PRINSOTEL

Información sobre el ciberataque sufrido en Prinsotel el pasado 16 de mayo

1. **Descripción general del incidente y momento en que se ha producido**

En el día 16-05-24 a las 8.15 hs en la Sede Central de Prinz Hoteles SA, sita en c/Ter 27 Palma, que gestiona los establecimientos PRINSOTEL (La Dorada, La Pineda, Alba, Mal Pas y La Caleta), detectamos un ataque malware (ramsomware) que bloqueó todos los servidores de la empresa anunciando que habían encriptado nuestros datos.

Se procedió a contratar un servicio experto de ciberseguridad, quienes se encargaron de gestionar los procesos de contención, remediación y análisis forense. Tras el análisis realizado sobre los equipos afectados en el ataque, hemos podido evidenciar que parte de los datos que fueron secuestrados han sido exfiltrados y, algunos publicados en distintos grupos de ciberdelincuentes.

2. **Descripción de los datos e información personal afectados.**

Le informamos que la compañía tecnológica que nos ha acompañado tras el incidente ha podido verificar entre los datos robados, se encuentran: datos personales de clientes y usuarios de PRINSOTEL, en concreto: nombre, apellido, dirección, DNI, pasaporte, teléfono, email. Por otro lado, también ha afectado a información societaria de PRINSOTEL. **En ningún caso se ha evidenciado que se hayan robado datos financieros ni contraseñas.**

3. **Resumen de las medidas implantadas hasta el momento para controlar los posibles daños.**

PRINSOTEL desde el momento que fue conocedor de este hecho puso en marcha un plan de respuesta que implicaba la involucración de un equipo técnico experto para identificar el origen de la brecha y contener el ataque, fue comunicado inmediatamente a la Guardia Civil (para su remisión ante la Brigada Central de Investigación Tecnológica de la Policía Nacional), así como a la Agencia Española de Protección de Datos.

Desde PRINSOTEL se creó un comité de crisis compuesto con profesionales expertos para poder contener el incidente y gestionar todas las comunicaciones con los afectados para mantenerlos informados en todo momento del incidente. En la actualidad la incidencia se encuentra subsandada y Prinsotel cuenta con un plan de acción detallado para evitar que situaciones similares en el futuro.

En cuanto PRINSOTEL fue conocedor de la exfiltración, el 26 de junio, remitió a los clientes y usuarios afectados por vía correo electrónico, información detallada sobre el incidente con un detalle de pautas de actuación para evitar que pudieran verse afectados directamente por conductas fraudulentas.

En la actualidad la incidencia se encuentra controlada y Prinsotel cuenta con un plan de acción detallado para evitar que situaciones similares en el futuro. Entre otras de las medidas de este plan de acción, se encuentra el establecimiento de un servicio de monitorización y gestión de incidentes de seguridad a través de un SOC que integre los principales sistemas de seguridad de la organización con el SIEM definido. Este servicio incluirá: (i) la monitorización de sistemas perimetrales, AD, IDS/IPS, servidores críticos, EDR, entre otros. Asimismo, este servicio será capaz de gestionar el sistema EDR de la organización, (ii) proveerá a Prinsotel de un servicio de gestión de vulnerabilidades sobre los sistemas digitales (servidores, endpoints, etc) de Prinsotel y alerta temprana de amenazas, con el objetivo de robustecer la seguridad continua de la organización, e (iii) incluirá además guías de bastionado seguro para los sistemas existentes.

PRINSOTEL

4. **Contacto del Delegado de Protección de datos de PRINSOTEL**

Para cualquier cuestión adicional o mayor detalle de la misma puede dirigirse al Delegado de Protección de Datos, contactando con él a través de dataprotection@prinsotel.com.

5. **Ejercicio de derechos de protección de datos**

Puede ejercitar los derechos en materia de protección de datos que le amparan: el derecho a acceder, rectificar, suprimir o pedir la portabilidad de sus datos personales o el derecho a oponerse o a limitar determinados tratamientos de sus datos en la dirección electrónica indicada.

Puede consultar información adicional sobre el tratamiento de sus datos (fines del tratamiento, categorías de datos, procedencia y destinatarios de los mismos, plazos de conservación, etc.) consultando nuestra política de privacidad incorporada en https://www.prinsotel.com/es/politica-privacidad/.

6. **Recomendaciones de actuación tras el incidente.**

Como consecuencia del ataque sufrido, es nuestra obligación darles algunas pautas para garantizar la seguridad de sus datos personales:

1. **Nunca** y bajo ningún concepto, le pediremos sus datos bancarios por medios electrónicos. Si reciben una llamada o mensaje solicitando este tipo de datos, no los compartan NUNCA.

