Seguridad informática en hoteles:

las necesidades del sector de proteger sus sistemas

Las empresas hoteleras manejan datos de mucho interés para los ciberdelincuentes, por lo que contar con buena tecnología para proteger sus equipos es esencial.

Bárbara Bécares

Febrero 2020

El sector hotelero es uno de los principales focos para los ciberatacantes. Al cabo del año, miles de millones de personas se trasladan de ciudad o de país, por ocio o por trabajo, y eso lleva a que los alojamientos muevan grandes cantidades de dinero y más aún de datos personales que resultan muy atractivos para los hackers. Tanto es así que un informe de Deloitte presentado el pasado año concluía que, tras el sector bancario y financiero y de seguros, el hotelero es el tercero que más ataques a sus sistemas reciben.

El sector hotelero es particularmente vulnerable debido a su naturaleza ampliamente distribuida y altamente conectada

Y es que, además del atractivo a causa de las grandes cantidades de información que guardan estas empresas, también encontramos que no siempre son conscientes de la importancia de mantener sus sistemas bien protegidos, por lo que existe una gran oportunidad de mercado para las empresas de seguridad informática.

De la mano de Eduardo Valenzuela, Senior Presales Manager de A3Sec, Daniel Just, el Director del canal de Hospitality de Cerium Tecnologías, de Manuel Prieto, CEO de Easy Payment Gateway y Alex Capurro, fundador de la misma firma de pagos, todas ellas empresas expertas en este sector, analizaremos la situación, sus debilidades y vere-

Robo de tarjetas de crédito, usurpaciones de datos personales, vulnerabilidades en los servicios wifi o ataques a los puntos de venta son el tipo de ataques que más afecta al sector hotelero

mos unas pautas para saber dónde se deben enfocar los esfuerzos.

¿Por qué el sector hotelero atrae a los ciberdelincuentes?

Primero, vamos a comprender cuál es el atractivo de estas empresas para los hackers:

- **1. Son compañías muy conectadas.** Eso permite que puedan ser un blanco fácil desde muchos puntos. Primero, explica Eduardo Valenzuela, Senior Presales Manager de A3Sec, empresa que opera en España, México, Colombia y Estados Unidos, “se trata de un sector particularmente vulnerable debido a su naturaleza ampliamente distribuida y altamente conectada, lo que conlleva que las amenazas puedan llegar desde muchos puntos”. Como recuerda Daniel Just desde Cerium Technologies, no son solos los sistemas de un hotel lo que guarda información, también se usa tecnología que puede ser vulnerable para la seguridad perimetral, incluidos los procesos de pago o el uso del wifi por parte de los huéspedes.
- **2. Muchas personas se conectan a su WiFi.** Recuerda el portavoz de Cerium que “el modelo de custodiar únicamente nuestros datos ha cambiado por uno donde además debemos custodiar nuestras infraestructuras y velar por la seguridad de los equipos de nuestros huéspedes, que no sufran ningún percance mientras navegan por nuestras redes”. No hay que olvidar que las redes de conexión a Internet en estos lugares son usadas por infinidad de equipos y en ocasiones, para facilitar el acceso, ni siquiera son seguras.
- **3. Datos que resultan relevantes para los delincuentes.** Además de que diferentes servicios están conectados, estas compañías manejan una gran cantidad de información personal y de calidad de clientes que puede resultar muy atractiva para los delincuentes. “El elevado volumen de

CIBERSEGURIDAD,
TALÓN DE AQUILES DE LOS HOTELES

CLICAR PARA
VER EL VÍDEO

transacciones financieras que se ejecutan o, los sistemas de información publicados en la web, como son los sistemas de reservas, lo convierte en objetivo prioritario para los hackers", añade Valenzuela desde A3Sec. El CEO y fundador de Easy Payment Gateway recuerdan que las firmas de este sector "manejan información muy sensible, como los datos de tarjetas de crédito de sus clientes". Otro dato lo añade el portavoz de Cerium Technologies y explica que "a esto hay que sumar que las importantes cifras de negocio que mueve este sector son un atractivo importante".

