tpvnews Ahora es más
SOLUCIONES POS, CAPTURA DE DATOS Y RETAIL

La ciberseguridad y el software de gestión: dos desafíos en el camino de la digitalización del sector Horeca

El sector Horeca, que aglutina a hoteles y restaurantes, sigue avanzando en su proceso de transformación digital, aunque se observan diferentes velocidades por la tipología de los establecimientos y su tamaño. En este camino, los responsables de TI consultados por TPVnews han señalado dos grandes áreas, claves para su digitalización, que siguen siendo asignaturas pendientes: la ciberseguridad y la incorporación de soluciones de software de gestión. Check Point Software, Serval Networks, Cegid y Wolters Kluwers Tax & Accounting España repasan el nivel de digitalización de estas empresas y dan respuesta a sus principales inquietudes.

Rosa Martín

IR A PÁGINA SIGUIENTE

La ciberseguridad preocupa a los CIO de las empresas del sector Horeca por el auge de las ciberamenazas y, en muchos casos, los escasos medios que tienen para combatirlas. Los datos confirman que el sector está en el punto de mira de los ciberdelincuentes. Según datos de Check Point Research, en mayo de este año el número promedio de ataques semanales por organización en esta industria se cifró a nivel global en 1.934, lo que supone un incremento del 48 % con respecto a mayo de 2024 y un incremento del 78 % en dos años.

Eusebio Nieva, director general técnico de Check Point Software para España y Portugal, explica que los hoteles y restaurantes por su creciente nivel de digitalización y la cantidad de información sensible que manejan son objetivos atractivos para los ciberdelincuentes.

Serval Networks tiene una visión similar. Considera que este sector por "su nivel de digitalización creciente, combinado con recursos limitados en ciberseguridad, lo convierte en un blanco fácil", como apunta Óscar Vierge, *sales director strategic accounts* de Serval.

Eusebio Nieva, director general técnico de Check Point Software para España y Portugal

Los especialistas en ciberseguridad indican que este sector se enfrenta a múltiples amenazas como *ransomware, phishing* y *spear phishing*, ataques contra terminales de punto de venta (POS), vulnerabilidades en dispositivos IoT e incluso wifi mal protegida. "También son cada vez más frecuentes los ataques con doble extorsión, que combinan el cifrado de los datos con su robo para forzar el pago de un rescate", destaca Nieva.

"En demasiados casos, las defensas son básicas y no se abordan las amenazas actuales con un enfoque preventivo y avanzado"

Óscar Vierge añade que entre las amenazas más comunes que enfrentan como el robo de datos, especialmente de la información de tarjetas de crédito y pasaportes, también

es frecuente “el compromiso de los terminales punto de venta y los ataques que se aprovechan de sistemas obsoletos o mal segmentados en la red”.

Nivel de madurez en ciberseguridad

Los expertos coinciden en señalar que el nivel de madurez en ciberseguridad es muy desigual. Las grandes cadenas hoteleras y de restauración tienen equipos, recursos y soluciones avanzadas, mientras que las pequeñas empresas no cuentan con una estrategia sólida en este apartado. Nieva indica que “en demasiados casos, las defensas son básicas y no se abordan las amenazas actuales con un enfoque preventivo y avanzado”.

Muchas pymes no han adoptado medidas como la segmentación de redes, la monitorización continua o la autenticación multifactor. Y “la concienciación del personal y la gestión de accesos privilegiados siguen siendo asignaturas pendientes”, apunta Vierge.

Un factor que ha contribuido a esta situación es que la inversión en ciberseguridad se ve como un coste y no como una necesidad estratégica para la continuidad del negocio.

Principales preocupaciones

En este contexto los responsables de TI de las empresas del sector Horeca tienen que combatir numerosas amenazas. Entre estos riegos sus principales preocupaciones son las vulnerabilidades de día 0, la protección de los dispositivos BYOD, las amenazas que entran por el correo electrónico y la responsabilidad ante usos incorrectos del wifi.

