LITORALPRESS

Fecha: 28-06-2024
Medio: Revista La Agencia de Viajes
Supl. : Revista La Agencia de Viajes
Tipo: Noticia general
Título: Ciberseguridad, un desafío para el turismo

Pág. : 28
Cm2: 528,5

Tiraje: 207
Lectoría: 621
Favorabilidad: No Definida

Ciberseguridad, un desafío para el turismo

La digitalización se ha vuelto un mandato salvador para las empresas de turismo, pero tiene su lado B: los delitos informáticos. La ciberseguridad es un factor clave para la supervivencia.

POR JUAN SCOLLO
juanscollo@ladevi.com

La transformación digital experimentada por las empresas turísticas les ha permitido seguir siendo relevantes en el marco de una industria en crecimiento. Pero el lado B de esa innovación es que las puso en el blanco de la delincuencia informática. Por lo que la ciberseguridad es la próxima adaptación en el camino de la evolución del ecosistema de los viajes.

El Instituto Nacional de Ciberseguridad de España (Incibe) da en el blanco cuando afirma que, en el desarrollo de su actividad, las empresas de turismo gestionan una gran cantidad de información de los clientes, propios y de sus proveedores: datos personales y bancarios necesarios para realizar reservas, compras, suscripciones a servicios, entre otros.

Ello implica la utilización de un conjunto de soluciones tecnológicas cada vez más amplio, con el objetivo de conseguir una mayor ventaja competitiva, más productividad y/o una mejor rentabilidad de sus procesos. Justamente, de eso se trata la transformación digital operada en los últimos años.

La transformación digital pone al sector al alcance de los piratas informáticos.

En su estudio titulado "Cybersecurity in travel goes beyond technology" (La ciberseguridad en los viajes va más allá de la tecnología), Robert Cole, analista senior de Phocuswright, ahonda en las características del sector que lo hacen susceptible a los piratas informáticos, entre ellas: complejas arquitecturas de sistemas; tecnologías centrales heredadas; múltiples puntos de contacto con los empleados y los clientes; escasez de personal y alta rotación de los mismos; baja sofisticación técnica; operaciones dispersas y localizadas; puntos de venta digitales y en las instalaciones; múltiples métodos de pago; y la lista continúa...

Datos: el oro del siglo XXI

Esa enorme montaña de datos, no siempre gestionada con criterios de ciberseguridad, convierte a la industria turística en un escenario perfecto para los ciberdelincuentes, que encuentran en estas tecnologías brechas digitales que aprovechar. "El robo de información y los ataques a sistemas son algunos de los principales riesgos que corre el sector turístico, pues los datos se han convertido en el nuevo oro del siglo XXI para los piratas informáticos, que ven en la venta de los mismos en el mercado negro una vía rápida para la obtención de un alto rédito económico", señala en su ebook ("Ciberseguridad en el sector turístico") la plataforma Thinktur.

De ahí que a medida que el sector avanza en su digitalización, "también deba hacerlo en materia de seguridad, pues prácticamente todo el itinerario de sus clientes y su cadena de valor suponen la generación de datos", afirma Thinktur.

La cuestión es que el desafío no se resuelve bajando la palanca de la digitalización. De hecho, es una carrera que corre a una velocidad exponencial, en la cual las tecnologías disruptivas, como el IoT (Internet de las cosas), la inteligencia artificial, el big data, la realidad aumentada o la robótica son la piedra angular de la nueva fase de transformación, que -a su vez- proporcionan nuevas vulnerabilidades y amenazas a las ciudades y empresas inteligentes.

Un enemigo silencioso, pero en auge

Los daños producidos por problemas derivados de ciberseguridad en las empresas y destinos turísticos van desde la pérdida de reputación o confianza por parte de los clientes, la interrupción de las operaciones, hasta el gasto en la renovación de sistemas de información o la apertura de procesos legales, con la consecuente pér-

LITORALPRESS

Fecha: 28-06-2024
Medio: Revista La Agencia de Viajes
Supl. : Revista La Agencia de Viajes
Tipo: Noticia general
Título: **Ciberseguridad, un desafío para el turismo**

Pág. : 29
Cm2: 510,1

Tiraje: 207
Lectoría: 621
Favorabilidad: No Definida

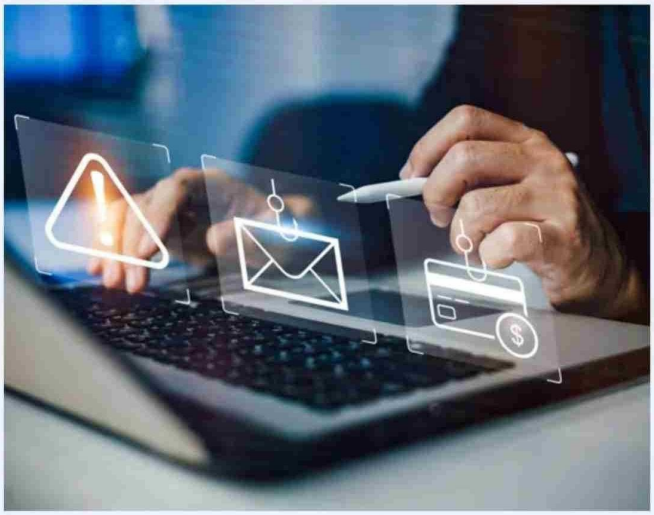
dida económica que ello supone. En definitiva, los ataques cibernéticos pueden tener un impacto devastador.

