36 **Salud.** Amancio Ortega dona un mamógrafo al Hospital Comarcal del Pallars

44 **Certamen.** El Som Cinema, con un film sobre la anorexia con pacientes reales

ICS LLEIDA

TECNOLOGÍA FRAUDES

Blindaje contra los 'hackers'

Tres de cada diez empresas sufren ataques informáticos para conseguir información sensible y dinero de forma fraudulenta || Los expertos abogan por un plan de contención, sobre todo en pymes

M. CABELLO

| LLEIDA | Los ataques informáticos para 'secuestrar' datos y enriquecerse de forma fraudulenta son una práctica cada vez más habitual que, según el último informe de la compañía de ciberseguridad Bitdefender, ya afecta a tres de cada diez empresas en España. Las pymes son las más vulnerables a estos delitos, que pueden suponer un coste más allá de los 70.000 euros. Sin ir más lejos, hace apenas unas semanas se propagó un virus informático que afectó a varios ayuntamientos leridanos y a la Diputación y que, mediante un correo electrónico fraudulento que se hacía pasar por estas instituciones, pretendía recabar información sensible de los usuarios, como sus datos bancarios, contraseñas y su actividad en internet. En la mayoría de casos, se trata de un *malware*, un programa malicioso que infecta el sistema, y de mensajes que suplantan la identidad de terceras personas o compañías para conseguir dinero. Los expertos en ciberseguridad apuestan por un plan de contención que evite estos *hackeos*, pues "recuperarse de estos problemas con garantías es una labor muy difícil o prácticamente imposible para una empresa, especialmente si no está asesorada por especialistas", explica Laura Palacín, líder del departamento de 'ciber riesgo' de la aseguradora de Mollerussa Asur Brok. "Este tipo de delitos son cada vez más frecuentes y sofisticados", explica Palacín, mientras destaca que el tiempo medio que necesita una pyme para darse cuenta de que ha sido pirateada puede llegar a un año. "En algunos casos se trata de programas espía que infectan el ordenador y durante meses observan la actividad de la empresa hasta conseguir la información que les interesa a los hackers". Más allá de ser un problema puntual, el 80% de las compañías que han sufrido una violación de las medidas de seguridad vuelven a ser víctimas otro ataque.

RIESGO

En la mayoría de casos se trata de un 'malware' o mensajes que suplantan la identidad