Vulnerabilidades de día 0

Las vulnerabilidades de *zero day* o día 0 son uno de los mayores retos de la ciberseguri-

Óscar Vierge,
sales director strategic accounts de Serval Networks

dad porque explotan antes de que exista un parche oficial o una solución definitiva. Para combatirlos la recomendación de Serval Networks es adoptar un enfoque basado en la detección avanzada y la respuesta proactiva.

"Apostar por los servicios gestionados permite tener vigilancia continua, capacidades de detección y respuesta ante amenazas y actualizaciones en tiempo real frente a nuevas vulnerabilidades"

El especialista de esta compañía recomienda contar con soluciones EDR o XDR que incorporen análisis de comportamiento capaces de detectar actividades anómalas. La microsegmentación de red que ayuda a limitar los movimientos laterales dentro del entorno en el caso de que una amenaza consiga acceder a la red y los parches virtuales son otras de sus recomendaciones.

Nieva coincide en estas medidas y añade el uso de *sandboxing* avanzado para detectar comportamientos anómalos y el uso de herramientas avanzadas. "Es esencial utilizar tecnologías de prevención proactiva impulsadas por inteligencia artificial como ThreatCloud AI de Check Point Software, que analiza más de 2.000 millones de eventos de seguridad diarios", destaca.

Vierge comenta que otro imprescindible para combatir este tipo de amenazas es contar "con una monitorización continua del entorno con servicios gestionados de detección y respuesta (MDR/SOC). Estos servicios permiten a las organizaciones contar con una supervisión especializada 24x7 y reaccionar con rapidez ante cualquier indicio de ataque".

tpv news Ahora es más
SOLUCIONES POS, CAPTURA DE DATOS Y RETAIL

Protección de los dispositivos BYOD

El uso de los dispositivos personales para entornos corporativos que se denomina por sus siglas en inglés BYOD (*Bring your own device*) es una práctica extendida que incrementa la superficie de exposición a amenazas si no hay una gestión correcta. Para proteger estos dispositivos los especialistas en ciberseguridad aconsejan adoptar un modelo de *Zero Trust Networks Access*, limitando el acceso a los recursos de la organización en función de la seguridad del dispositivo, utilizar herramientas de gestión de dispositivos móviles y aplicaciones móviles (MDM/MAM), establecer controles de acceso basados en roles y aplicar políticas de cifrado de datos tanto en reposo como en tránsito para proteger la información sensible.

Nieva recuerda que cuentan con soluciones específicas como Harmony Mobile Check Point Software, que ofrece defensa avanzada contra el *malware, phishing* y aplicaciones maliciosas en dispositivos BYOD. Y el responsable de Serval insiste que es "recomendable complementar estas tecnologías con formación al personal, sensibilizándolos sobre los riesgos asociados al uso de dispositivos personales y promoviendo prácticas seguras en el manejo de datos y accesos".

El correo electrónico sigue siendo el principal vector de entrada de los ataques en España

Amenazas en el *email*

El correo electrónico sigue siendo el principal vector de entrada de los ataques en España. El Security Report Iberia 2025 indica que el 58 % de los archivos maliciosos detectados se propaga a través de este canal. Este dato justifica la preocupación que tienen los equipos de seguridad y de TI ante esta amenaza. Para combatirla, además de las soluciones avanzadas de protección del correo electrónico, que combinan inteligencia artificial, *sandboxing* y análisis avanzado para detectar *phishing* y *malware* en archivos adjuntos y maliciosos, es aconsejable realizar de forma periódica simulacros de *phishing* para empleados para sensibilizarles y formarles para que sepan identificar los correos fraudulentos.

El experto de Serval Networks señala que "integrar el correo con herramientas de automatización y orquestación de seguridad (SOAR) para respuestas automáticas" es un modo de mejorar la capacidad de respuesta ante incidentes ya que estas herramientas permiten generar alertas, aplicar políticas o ejecutar acciones correctivas de forma automatizada ante las posibles amenazas.

Ambos expertos recalcan que la seguridad del correo electrónico es una cuestión inter-

na que tiene que abordar la empresa porque los filtros de las empresas proveedoras de aplicaciones de correo son útiles, pero no suficientes ante las amenazas avanzadas y dirigidas. Y, al mismo tiempo, las operadoras también están contribuyendo a reducir el tráfico malicioso, pero esto no sustituye a la protección interna de cada empresa.