- **4. Falta de concienciación.** Muchas de las empresas del sector no son conscientes de la importancia de integrar medidas de seguridad para sus sistemas. Y los ciberatacantes se aprovechan de ello.

"No son solo los sistemas de un hotel lo que guarda información, también se usa tecnología que puede ser vulnerable para la seguridad perimetral, incluidos los procesos de pago o el uso del wifi por parte de los huéspedes"

Daniel Just, Director del canal de Hospitality, Cerium Tecnologías

¿Es necesario que haya un CISO en una empresa hotelera?

Hay historias de grandes ataques realizadas a empresas de este sector y que demuestran lo importante que es proteger los sistemas. El mayor escándalo registrado hasta el momento fue el hackeo, durante años, vivido por la cadena de hoteles Marriott que a finales de 2018 anunció que una brecha de datos había expuesto datos sensibles de más de 500 millones de clientes. La empresa se dio cuenta, tras una alerta recibida de que había habido accesos no autorizados a la red de Starwood desde 2014. Marriot ha sido condenada a pagar 123 millones de dólares por el fallo.

En España, aún muchas empresas están desprotegidas pero son un blanco importante. No hay que olvidar que a comienzos del pasado mes de diciembre de 2019 se hizo público que desde 2015 está activo RevengeHotels, una campaña de malware en la que participan varios grupos con el objetivo de infectar a empresas hoteleras mediante la utilización de Troyanos de Acceso Remoto (RATs). La campaña ha aumentado de forma significativa su presencia en 2019, e investigadores de Kaspersky

"No es muy común que las empresas hoteleras cuenten con un CIO o CISO responsable de todo lo relacionado con la tecnología del negocio, pero poco a poco se irá implementando esta figura debido al aumento de estos ciberataques"

Manuel Prieto, CEO, Easy Payment Gateway

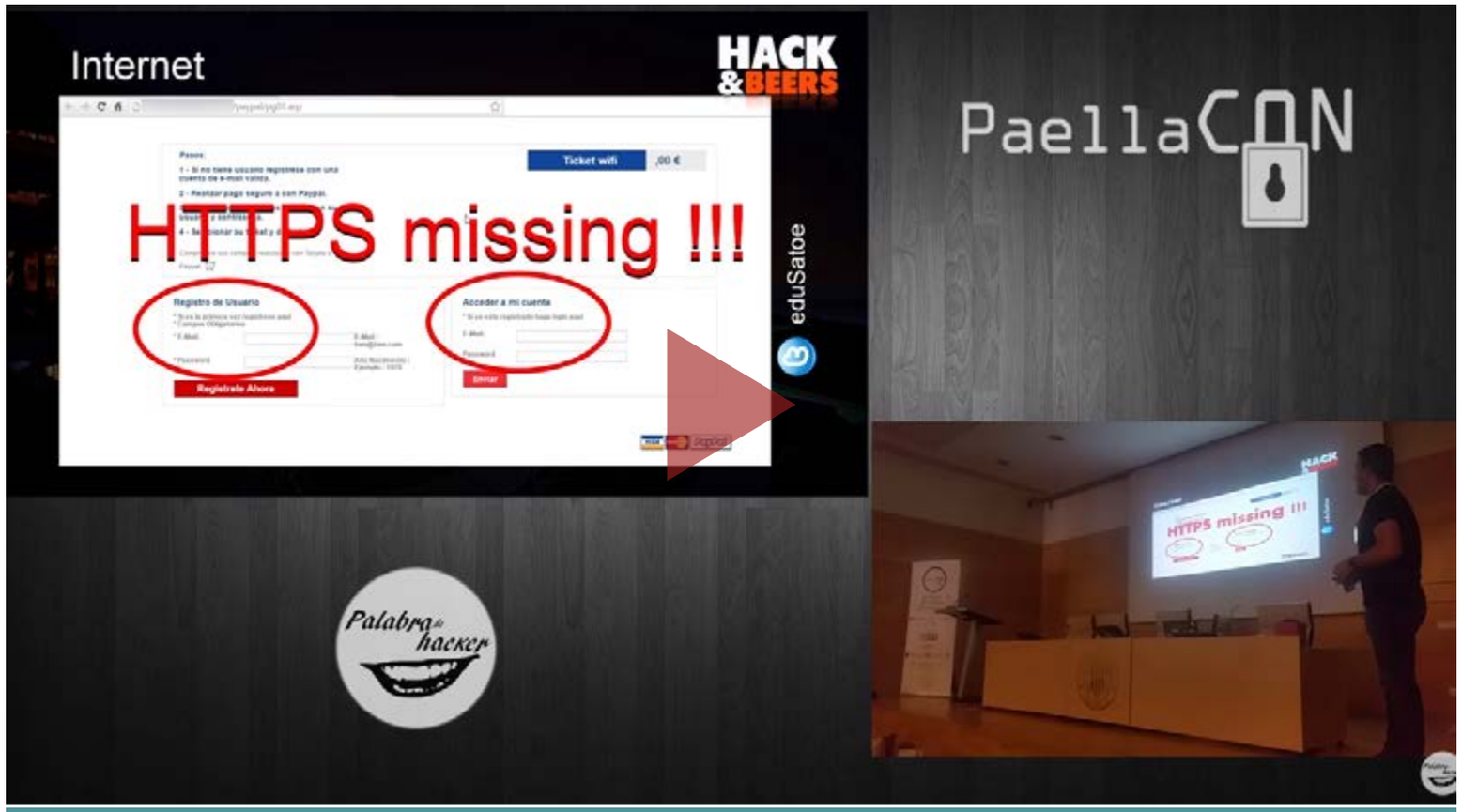
pudieron confirmar que más de 20 hoteles en Europa, Asia y América Latina han sido víctimas de ataques dirigidos.

