Tirada: 30.782
Difusión: 21.772
(O.J.D)
Audiencia: 76.202
Ref: 9184670

CincoDías

Economico Diaria
Economia
2 ª Edición 15/05/2017

Superficie: 1.011 cm²
Ocupación: 89.7%
Valor: 11.389,19 €
Página: 5

1 / 1

El Foco

El ataque 'ransomware' y las alarmas

Este tipo de crisis diferencia a las empresas que se toman en serio su seguridad

ENRIQUE DANS

Profesor de Innovación en IE Business School

La pasada semana estuvo marcada por un alarmismo desenfrenado en torno al *ransomware*, un tipo de virus cuya denominación correcta es la de extorsión criptoviral, ideado en 1996 en la Universidad de Columbia. Estos virus responden a un esquema sencillo: tras infectar al usuario, generalmente cuando hace clic en un enlace, cifran el disco duro y generan una alerta que demanda un pago supuestamente a cambio de la clave que permite descifrarlo y volver a acceder a la información.

El mecanismo de difusión de este tipo de virus suele ser aleatorio: enlaces en mensajes de *spam* o en páginas web.

Sembrar y esperar. Nada de sofisticado en ello: ni conspiración para atacar a compañías o países concretos, ni ataque dirigido contra nadie, ni mucho menos ciberguerra. Pura y simple casualidad. Los creadores del virus, que aprovechaba una vulnerabilidad que Microsoft desarrolló para la NSA norteamericana, estarán sorprendidos con el eco mediático de su creación.

Si alguien puede sufrir con este tema es, precisamente, Microsoft. Su política de actualizaciones, su vocación por dejar fuera de ella a los usuarios que no pagan o utilizan software antiguo –algo que muchos definen como otra forma de *ransomware*– y el contexto completo de su relación con esta vulnerabilidad debería llevar a que algunos se replanteasen la conveniencia de vivir en un monocultivo que ha generado una indudable situación de riesgo para muchos. A lo largo del tiempo, Microsoft se ha convertido no en el único, pero sí en el más claro responsable de los problemas de muchas compañías. Obviamente, el resto de la responsabilidad recae en esas propias compañías y en la necesidad de entender el contexto en el que desarrollan algunas de sus actividades más críticas.

Ser infectado por un virus de este tipo no es deshonroso o infamante: supone, como mucho, que no hemos sido completamente diligentes para aplicar las actualizaciones correspondientes, pero eso, en entornos corporativos, puede responder a muchas cosas, no solo a la desidia. Muchas veces es más recomendable esperar y verificar un parche antes de ponerlo en producción, que lanzarse a actualizar todo lo que surge.

Lo importante, en estos casos, es que los riesgos estén bajo control. La seguridad total no existe, y lo que tenemos que pedir a un departamento de seguridad es que tenga los planes preparados para eventualidades que tengan un cierto nivel de probabilidad.