Wifi

El uso incorrecto que pueden realizar algunos clientes cuando los establecimientos ofrecen wifi pública es un aspecto que genera dudas entre los CIO. El director general técnico de Check Point Software para España y Portugal aclara esto señalando que "el establecimiento no es responsable de forma directa de los actos individuales de un cliente mientras usa su wifi, pero sí tiene responsabilidad legal sobre cómo gestiona este servicio".

Si el establecimiento no toma las medidas técnicas para proteger el servicio y cumplir con la normativa puede enfrentarse a sanciones o incluso a responsabilidad penal por omisión ante delitos graves o brechas de datos. Por tanto, tiene que registrar conexiones, informar al usuario sobre los términos de uso antes de la conexión, implementar medidas de seguridad, notificarlas y segmentar la red.

Recomendaciones para reforzar la seguridad

Ante el crecimiento de los riesgos y las ciberamenazas que cada vez son más complejas y sofisticadas, los expertos recomiendan establecer una base de seguridad sólida con medidas esenciales y a partir de ahí continuar implementando otras más avanzadas. Nieva considera que "lo primero es adoptar

un enfoque de seguridad integral y preventivo que contemple la protección de todos los vectores de ataque".

Las medidas que citan los especialistas como claves para reforzar la seguridad comprenden desde la implantación de arquitecturas de seguridad basadas en la filosofía *Zero Trust* hasta el uso de soluciones unificadas que protejan la red, los *endpoints*, la nube, el correo electrónico y los dispositivos IoT, pasando por la segmentación de redes, el establecimiento de copias de seguridad y la adopción de herramientas avanzadas para la detección de amenazas y *antiransomware*. Y, además, formar al personal para que pueda detectar correos maliciosos y mantener buenas prácticas de navegación. Sin olvidar el cumplimiento normativo como la Directiva NIS2.

Si las empresas no disponen de recursos internos Óscar Vierge recomienda externalizar la seguridad. "Apostar por los servicios gestionados permite tener vigilancia continua, capacidades de detección y respuesta ante amenazas y actualizaciones en tiempo real frente a nuevas vulnerabilidades sin necesidad de grandes inversiones".

Enrique Blanco, director de la unidad de negocio para *mid market* de Cegid

"El uso del software de gestión todavía genera dudas, principalmente por desconocimiento, falta de tiempo y miedo al cambio"

Software de gestión

La adopción de herramientas de software para mejorar la gestión es otro de los retos que sigue teniendo el sector Horeca. En este ámbito, al igual que ocurre en ciberseguridad, el nivel de digitalización es desigual, estando a la cabeza los establecimientos más grandes y en una posición más rezagada los más pequeños. Los últimos datos apuntan a que solo el 16 % de los establecimientos hoteleros se considera altamente digitalizado y un 32 %

está en proceso de transformación digital e incorporando herramientas para gestionar las reservas y automatizar procesos. En los más pequeños la brecha es mayor. Por ejemplo, solo el 32 % tiene página web y únicamente el 18 % utiliza redes sociales de forma activa. Estos datos, según indica Ana Belén Moreno, Payroll & HCM *product manager* en Wolters Kluwer Tax & Accounting España, revelan que limitan "su visibilidad *online* y su capacidad para competir en un mercado más digital".

Enrique Blanco, director de la unidad de negocio para *mid market* de Cegid, cree que, además del tamaño, el grado de digitalización de las empresas de este sector depende de la ubicación y de la mentalidad del propietario. En este sentido, subraya que "la actitud, visión y apertura al cambio del propietario son factores claves que determinan el grado de adopción tecnológica".

Ambas compañías señalan que grandes cadenas hoteleras y de restauración avanzan

hacia la automatización con el uso de herramientas específicas para gestionar puntos de venta, reservas, personal o el *stock* e incluso ya hacen un uso intensivo del *big data*, pero las más pequeñas tienen todavía barreras que salvar.

"El uso del software de gestión todavía genera dudas, principalmente por desconocimiento, falta de tiempo y miedo al cambio", destaca Enrique Blanco. "La gestión del cambio o la formación tecnológica son factores que actúan como freno", añade Ana Belén Moreno.