Con este panorama, un director de seguridad que pueda gestionar la protección a los diferentes equipos de una empresa hotelera, no parece que sea una idea descabellada. Pero aún no está tan integrada como cabría esperar. Los portavoces de Easy Payment Gateway explican que "no es muy común que las empresas hoteleras cuenten con un CIO o CISO responsable de todo lo relacionado con la tecnología del negocio", pero las previsiones se presentan positivas. Manuel Prieto y Alex Capurro consideran que "poco a poco se irá implementando esta figura debido al aumento de estos ciberataques y para mantenerse al día de los avances tecnológicos de los que puedan beneficiarse". Y es que consideran que "el sector hotelero es un sector muy internacionalizado, por lo que, tanto en España como en el resto del mundo, hay conciencia de los riesgos y consecuencias de sufrir un ciberataque".

Desde Cerium Tecnologías explican que "las empresas hoteleras en España tienen que concienciarse mucho más en este sentido, aunque generalizar

no es bueno. Si nos medimos con la otra potencia hotelera internacional, que es la americana, hay que resaltar que las compañías hoteleras americanas invierten mucho más que las españolas". Daniel Just afirma que "la contratación de un CISO la están abarcando grandes compañías hoteleras. Las funciones de seguridad las están asumiendo los tradicionales CIO, o simplemente los responsables de sistemas". Los servicios de seguridad gestionados, incluida la consultoría o formación para las empresas que pueden tener un CISO en plantilla son una gran alternativa.

Por su parte, desde A3Sec Eduardo Valenzuela considera que "en líneas generales, la implementación de soluciones de protección en el sector es a día de hoy una asignatura pendiente". A pesar de que, añade, "se hace necesario proteger tanto las IT (Tecnologías de la Información) como las OT (Tecnologías de Operaciones). Y es que sólo el 14% de las empresas controlan las OT, lo que



HACKERS EN HOTELES DE CINCO ESTRELLAS

CLICAR PARA VER EL VÍDEO

provoca grandes brechas de seguridad en las empresas del sector hotelero".

Los expertos "consideran fundamental la concienciación de las empresas hoteleras y del sector turístico, la formación de todos los trabajadores, así como la contratación de servicios de ciberseguridad y de seguros a medida que reaccionen ante los ataques y restablezcan la actividad lo antes posible, minimizando los daños, tanto reputacionales como a terceros", de acuerdo con Valenzuela.