EFE

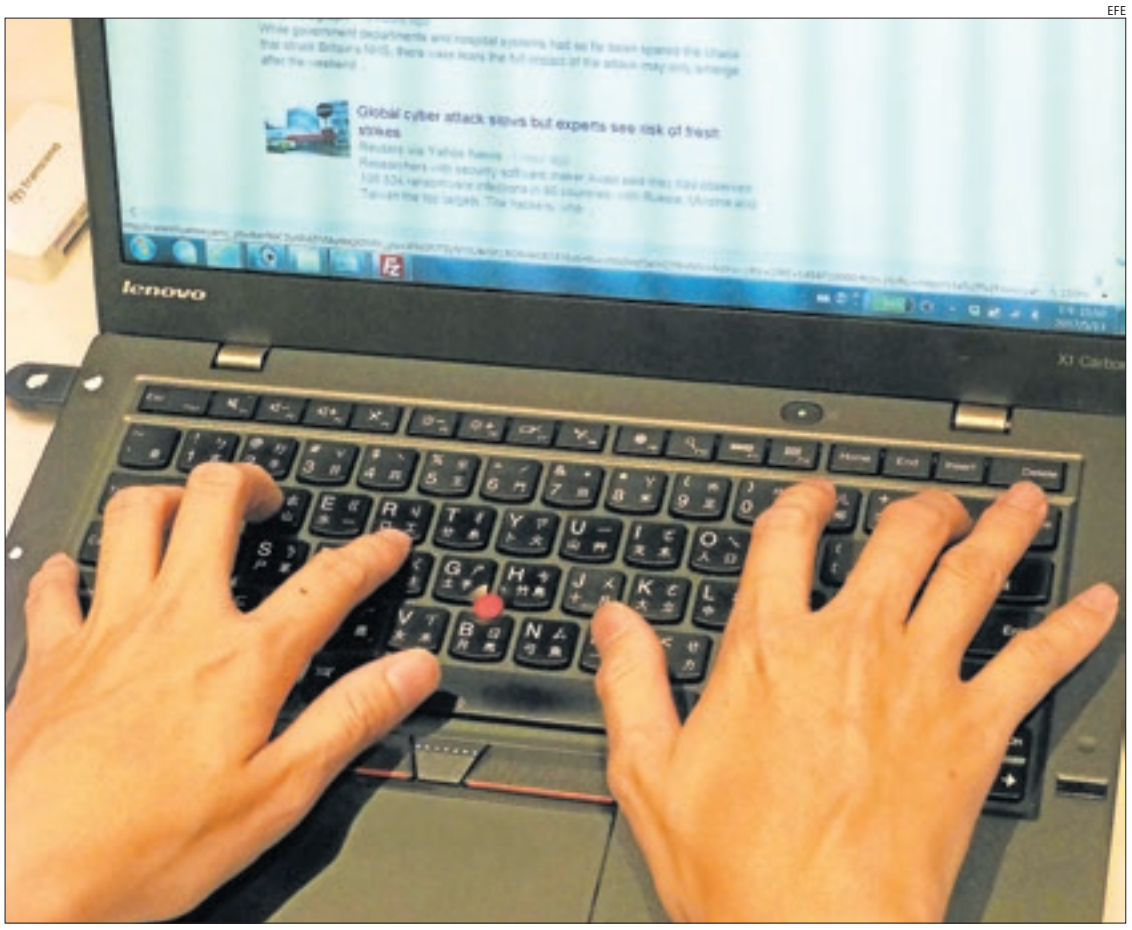

Imagen de archivo de un usuario navegando en internet.

LAS CLAVES

Más ciberdelincuencia

Las causas abiertas en los juzgados leridanos por delitos informáticos se han disparado en el último año. Según la última Memoria de la Fiscalía, en 2018 llegaron a los juzgados un total de 126 denuncias por parte de las fuerzas de seguridad por delitos informáticos de diferente índole, la mayoría de ellos contra el patrimonio. Esto supone un incremento de cerca del 58% respecto a las causas judiciales abiertas por este tipo de delincuencia en 2017.

Ataques a ayuntamientos

Un virus informático afectó hace unas semanas a varios ayuntamientos de Lleida y a la Diputación. Hasta ellos llegaron correos electrónicos cuya procedencia es aparentemente de un consistorio de la demarcación, pero eran en realidad de una falsificación y suplantación de la identidad de estos para conseguir información sensible de los usuarios.

ENTREVISTA

«Los ciberataques son cada vez más sofisticados»

Laura Palacín
EXPERTA EN CIBERSEGURIDAD DE ASUR BROK

MAITE MONNÉ

Mucha gente cree que los ataques informáticos son problemas que solo afectan a las grandes corporaciones.
Nada más lejos de la realidad. Los 'hackers' atacan indistintamente a todo tipo de empresas, pero las pymes son las más vulnerables porque no tienen grandes recursos para protegerse. Ahora la sociedad empieza a estar más sensibilizada y nos estamos dando cuenta de que 'esto también me puede pasar a mí', aunque todavía hay muchas empresas sin medidas específicas.

¿Qué riesgos conllevan los delitos cibernéticos?
Cada vez son más sofisticados. Normalmente se trata de programas maliciosos que quieren recabar información sensible y que, además de los datos de las empresas, pueden comprometer la privacidad de terceras personas, como los clientes. En otros casos, el 'hacker' suplanta la identidad de otras empresas o instituciones para conseguir dinero. El coste que puede suponer para una empresa esta brecha en la seguridad es muy difícil de calcular, pues algunos virus incluso pueden frenar la producción. No solo acarrea problemas informáticos, también legales (posibles multas por responsabilidad civil) y de reputación de la empresa.

¿Cómo se puede solucionar este problema?
La gran mayoría de empresas no están preparadas para hacer frente al incremento exponencial de los delitos informáticos, que habitualmente son consecuencia de errores humanos debido a la transmisión de datos de forma involuntaria o la pérdida de un dispositivo móvil. Es necesario un plan de contención que, además de contar con el asesoramiento de expertos, tenga en cuenta la formación de los trabajadores para reducir al mínimo el 'ciber riesgo'.

¿Cuánto tiempo puede pasar hasta que se detecta la brecha en la seguridad informática?
Pueden pasar meses. Los 'hackers' se instalan en el sistema y observan las operaciones hasta que consiguen la información que les interesa. Cuando te das cuenta ya es tarde.