Expansión

economía digital

COMPAÑIAS ◆ PROTAGONISTAS ◆ INNOVACIÓN

¿Quién es el responsable de un ciberataque?

Un nuevo ciberataque infecta a decenas de grandes empresas de todo el mundo

| DREAMSTIME | EXPANSIÓN

Actualizado: 29/06/2017 00:17 horas

La parte positiva de sufrir un ciberataque, si la hay, es que nos ayuda a ser conscientes de lo vulnerables que somos. A partir de allí, comenzamos a plantearnos si de verdad estamos haciendo todo lo necesario para proteger nuestros negocios convenientemente, pero también si podemos seguir confiando en los proveedores que nos facilitan sus soluciones tecnológicas o sus servicios de telecomunicaciones.

Una de las cosas que nos han enseñado los últimos incidentes de seguridad, como WannaCry o el ataque global de *ransomware* de esta semana, es que para causar daño a través de un ataque no hace falta centrarse en el Centro de Proceso de Datos (CPD), en el que se guarda la información más sensible del negocio y al que seguramente se destina gran parte del presupuesto de seguridad. **Dirigiéndose de forma indiscriminada a activos menos estratégicos, pero mucho más numerosos, también es posible causar un gran perjuicio**.

Por otra parte, este tipo de incidentes abren también un debate sobre la cuota de responsabilidad que debe asumir cada parte implicada, y sobre qué medidas tomar para evitar similares ataques en el futuro. Para ello, **habría que preguntarse quién ha abierto la puerta al ciberdelincuente**. ¿Ha sido el usuario con su software desactualizado, el fabricante del sistema operativo al haberlo comercializado con una vulnerabilidad o el operador de la red al permitir el paso al *hacker*?

Naturalmente, el primer responsable es quien comete el delito. En este caso, no nos queda más remedio que confiar en los cuerpos y fuerzas de seguridad para que lo identifiquen y lo paren. Pero tal y como están las cosas últimamente quizá habría que empezar a valorar tanto los medios disponibles como los resultados alcanzados por los responsables de investigar y prevenir ataques en el ciberespacio. Es posible que en este punto sea necesario hacer algún cambio con urgencia.

En segundo lugar aparecen los desarrolladores de software y sus actuales modelos de negocio. Si el *hacker* ha sido capaz de aprovechar una vulnerabilidad de un sistema operativo para introducirse en un dispositivo, es porque ese software se comercializó con un defecto. Es cierto que los fabricantes de software están continuamente publicando parches para evitar este tipo de problemas, pero también es cierto que en un determinado momento deciden dejar de hacerlo para las versiones de sus productos que consideran obsoletas, lo que aumenta la vulnerabilidad para los clientes que no renuevan su software antiguo.

Aparecen después los propietarios de la red de telecomunicaciones, que es un medio que podrían utilizar los *hackers* para llegar hasta sus víctimas, es decir, los clientes del operador. **En un mundo en el que todo está conectado, parece lógico exigir a los operadores de telecomunicaciones la implantación de todas las medidas de seguridad posibles para evitar el uso malintencionado de su infraestructura y el daño que este mal uso pueda causar a terceros**.

En esta situación, habría que preguntar a los operadores si han adjudicado la responsabilidad de la seguridad de sus redes y sistemas a una persona concreta en su organización, con apoyo desde la más alta dirección y dotado de los medios necesarios para abordar los aspectos relativos a la seguridad de forma integral. Y

OTRAS NOTICIAS DE INTERÉS

- Vestager, la comisaria que hace temblar a Silicon Valley
- Lindsey Argalas, nueva responsable de Tecnología Digital e Innovación de Banco Santander
- "Telefónica no hará grandes compras, ya es una de las mayores del mundo"
- "Lenovo puede duplicar su tamaño gracias a los móviles"
- Sin seguridad no habrá negocio

LO MÁS LEÍDO

1. El nuevo edificio de Apple está hecho para personas mayores
2. La cultura digital de Ferrovial
3. Microsoft despedirá a 3.000 trabajadores en todo el mundo
4. Las 'fintech' recaudan 13.600 millones de dólares de inversión
5. Baidu ofrece software de código libre para conseguir información de los usuarios

cabría preguntarse también si los operadores, vez de fiarse ciegamente de los proveedores de tecnología y soluciones, revisan de forma proactiva sus configuraciones y realizan pruebas exhaustivas de sus sistemas para no solo parar, sino también prevenir posibles ataques.

Finalmente, no hay que olvidarse del regulador. **La CMT, en el caso de España, debería poner a la seguridad en el centro de sus prioridades**. Quizá sea necesario imponer a los *players* de este sector la adopción de una serie de medidas que garanticen un nivel óptimo de seguridad en las redes de telecomunicaciones, a fin de proteger al máximo los negocios y los datos de empresas y usuarios. ¿Si casi todo en la sociedad está regulado, como es posible que en un mundo cada vez más conectado y con alta dependencia de las infraestructuras de telecomunicaciones el área de seguridad de redes aún no lo esté?

> ¿Si casi todo en la sociedad está regulado, como es posible que en un mundo cada vez más conectado y con alta dependencia de las infraestructuras de telecomunicaciones el área de seguridad de redes aún no lo esté?"

Por la táctica empleada en recientes ataques masivos, como el caso de WannaCry, estos incidentes han supuesto un antes y un después en el ámbito de seguridad. **Ya no se trata solo de proteger los activos propios, sino de evitar los daños que estos ataques pueden causar a terceros**. Si es verdad eso de que ahora el cliente se sitúa en el centro de todas las estrategias, sería conveniente que las partes implicadas comenzaran a trabajar de forma coordinada y actuaran con la responsabilidad que de ellos se espera.

Si no lo hacen, a lo mejor ese cliente, del que también decimos que es más exigente y está más informado que nunca, comenzará a pedir responsabilidades de una forma también más contundente.

Por Miguel Ángel García Matatoros. Director General en Blue Telecom Consulting