hasta la cocina en los sistemas del CSIC, inutilizándolos durante casi dos meses y robando y publicando 41 gigas de información sensible (incluidos datos personales). En su momento, el **CSIC llegó a señalar a Rusia**, pese a que no está probada la relación de Vice Society con el Kremlin. Empleados del centro consultados aseguran que la parálisis del INIA tras el ciberataque es la prueba de que no se han tomado las medidas necesarias para evitar que lo ocurrido en el 2022 vuelva a suceder.

"Te doy un ejemplo: no existe un sistema de back-up centralizado. La normativa que tenemos es de 2017 y dice que cada investigador es responsable de hacer sus propios back-ups a cargo del presupuesto de cada proyecto. Es decir, tienes a biólogos o filósofos, que no saben nada de tecnología, ni tienen que saber, obligados a realizar por su cuenta copias constantes de terabytes de datos. Es un sinsentido", explican. Otra fuente consultada asegura que, pese a haberse anunciado cursos de concienciación y ciberseguridad a los más de 13.000 empleados del CSIC, los supuestos cursos en realidad se quedaron en presentaciones colgadas en una intranet disponibles para aquel que las quisiera consultar.

Tampoco se está cumpliendo de momento otra de las medidas estrellas del CSIC prometidas a raíz del ciberataque de 2022: **la certificación de buena parte de los 149 centros adscritos asegurando el cumplimiento del Esquema Nacional de Seguridad**. Dos años después, solo 6 han conseguido dicha certificación. "Por no cumplir, no cumplimos con algo tan básico como tener doble factor de autenticación activado", señala uno de los empleados del INIA.

La Comisión Europea avisó el pasado mayo de la necesidad de reforzar los centros de investigación por el creciente número de ataques que buscan robar información sensible y patentes. En su informe, advertía: "Los investigadores e innovadores establecidos en la Unión pueden ser objeto de acciones destinadas a adquirir conocimientos y tecnología de vanguardia, **en ocasiones utilizando métodos engañosos y encubiertos, o directamente mediante el robo o la coacción**". Es exactamente lo que le acaba de ocurrir, por segunda vez en dos años, al CSIC. Ahora le toca protegerse (de verdad).

Fuente: https://www.elconfidencial.com

LINK DE LA NOTICIA