Carencias y barreras

Casi la mitad de los hosteleros rechazan el uso de la tecnología porque consideran que

su gestión es difícil, así se reflejaba en el último informe "Las claves de la digitalización en Hotelería" de la plataforma ConedtadHos, integrada por Hostelería de España y tres grandes proveedores de este sector. En el terreno del software de gestión los especialistas han identificado varias carencias que están relacionadas con este indicador. Una de ellas es la falta de integración entre soluciones. "Muchos negocios operan con múltiples sistemas aislados que no se comunican entre sí, lo que genera duplicidades, errores y pérdida de eficiencia", destaca el responsable de Cegid.

Esta desconexión va unida a la escasa usabilidad, lo que implica "interfaces poco intuitivas y procesos complejos que hacen que el día a día digital se convierta en un obstáculo", avanza Moreno.

El coste es otro factor que frena la digitalización y hace que se vea como una inversión fuera de sus posibilidades. A esto se suma la falta de soporte técnico y de mantenimiento adecuado, lo que agrava la experiencia del usuario y alimenta la desconfianza hacia la tecnología.

Los proveedores de software están adaptando su oferta para responder a las necesidades específicas del sector

"Otra barrera es la falta de personalización o flexibilidad. Y es que muchas pymes del sector sienten que la tecnología está diseñada solo para grandes cadenas, no para su realidad, algo que no es del todo cierto en la actualidad", indica Blanco.

Para eliminar estos frenos y cambiar la idea de que el software es difícil de usar, los proveedores de software señalan que están adaptando su oferta para responder a sus necesidades específicas con el propósito de demostrar que la tecnología puede incrementar la productividad, optimizar recursos y ahorrar tiempo.

Facturación electrónica

Uno de los retos que tiene ante sí el sector Horeca es la adaptación a las nuevas normativas de facturación que digitalizan este proceso. El Reglamento de Sistemas Informáticos de Facturación, que se deriva de la Ley Antifraude, fija una serie de requisitos que tienen que cumplir los desarrolladores de software porque a partir del 29 de julio de este año no se podrán comercializar programas que no estén adaptados a esta normativa. Y las empresas que ya dispongan de un software de facturación tendrán que adaptarlo antes del 1 de enero de 2026 en el caso de que tri-

buten por el Impuesto de Sociedades y el 1 de julio de ese mismo año para el resto de empresas y autónomos.

Esta normativa, según indica Ana Belén Moreno, tiene especial incidencia en los negocios del sector Horeca debido al volumen de facturas que emiten a través del TPV que se considera un sistema informático de facturación. “Restaurantes, bares, cafeterías y hoteles deberán adaptarse a una nueva normativa y contar con un software homologado que garantice la inalterabilidad de las facturas”, insiste.

El desarrollo de la otra ley que establece la implantación de la factura electrónica en las relaciones de empresas y profesionales, la Ley Crea y Crece, va más despacio y todavía no se ha publicado el reglamento que detallará su aplicación.

El conocimiento sobre estas normativas y su ritmo de implantación está siendo desigual, como confirman los expertos. “Aunque las

Analítica e IA

Los especialistas en software recomiendan aplicar sobre las soluciones básicas de gestión una capa de analítica e inteligencia de negocio para tomar decisiones basadas en datos y anticiparse a la demanda. Blanco señala que el uso de soluciones de *Business Inteligence* es una “ventaja competitiva”. Este proveedor cuenta con la solución Cegid Revo Genius, que ofrece información en tiempo real sobre ventas, rendimiento de producto, comportamiento de cliente y, además, se puede integrar con otras soluciones como Cegid Revo Intouch para transformar los datos en programas de fidelización personalizados.

La inteligencia artificial es otra tecnología que interesa a los CIO de este sector y se preguntan cómo pueden sacarla el máximo partido. En hostería pueden usarse para analizar patrones de consumo, optimizar la gestión de turnos y personalizar la experiencia del cliente. A juicio de Blanco, “debe de atender necesidades reales y tangibles como aumentar los márgenes, reducir los costes de producción, fidelizar a los clientes, etc”.

