Señores

Panamá, 18 de diciembre de 2023.

SUPERINTENDENCIA DEL MERCADO DE VALORES
Ciudad de Panamá

Vía: Plataforma digital

Ref.: Notificación de Incidente de Ciberseguridad

Estimados señores **SUPERINTENDENCIA DEL MERCADO DE VALORES**,

Nosotros, **TROPICAL RESORT INTERNATIONAL INC..**, sociedad constituida bajo las leyes de la República de Panamá, debidamente inscrita en el Registro Público de Panamá en el Folio No. 313586, con domicilio en Gamboa, corregimiento Cristobal, Provincia de Colon, debidamente representada por **HERMAN BERN PITTI**, varón, panameño, soltero, portador de la cédula de identidad personal No. 4-79-786, en su calidad de Presidente y Representante Legal, comparecemos ante uds. con el debido respeto a fin de notificar un hecho de importancia o hechor relevante, hemos sufrido un incidente de ciberseguridad que ha impactado en los datos almacenados en los servidores del Hotel Gamboa Rainforest Reserve.

Así, después de investigar el incidente, comunicamos los detalles de los hallazgos obtenidos hasta la fecha:

DETALLES DEL INCIDENTE	
Empresa	**Hotel Gamboa Rainforest Reserve (Tropical Resort international Inc.)**
Resumen del Incidente: **Fecha y motivo del incidente de seguridad**	El 31 de octubre de 2023 se dio un incidente de ciberseguridad detectado mediante notificación de correo electrónico por la herramienta de Antivirus **Trend Micro,** que pudo haber afectado al Hotel Gamboa Rainforest Reserve. La notificación electrónica indicó que se habían cifrado servicios de aplicaciones a través del Código Malicioso (*Malware) Akira (Ransomeware*). Reunimos inmediatamente a nuestro equipo de expertos en TI (Tecnología de la Información) y contratamos a una firma forense de TI para que investigara el suceso. Simultáneamente, pusimos en marcha todas las medidas de recuperación de la información posiblemente impactada, examinando y cerrando nuestros servidores afectados y neutralizamos el malware que utilizaron los atacantes, a fin de contrarrestar los daños y evitar una posible repetición. Luego de investigaciones preliminares, se estableció que los servicios afectados podrían involucrar los siguientes Sistemas: • Sistema de Contabilidad (Zeus), • Sistema de Marcación (Kronos), • Sistema de Planilla (Payday),
Hechos y efectos del incidente de seguridad	Entre los hallazgos se han identificado que no hay certeza de que haya habido un robo de información, pero tampoco se ha podido descartar lo contrario; lo que si se produjo fue una encriptación de las bases de datos haciendo imposible la conexión a las citadas aplicaciones dejando las mismas inutilizables. A la fecha no se tiene conocimiento de ningún uso indebido o ilícito de los posibles datos indebidamente obtenidos.
Medidas adoptadas	En respuesta al ataque se tomaron las siguientes acciones: 1. Se aislaron todos los equipos supuestamente afectados. 2. Se iniciaron los trabajos de fortalecimiento de las políticas de seguridad de los servidores y equipos de usuarios a nivel de las actualizaciones de Sistema Operativo, Agentes de Antivirus y versiones de programas instalados. 3. Se restauraron respaldos de los servidores que no fueron comprometidos (Opera Gamboa Rainforest Reserve), por lo que no hay constancia que se atacara a las bases de datos de clientes. 4. Se revisaron las configuraciones del Directorio activo (directorio donde están los usuarios y sus contraseñas) y de las máquinas virtuales "VMware" 5. Revisión y aplicación de las principales recomendaciones dadas por el proveedor de Antivirus (Nextcom) para mejorar

	la seguridad de los sistemas de almacenamiento, respaldo, así como las reglas de bloqueo del cortafuegos ("Firewall") perimetral. 6. Se desplegó el agente antivirus "Apex One" en todos los equipos (servidores, estaciones de trabajo). Adicionalmente, se han dado las siguientes recomendaciones: 1. Utilizar contraseñas seguras y únicas para todos los servicios y cuentas. 2. No dejar ninguna sesión de usuario iniciada en servidores. 3. Proceder con la Activación del software "FortiClient" para las conexiones remotas y una red privada virtual (VPN). 4. Eliminar métodos de conexión remotos "AnyDesk", "TeamViewer" y "VNC", dado que podría ser una potencial brecha de seguridad para las plataformas de todo sistema productivo. 5. Actualizar de manera general los hipervisores en su red, para no contar con sistemas con vulnerabilidades conocidas. 6. Implementar un endurecimiento general en las políticas de los cortafuegos ("Firewall") perimetrales. 7. Realizar copias de seguridad periódicas de los datos y almacenarlas en un lugar seguro. 8. Dar de baja a equipos con sistemas operativos legados sin soporte. **Acciones en proceso de implementación actualmente:** 1. Migración de las aplicaciones y soluciones afectadas a la "nube", dado que cuentan con muchos más mecanismos de ciberseguridad. 2. Utilización de repositorios de respaldo con Inmutabilidad. 3. Implementación de copias del lado de almacenamiento ("QNAP") para realizar una reversión de las bases de datos a su estado original en caso de que ocurra un ataque (o cualquier cambio con resultados no deseados) a fin de que no se vean comprometidos los archivos de respaldo o cualquier dato almacenado en los servidores. 4. Habilitación del doble factor de autenticación en los servidores y en todos los sistemas disponibles. 5. Instalación de la solución de software llamada "Malware Remover" en el servidor y ejecutar análisis periódicos para detectar posibles infestaciones. 6. Instalación de softwares adicionales de seguridad como "*Security Counselor*" en el servidor "Qnap". 7. Restricción de los protocolos permitidos en las interfases del almacenamiento conectado en red ("NAS"). 8. Creación y definición de las estrategias y planes de recuperación considerando los niveles de tolerancia necesarios para la empresa.

Respetuosamente,

Herman Bern Pitti
Representante Legal
Tropical Resort International Inc.