2. En caso de recibir publicidad PRINSOTEL por correo electrónico, por SMS, o redes sociales **verifique siempre la identidad** del remitente y, en caso de duda, nunca haga clic en ningún enlace en el que no confíe.

3. **Desconfíe de llamadas en nuestro nombre** o desde cualquiera de nuestros hoteles. Verifique que se trata de una llamada desde un operador conocido y de nuevo, nunca aporte datos privados.

Adicionalmente, nos gustaría, a través del presente documento prevenirle de todos los posibles intentos de fraude como consecuencia del incidente como Phising, Spear Phising, Vishing, Smising, Pharming, Whaling …etc. con el fin de que puedan estar atentos a cualquiera de estas maliciosas acciones.

A continuación, se detallan este tipo de ataques o fraudes para que puedan identificar cualquier conducta anómala y puedan prevenir cualquiera de estas acciones:

- ***Phising:*** El phishing es una técnica de ingeniería social que consiste en el envío de correos electrónicos que suplantan la identidad de compañías u organismos públicos y solicitan información personal y bancaria al usuario. A través de un enlace incluido en el email, intentan redirigirlo a una página web fraudulenta para que introduzca su número de tarjeta de crédito, DNI, la contraseña de acceso a la banca online, etc.

  Estos correos electrónicos fraudulentos suelen incluir el logotipo o la imagen de marca de la entidad, pueden contener errores gramaticales y en ocasiones intentan transmitir urgencia y miedo para que el usuario realice las acciones que le solicitan.

Un email de tipo phishing también puede llevar un archivo adjunto infectado con software malicioso. El objetivo de este malware es infectar el equipo del usuario y robar su información confidencial.

- ***Spear Phising:*** Los atacantes crean correos electrónicos, páginas web e incluso mensajes cortos de carácter falso que parecen auténticos y que solicitan información de inicio de sesión de los usuarios. Es así como los estafadores se hacen con los datos de acceso para tiendas online, redes sociales o espacios de almacenamiento en la nube. En el peor de los casos, se hacen incluso con información bancaria o datos de la tarjeta de crédito. Los estafadores saben que hay muchos usuarios que no se toman en serio la seguridad de las contraseñas y que usan una misma contraseña para diferentes servicios. De esta forma, con una página web de phishing sencilla se pueden obtener datos sensibles, información que tiene un alto valor económico en el mercado negro digital.

- ***Vishing:*** El término vishing es una combinación de las palabras voice (voz) y phishing, por lo que también se denomina en ocasiones voice phishing. Con esta técnica, los atacantes usan la tecnología VoIP (voz sobre IP) para realizar de forma asequible o gratuita numerosas llamadas fraudulentas y conseguir así códigos, contraseñas o datos bancarios de la víctima, que no suele sospechar nada.

- ***Smising:*** El término smishing surge de unir los elementos SMS y phishing. De manera similar al phishing, los ciberdelincuentes que envían estos mensajes se hacen pasar por representantes de una empresa u organización fiable, solo que, en lugar de correos electrónicos, utilizan SMS (Short Message Service). Estos mensajes de móvil sirven, o bien para instar a la víctima a revelar datos de su cuenta, o bien para instalar malware y troyanos en su dispositivo sin que se percate.

- ***Pharming:*** El pharming, una combinación de las palabras "phishing" y "farming", es una estafa en línea similar al phishing, en la que se manipula el tráfico de un sitio web y se roba información confidencial. Este es un tipo de ciberataque de ingeniería social en el que los delincuentes redirigen a los usuarios que intentan acceder a un sitio web específico a un sitio diferente y falso. Estos sitios "falsos" pretenden capturar la información de identificación personal de la víctima y sus credenciales de inicio de sesión, como contraseñas, números de la seguridad social, números de cuenta, etc. o bien intentan instalar malware de pharming en su equipo.

- ***Whaling:*** Un ataque de whaling es un método que usan los cibercriminales para simular ocupar cargos de nivel superior en una organización y así atacar directamente a los altos ejecutivos u otras personas importantes dentro de ella, con el objeto de robar dinero, conseguir información confidencial u obtener acceso a sus sistemas informáticos con fines delictivos. El whaling, también conocido como CEO fraud, es similar al phishing en cuanto a que usa métodos, como la suplantación de sitios web y correos electrónicos, para engañar a la víctima y hacer que revele información confidencial o haga transferencias de dinero, entre otras acciones.

Lamentamos mucho esta situación que nos ha sobrevenido, pero sepa que para nosotros su tranquilidad es lo primero y hemos atajado y contenido esta situación de una forma rápida y eficaz.

Prinsotel ya se encuentra trabajando en el plan de acción generado tras el incidente y, en concreto, en la implantación de medidas de seguridad reforzadas para evitar situaciones similares en el futuro.