En Cegid Revo utilizan la inteligencia artificial para simplificar la toma de decisiones, para sugerencias de venta cruzada en autopedidos, en análisis predictivos o recomendaciones de campañas de fidelización, pero siempre “con un enfoque de inteligencia aumentada, donde la tecnología complementa, pero no sustituye, el valor humano”, recalca el responsable de Cegid.

Ana Belén Moreno, *Payroll & HCM product manager* en Wolters Kluwer Tax & Accounting España

"Los nuevos softwares de facturación no solo deben garantizar el cumplimiento legal, sino que también deben aportar valor en términos de automatización, reducción de errores y mejora en la transparencia y trazabilidad fiscal"

grandes cadenas ya están adoptando software compatible con las nuevas normativas, muchas micropymes todavía no conocen bien los requisitos de la Ley Antifraude ni del sistema Verifactu, que será obligatorio a partir del año que viene", confirma Blanco. Según datos de la última edición del "Barómetro de la Asesoría", que realiza Wolters Kluwer, el 55,6 % de los despachos profesionales considera que las empresas aún no están preparadas para los inminentes cambios en facturación.

A pesar de esta falta de preparación, los proveedores de software no solo han adaptado sus soluciones para cumplir con las normas, sino que han realizado diversas acciones de concienciación y divulgación. "Es fundamental acompañar al sector en este proceso de adaptación y esto es precisamente nuestro papel", sostiene Blanco.

La responsable de Wolters Kluwer Tax & Accounting España cree que la adaptación a la nueva normativa de facturación es un reto, pero también una oportunidad. "Los nuevos softwares de facturación no solo deben garantizar el cumplimiento legal, sino que también deben aportar valor en términos de automatización, reducción de errores y mejora en la transparencia y trazabilidad fiscal", destaca. Estas nuevas funcionalidades convierten a este proceso en una ocasión para,

además del cumplimiento legal, “modernizar la gestión interna de los negocios”, reitera.

Los proveedores están listos para acompañar a las empresas en la adaptación de sus sistemas de facturación a la normativa. Y, además, recuerdan que todavía hay ayudas como el Kit Digital que facilitan a los negocios más pequeños el acceso a estas soluciones.

Herramientas para la digitalización

A la hora de afrontar un proceso de transformación digital, los proveedores de software aconsejan disponer de soluciones integrales, que cubran varias necesidades, y cumplan con la normativa.

Wolters Kluwer considera que lo más básico es contar con un software de facturación, que cumpla con la normativa vigente y facilite la automatización contable, y disponer de soluciones integradas de gestión empresarial (ERP) que permitan controlar los inventarios, las compras, las ventas y la trazabilidad del negocio. Ana Belén Moreno apunta que en su oferta hay herramientas como a3ERP y a3innuva ERP que ayudan a las empresas a mejorar su gestión. Al mismo tiempo, cree que para los restaurantes es esencial disponer de un TPV conectado al sistema de gestión para agilizar el servicio en la sala y centralizar la información. Y para la gestión interna del área laboral y de Recursos Humanos cuenta con otras soluciones como a3innuva Nómina.

Contar con soluciones modulares, escalables y en la nube es la mejor vía para lograr una gestión eficiente

Su recomendación general es “contar con soluciones modulares, escalables y en la nube” porque es la “mejor vía para lograr una gestión más eficiente, rentable y preparada para un sector tan dinámico y con alta rotación como el de Horeca”.

Cegid comparte con Wolters Kluwer que contar con una solución integral que abarque desde el punto de venta hasta la gestión administrativa es esencial para optimizar operaciones y mejorar la experiencia del cliente. Blanco señala que Cegid Revo ofrece a los restaurantes una *suite* 360º para proporcionar un ecosistema de herramientas diseñadas para satisfacer sus necesidades, que incluye desde un software POS avanzado hasta un sistema de gestión de inventarios en tiempo real.

La facilidad de uso es otro factor que está cuidando para que las empresas vean que las soluciones de software de gestión se adaptan a sus necesidades. El directivo de Cegid pone como ejemplo Cegid Revo Xef que está diseñada para iOS y ofrece “una experiencia de uso simple, intuitiva y ágil”.