businessinsider.es

Así se vivió el ciberataque al SEPE desde dentro: 19.000 horas extra

Alberto R. Aguiar

5-7 minutos

Casi 9 meses después, **se conocen más detalles del ciberataque que afectó al Servicio Público de Empleo Estatal (SEPE).** La encargada de profundizar en el incidente ha sido, además, una de sus protagonistas: Gema Paz, jefa del Área de Arquitectura, Calidad, Seguridad y Desarrollos Transversales del organismo.

El 9 de marzo de 2021 el SEPE estuvo bajo ataque. Las primeras informaciones se dieron a conocer a media mañana de aquel día, y por la tarde ya se pudo confirmar que se trataba de un incidente relacionado con un *ransomware*. En concreto, fue Ryuk el que comenzó a cifrar los archivos del organismo.

La gravedad del incidente fue notable. Los colectivos que operan este tipo de códigos maliciosos han desarrollado sus técnicas, y ya no se limitan a cifrar los archivos de sus víctimas para exigir después un rescate. Las bandas de ciberdelincuentes ahora también roban

parte de esos datos para chantajear a su objetivo.

El SEPE regresa a la normalidad y la ministra de Trabajo pide "altura de miras" para dejar de politizar el ciberataque que provocó un apagón informático durante días

Por ello, muchos medios elucubraron entonces si los datos de los usuarios estaban en peligro. "Se dijeron en prensa **muchas mentiras"**, aseguró Paz sobre las tablas de las XXV Jornadas del CCN-CERT, el Centro Criptológico Nacional, organismo de ciberseguridad dependiente de la agencia de inteligencia española, el CNI.

"Los datos de los ciudadanos estuvieron en todo momento limpios". **Nunca estuvieron en peligro, zanjó.**

Más de 19.000 horas extras

Pero si de algo sirvió la charla que Gema Paz dio en estas Jornadas fue para poder imaginar cómo de intenso es el trabajo de respuesta ante un incidente de esta magnitud. Hace unos meses, el responsable de seguridad de una universidad pública que también sufrió un ataque lo lamentaba así: "En un atentado, la policía acordona la zona y toma el control, aquí no ha sido así".

El incidente que registró el SEPE en marzo de este año significó, para los técnicos del organismo, **más de 19.000 horas extras.** Se tuvo que reforzar el personal para reinstalar hasta 25 puestos de trabajo en la oficina. Paz

recuerda que aquellos momentos llegaron a suponer un *shock* para muchos de sus compañeros: el ataque fue en marzo de este año, en plena pandemia.

Eso significaba que muchos de ellos llevaban meses trabajando en remoto desde casa. De la noche a la mañana se tuvieron que ver obligados a **acudir a la oficina al completo.** El trasiego fue tal que muchos de ellos tuvieron que hacerse tests de antígenos diarios para evitar contagios. La propia jefa de Seguridad del SEPE recuerda desvelarse de madrugada pensando en el trabajo.

Varias mafias de ransomware cesan su actividad, pero sus estragos continúan: "Da igual la cantidad de recursos que se inviertan, sus cifrados no se pueden romper"

El personal estuvo movilizado **20 horas al día durante 3 semanas, los 7 días de cada una de ellas.** De hecho, los técnicos continuaron movilizados en Semana Santa, que se celebró apenas unas semanas después de que se detectase el incidente. Un incidente que los protocolos de ciberseguridad del SEPE llegó a detectar, pero no logró frenar a tiempo.

El atacante desplegó y ejecutó Ryuk **"en el mayor número de equipos posibles"**, aunque solo afectaron los sistemas Windows, y no los sistemas CORE del SEPE, como Solaris o Linux. "Desde el primer momento el pago de las prestaciones y la estadística de empleo estaban asegurados", reivindica Paz.

Fue el 9 de marzo cuando se detectó el ataque. Dos días después, para el 11, los técnicos del organismo lograron reabrir el portal web. El 15 se reabrió el sistema de cita previa, y el 17 se garantizó la interoperabilidad entre el SEPE y la Gerencia de Informática de la Seguridad Social, algo esencial en su servicio.

Para el 20 de abril **el incidente se dio por resuelto**, a pesar de que todavía quedaba trabajo por hacer, según confirma la propia Gema Paz.

Qué se aprendió

Al término de su presentación Gema Paz señaló que, entre las principales conclusiones a las que ha llegado el organismo, una de ellas es la necesidad de contar con sistemas de monitoreo las 24 horas los 7 días de la semana. Fruto de esa idea, el SEPE está trabajando en un acuerdo de colaboración con el CCN-CERT y con la Secretaría General de Administración Digital.

La finalidad de ese nuevo convenio será constituir **un SOC o Centro Operativo de Ciberseguridad para el SEPE.**

Además, la propia Paz señaló que especialistas informáticos en toda su Subdirección hay unos 70, aunque **especializados en ciberseguridad "no tantos".** A la misma conclusión llegaron en su momento sindicatos y colegios profesionales de técnicos informáticos, que consideraron en declaraciones a este medio que ataques

como el del SEPE eran, como poco, más fácilmente mitigables.

Los ciberataques a la administración se disparan tras el golpe al SEPE: un organismo de Hacienda alerta de que lo están suplantando con correos maliciosos

Falta inversión, adujeron entonces, y falta regulación. "Esa falta de regulación de la profesión puede provocar ciberataques como este y peores cosas". "Sin esa regulación, los profesionales informáticos no podemos trabajar con la libertad y las garantías suficientes siendo apolíticos, neutrales y centrándonos en nuestro trabajo".

Lo que sobre todo se aprendió, rememoraba Paz en las Jornadas del CCN-CERT, es que cuando el sistema cae "no lo levanta una máquina". **"Lo levantan humanos".** Un equipo de profesionales que dedicó horas y jornadas maratonianas para hacer frente a una grave crisis digital.