Si bien -como veremos- ha habido un puñado de atentados contra empresas turísticas que ganaron notoriedad en los medios, lo cierto es que la mayoría permanecen ocultos, lo que dificulta la trazabilidad estadística en el sector.

Según un informe de Phocuswright los intentos de fraude digital en 2022 en el sector de los viajes crecieron un 156%. "El sector funciona en un entorno en el que numerosos puntos potenciales de fallo hacen que la prevención y detección de violaciones de la ciberseguridad sean significativamente más difíciles en comparación con otros sectores", afirmó Robert Cole, de Phocuswright. Según el estudio, el 88% de los consejos de administración de las empresas consideran que la ciberseguridad es un riesgo para el negocio, más que un problema técnico de IT.

Frente a la falta de estudios específicos en el sector, un trabajo académico publicado en febrero pasado por Lázaro Benítez Florido, doctor en Turismo de la Universidad de Málaga, logró documentar y analizar 61 ciberataques contra empresas turísticas entre 2000 y 2023. De acuerdo con el informe, los hoteles fueron los más afectados, con 26 incidentes, seguidos de las OTA, con 10, y las aerolíneas (8).

"Cada ataque incluido en nuestra muestra se produjo en una fecha diferente y/o afectó a diferentes OTA, hoteles y restaurantes situados en diversas zonas geográficas y ciudades. Además, estamos seguros de que la industria de viajes y turismo ha sufrido más de 61 ciberataques, la cuestión es que no todas las empresas informan de los delitos cometidos porque estos incidentes afectan la reputación de las empresas y su imagen corporativa, así como la confianza de los consumidores", señaló el catedrático.



Los daños producidos por situaciones de ciberseguridad son imposibles de medir.

Los casos más resonados

La muestra del académico Benítez Florido incluye ciberataques contra gigantes del sector, como Marriott, Wyndham, Hyatt, InterContinental, Mandarin Oriental Hotel Group, Booking.com, FTI company, Sabre Corporation y las agencias de viajes Orbits y Expedia, así como las aerolíneas EasyJet y Air France, entre muchas otras.

Solo por detallar algunos de ellos, en 2018 una filtración de datos afectó a 500 mil clientes de British Airways. La violación comprometió las fichas de inicio de sesión, pago con tarjeta y reserva de viajes. Ese mismo año Marriott International sufrió una filtración de datos que perjudicó a más de 500 millones de usuarios (una de las más grandes de la historia) y expuso datos personales como nombres, direcciones, correos electrónicos y números de pasaporte.

En 2020, easyJet admitió que se había accedido a los datos personales de 9 millones de clientes y a los datos financieros de más de 2.000 pasajeros en un sofisticado ciberataque. De hecho, la aerolínea fue condenada a pagar una indemnización importante a cada cliente.

¿Son vulnerables las empresas más pequeñas?

En general, los casos más documentados son contra grandes marcas de viajes, pero ya sea una multinacional como una pequeña empresa emergente, ninguna compañía es inmune a la amenaza de ciberdelincuentes y estafadores.

De hecho, según Darren Williams, CEO de la empresa de ciberseguridad BlackFog, "los delincuentes buscan los objetivos más fáciles que puedan encontrar, por lo que las pequeñas cadenas hoteleras sin una infraestructura adecuada son las principales candidatas, ya que es menos probable que hayan invertido en herramientas, procesos y personas para proteger la organización. Menos aún dispondrán de tecnología contra la filtración de datos".

El experto consultado por Phocuswright coincidió en que, aunque un ciberataque puede resultar embarazoso y costoso para una gran empresa, "suele ser sobre todo una molestia". Sin embargo, una brecha puede suponer una "crisis existencial" para una startup. "Si eres una organización pequeña y sufres un incidente grave de ciberseguridad, puede ser suficiente para acabar contigo", confirmó Chris Clements, vicepresidente de Cerberus Sentinel.

¿Cuál es el nivel de riesgo de mi empresa?

Existen diversas herramientas y servicios en el mercado con el objetivo de que las empresas puedan evaluar su nivel de riesgo en ciberseguridad.

El Incibe de España, por ejemplo, ofrece una herramienta inicial de autodiagnóstico para en cinco minutos conocer el estado actual de ciberseguridad de la organización.

CONSULTAR DIAGNÓSTICO