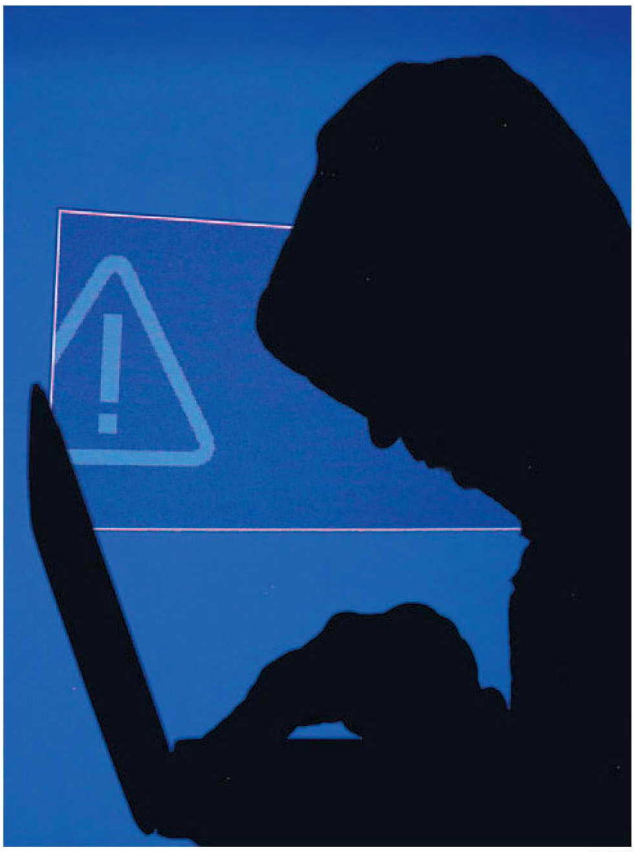
Dado que la seguridad total no existe, tenemos que invertir para estar preparados para todos los escenarios que tengan una cierta probabilidad y cuantificar el riesgo que puede llegar a suponer no estarlo. En caso de ataque de un virus como este, todo el problema está en aislar los ordenadores infectados, detener el proceso de infección a través de la red corporativa, borrar esas máquinas y recuperar sus contenidos desde la copia de seguridad. Para quien está adecuadamente preparado, simplemente molestias menores y "un día más en la oficina".

> **La seguridad total no existe, y lo que tenemos que pedir a un departamento de seguridad es que tenga planes preparados**

Y ahí es, precisamente, donde reside la cuestión: sufrir una infección no es, en realidad, nada de lo que nuestro departamento de seguridad sea responsable: simplemente, es un evento con una cierta probabilidad, e intentar eliminarla sería demasiado costoso en términos de restricciones que sería preciso imponer a los usuarios.

Sin embargo, si sufrimos una infección y nuestro departamento de seguridad, teniendo los medios adecuados para ello, no tenía prevista esa eventualidad, no sabe cómo reaccionar o no tiene una rutina adecuada de copias de seguridad, eso sí es un problema que cae íntegramente bajo su responsabilidad, y deberían rodar cabezas.

Este tipo de crisis diferencia a las empresas que se toman en serio su seguridad de aquellas que no lo hacen: las que hacen las cosas bien, actúan con celeridad y transparencia, no dramatizan y evitan una disrupción excesiva de los procesos de negocio. En una empresa que no haya hecho sus deberes, en cambio, una infección de ese tipo puede hacer que se pierda información importante, que se alteren flujos productivos o incluso que haya quien tenga la tentación de pagar el rescate para intentar solucionar el tema. Un pago que no garantiza nada: no son pocos los casos en los que, tras hacer ese pago, los delincuentes simplemente no han vuelto a contactar.



REUTERS

Hacer dramas, repicar las campanas como si hubiese una ciberguerra o apuntar con el dedo a la compañía que se ve implicada en un incidente de esta naturaleza es, simplemente, un ejercicio de mal periodismo, de sensacionalismo y de irresponsabilidad.

Hablamos de un suceso aleatorio: una compañía más grande tiene, matemáticamente, más probabilidades de sufrirlo. No se puede juzgar a las compañías por haber sido infectadas: hay que hacerlo en función de cómo reaccionan cuando lo son y de hasta qué punto son capaces de poner bajo control esa eventualidad.

Debemos entender este tipo de cuestiones como algo perfectamente normal: con el tiempo y el desarrollo de internet, los delincuentes se adaptan al nuevo entorno y desarrollan formas más imaginativas de delincuencia, al tiempo que las policías también se esmeran más en capturarlos y los responsables de seguridad en ponderar adecuadamente sus riesgos. Desgraciadamente, ni el *ransomware* ni otras amenazas van a desaparecer: son fenómenos que forman parte del entorno en el que vivimos. La tecnología genera escenarios con infinitas ventajas, pero nada está exento de riesgos. Total normalidad. Menos dramas, menos histeria, más aprovechar para educar al público y, sobre todo, más seriedad. Seguro que así nos irá mejor a todos.