

# El Confidencial

EL DIARIO DE LOS LECTORES INFLUYENTES

## El Corte Inglés, Santander, Renfe, Correos... ensayan la respuesta a un ciberataque crítico

### Quince grandes empresas simulan cómo sobrevivir a una intrusión informática que bloquee sus sistemas, con ayuda del CNI y el Departamento de Seguridad Nacional

El 'hacking' sufrido por Telefónica hace unos meses ha puesto en alerta a todas las grandes empresas españolas. Para evitar ser víctimas de ciberataques similares, quince de ellas –pertenecientes a todos los sectores- se han sometido a una evaluación para comprobar cómo reaccionarían ante un incidente crítico de grandes proporciones. Ha colaborado el CNI.



Quince empresas españolas ponen a prueba sus sistemas de seguridad contra ciberataques.

19/07/2017 01:00 [http://www.elconfidencialdigital.com/seguridad/Corte-Ingles-Santander-Renfe-Correos\\_o\\_2967903193.html](http://www.elconfidencialdigital.com/seguridad/Corte-Ingles-Santander-Renfe-Correos_o_2967903193.html)

El viernes 12 de mayo, **Telefónica** sufrió el que ya es considerado como el peor **ciberataque** de la historia de España. O al menos el más mediático. El virus **WannaCry**, un 'ransomware' que secuestra virtualmente ordenadores y pide un rescate a cambio de liberarlos, afectó a toda su sede central de Las Tablas, en Madrid.

El balance final de ese ataque fueron miles de empresas paralizadas en todo el mundo, incluido el **sistema sanitario del Reino Unido**.

Tras 'WannaCry' llegaron otros como '**Petya**', mucho más sofisticado, que atacó la pasada semana a los servidores informáticos de **ochenta multinacionales en todo el mundo**. En España afectó a la delegación de la naviera danesa APM, que se vio obligada a interrumpir su actividad en el puerto de Barcelona.

El aumento exponencial de las **ciberamenazas** registrado en los últimos años ha llevado a las empresas a reevaluar de forma constante sus **sistemas y protocolos de seguridad** frente a la infección de virus y las intrusiones de hackers en sus servidores.

## ***Quince grandes empresas a examen***

Uno de los últimos movimientos en este sentido ha tenido como protagonistas a **quince destacadas empresas españolas**, que han participado en un **gran simulacro de ataque informático** crítico.

Se trata de **Banco Santander, Renfe, El Corte Inglés, Acciona, Ferrovial, Abanca, Bankinter, Abertis** –división de Infraestructuras y división de Autopistas-, **Cortefiel, Correos, Mediaset, Inversis, Cepsa y Sanitas**. Una muestra representativa de casi todos los sectores de la economía española.

El ejercicio, dirigido y planteado por el organismo de ciberseguridad **ISMS Fórum**, contó con la participación del **Centro Criptológico Nacional** (dependiente del CNI), el **Departamento de Seguridad Nacional** (dependiente de Presidencia del Gobierno), el **INCIBE** (Instituto Nacional de Ciberseguridad de España), y el **Centro Nacional de Protección de Infraestructuras Críticas**.

## ***Intrusiones, 'secuestros'...***

El simulacro de ciberataque de nivel crítico puso a prueba la reacción de todas estas empresas ante sucesos muy semejantes a los que vivió Telefónica durante la tarde del pasado 12 de mayo.

Sin embargo, en este caso –tal y como explican a El Confidencial Digital fuentes de algunas de las empresas participantes- se pusieron en práctica muchas otras situaciones, como **penetraciones en servidores para extraer información** y ataques de **Denegación de Servicio** o 'DDoS'.

Sólo los departamentos de seguridad informática de estas empresas estaban al corriente de este gran ejercicio, que se realizó **sin conocimiento previo del tipo de amenaza por parte de los equipos de respuesta**. De esta manera, se obligó a las empresas a poner en práctica los mismos procedimientos de coordinación que aplicarían ante un caso real.

## ***Conclusiones: "Muy bien" pero no "excelente"***

Al finalizar el ejercicio, los organizadores han evaluado la **reacción y respuesta de las empresas** ante el ciberataque, teniendo en cuenta: el tiempo de respuesta al incidente y las comunicaciones utilizadas para su resolución.

La nota final obtenida por estas quince grandes empresas ha sido un **"muy bueno"**, es decir, un tres en una escala de cuatro niveles en el que el nivel máximo es **"excelente"**. Por lo que aún queda margen de mejora.