"El elevado volumen de transacciones financieras que se ejecutan convierte al sector hotelero en objetivo prioritario para los hackers"

Eduardo Valenzuela, Senior Presales Manager, A3Sec

¿En qué deben enfocarse las empresas hoteleras cuando busquen proteger su información?

Hay diversos problemas que puede confrontar un hotel, teniendo en cuenta toda la tecnología que pueden usar para mejorar sus servicios y hacer la estancia más cómoda a sus huéspedes.

Por un lado, explica el directivo de A3Sec que "los ataques que más se reproducen en el sector afectan a robos de tarjetas de crédito, usurpaciones de datos personales, vulnerabilidades en los servicios wifi o ataques a los puntos de venta". Y recuerda que "con el auge del IoT o Internet de las Cosas, el número de dispositivos conectados va en aumento y un ataque puede afectar y hasta inhabilitar servicios tales como el control de las cámaras de videovigilancia, los sistemas de ventilación, la apertura y cierre de puertas, etc., lo que abre un gran número de oportunidades para la ciberdelincuencia".

De hecho, recuerda Daniell Just desde Cerium la historia de un hotel en Austria "donde los ciberdelincuentes bloquearon los sistemas e incluso las puertas para que los huéspedes no pudieran entrar en sus habitaciones, y solicitaron un rescate para liberarlos". Y añade que "debido al incremento de la presencia de la tecnología y la comunicación en los sistemas, yo diría que son casi innumerables las maneras en las que podría afectar… Pero tal vez las más habituales o conocidas serían: el robo y la posterior exposición de los datos del hotel y sus clientes, paralizar la recepción de un hotel (impidiendo realizar check-ins en plena temporada), bloquear infraestructuras como la luz o la calefacción, o incluso las puertas de las habitaciones, en caso de que estuvieran conectadas las cerraduras".

Otra opción es la de externalizar algunos servicios como el de pagos a empresas eliminando posibles puntos de compromiso, "ya que cuantos más sistemas hay implicados en una transacción, mayor es la gama de opciones que tienen los atacantes potenciales", aseguran desde Easy Payment Gateway.

La Ley General de Protección de Datos

La normativa de privacidad hace muchas más duras las multas a aquellas empresas que filtren o pierdan información. Recuerda Eduardo Valen-

zuela, Senior Presales Manager de A3Sec que “el sector hotelero y de alojamiento en general, en su día a día, recopilan grandes cantidades de datos de carácter sensible de terceras personas y “están sujetos a cumplir las obligaciones de la Ley Orgánica 15/1999 de Protección de Datos de Carácter Personal y, a partir del pasado 25 de mayo de 2018, deben cumplir las obligaciones del nuevo Reglamento General de Protección de Datos”.

Por ello, las compañías deben realizar un registro de actividades de tratamiento: qué clase de datos se manejan, por qué se necesitan esos datos, cómo se almacenan, qué cesiones a terceros se realizan, etc.; se deben firmar los contratos con terceros: agencias de viajes, empresas de transporte, empresas informáticas, etc. Y, por supuesto, hay que asegurarse de que el cliente sepa qué datos suyos se recopilan a través de las páginas web de dichas empresas; o firmar contratos de confidencialidad con los empleados que manejan datos sobre clientes, entre otros asuntos.

Desde Cerium recuerda Just que “ya no basta como se hacía anteriormente con inscribir los ficheros de datos de clientes y proveedores, sino que en la actualidad hay que aplicar criterios como la responsabilidad proactiva, la privacidad por defecto y por diseño, las evaluaciones de impacto y el análisis de riesgo o la determinación de las medidas de seguridad aplicables, lo que supone un cambio radical de filosofía y de organización para las empresas”.

Enlaces de interés...

- La brecha de datos de Marriott International, la mayor de las conocidas en 2018
- El 52% de los incidentes de ciberseguridad en redes industriales están causados por el ser humano
- Los sistemas de reserva de la mayoría de los hoteles exponen datos de usuarios

Compartir en RRSS