El turismo, en el punto de mira de los ciberataques

RIESGOS Es uno de los tres sectores más afectados, tras la administración pública y la banca.

N. Serrano. Madrid

La ciberseguridad parece ser algo más que una tendencia pasajera. El proceso de transformación digital que están viviendo las compañías, ya sea por motivación propia u obligada por las necesidades del mercado, ha provocado un incremento del uso de la tecnología en cualquier entorno al que se haga referencia. Ya en el World Economic Forum de Davos del año 2014, el informe *Riesgos globales* planteaba las amenazas de ciberseguridad como uno de los cinco principales riesgos a tener en cuenta, en base a la probabilidad de materialización y a su impacto potencial en las organizaciones. Es por ello que el informe *Expectativas 2017* de Deloitte, presentado ayer, hace especial hincapié en este fenómeno.

El sector público y el financiero son las dos principales industrias para el cibercrimen a nivel global. Pero, ¿sabe cuál es la tercera? El turismo entra en este dudoso podio como uno de los sectores en el punto de mira. El riesgo propio de esta industria se incrementa en su cadena de valor, en la que aparecen negocios de terceros que completan la propuesta, como explican Fernando Pons, socio de Travel, Hospitality, Leisure & Transport de Deloitte, y Antonio García Estopa, gerente IT de Risk Advisory, en el citado informe.

Las principales amenazas a las que se enfrenta el sector son: el robo de información, un bien preciado en el mercado negro donde es monetizada hasta la mínima expresión; los ataques que provocan las disrupción del negocio y no permiten a las compañías poder prestar los servicios; y los ataques que afectan a la calidad del servicio y que degradan la experiencia del usuario.

Más allá de la metodología empleada, el cibercrimen trae consigo una serie de consecuencias para las organizaciones, como la pérdida de confianza de los clientes, el daño a la reputación y a la marca, los riesgos legales y... las pérdidas económicas.

Dreamstime

Los ciberataques también impactan en la industria del turismo.

450 mill.

En 2016, la UE hizo público un comunicado sobre el establecimiento de una estrategia público-privada en ciberseguridad, con una inversión de 450 millones de euros.

89%

El 89% de los ataques se produce por motivos financieros y de espionaje. Esto pone de manifiesto que cualquier información es susceptible de convertirse en monetizable.

Top 5

Ya en el World Economic Forum de Davos de 2014, el informe 'Riesgos globales' planteaba la ciberseguridad como uno de los cinco principales riesgos a tener en cuenta.

Como señalan desde Deloitte, los objetivos que persiguen estos ataques cibernéticos suelen ser fundamentalmente económicos, ya que el 89% tiene de base motivos financieros y de espionaje.

¿Qué pueden hacer las compañías turísticas para protegerse? Lo primero sería profundizar en el modelo de funcionamiento del cibercrimen, que muestra que el atacante no trabaja de forma arbitraria y que su técnica es elaborada y dirigida. Además su comportamiento se puede enfocar de tres maneras. En primer lugar, focalizarse en un objetivo concreto. Son los más difíciles de detectar y se realizan durante un amplio periodo de tiempo antes de que se identifique. Tienen un impacto muy elevado, pero son los menos comunes porque su complejidad conlleva que su probabilidad de ejecución disminuya.

En segundo lugar estarían los ataques que tienen a un sector concreto en el disparadero. Estas ofensivas suelen tener una gran afectación porque el nivel de personalización, aunque no muy depurado, permite que la probabilidad de éxito sea más alta.

Los expertos sitúan en tercer lugar el objetivo global, es decir, un ataque masivo indistintamente del sector y cuya única consideración es llegar al máximo número de objetivos. Su nivel de sofisticación es muy bajo, al igual que el coste de su preparación, de modo que es el principal al que se enfrentan los directivos. Sí, los directivos, porque la seguridad en Internet se ha convertido en uno de los protagonistas de la agenda del CEO.

Seis soluciones frente a los ataques en Internet

Seguridad en los datos

No reunir información personal que no sea necesaria y limitar

Control de acceso

Restringir los accesos de datos a los empleados limitando el

Segmentación de la red

Monitorización de la Red para detectar accesos no autorizados y

Cuidado con el acceso remoto

Según el informe, hay que limitar los accesos para clientes y

Exigir medidas de seguridad

Exigir medidas de seguridad a proveedores de

En la agenda del líder

Sin medidas organizativas no tienen sentido las soluciones