CSIRT

Equipo de Respuesta ante Incidentes de Seguridad Informática

Resumen ciberataque que afectó a sistema aeronáutico provisto por **SITA**

Santiago, 7 de enero de 2021

TLP: BLANCO

Ministerio del Interior y Seguridad Pública

Gobierno de Chile

Nota

La información consignada en el presente informe es producto del análisis de múltiples fuentes, de terceras partes e investigación propia del equipo CSIRT. La información contenida en los informes o comunicados está afecta a actualizaciones.

Este informe fue clasificado como TLP BLANCO. La información puede ser distribuida sin restricciones.

Contenido

1. Resumen ejecutivo

Este resumen de ciberataques, vulnerabilidades e incidentes de seguridad cibernética tiene como propósito destacar algunos eventos acaecidos en días pasados para que puedan ser interpretados y discutidos por las diferentes entidades que tengan acceso a su lectura.

Este informe reúne los antecedentes conocidos hasta el día de su publicación, referentes al ataque que afectó a la plataforma SITA PSS, la cual es usada por numerosas líneas aéreas, y que resultó en una brecha informatica que tuvo como consecuencia la exfiltración de datos de pasajeros pertenecientes a programas de fidelización de varias de éstas. La brecha fue reconocida por SITA el 3 de marzo, pero el ataque habría sucedido durante el mes anterior.

La información consignada en el presente documento es catalogada como TLP BLANCO.

2. Detalles de la alerta

El jueves 4 de febrero de 2021, SITA, firma proveedora de servicios de comunicación y tecnología de información para la industria aérea, informó en su sitio web el haber sufrido un ciberataque "altamente sofisticado", que derivó en un incidente de seguridad teniendo como consecuencia la exfiltración de datos desde los servidores en que se almacena su servicio SITA Passenger Service System (PSS).

La empresa agregó haber confirmado la gravedad del ataque el 24 de febrero de 2021, y de haber tomado contacto inmediatamente con todos los clientes de SITA PSS y organizaciones relacionadas.

SITA no entregó ningún otro detalle sobre la naturaleza del ataque o el vector de entrada a los sistemas, el que había sido informado ya por Singapore Airlines el día anterior (3 de marzo).

Varias aerolíneas afectadas informaron (en forma separada cada una de ellas) a la prensa y a sus clientes sobre el ataque. Algunas de las firmas que han revelado ser parte de la brecha de seguridad en los sistemas de SITA son American Airlines, British Airways, Lufthansa, Air New Zealand, Finnair, Singapore Airlines, Malaysia Airlines, Aegean y Jeju Air.

Lufthansa señaló que la exfiltración de datos ocurrió entre el 21 de enero y el 11 de febrero.

Estas empresas aseguran que el incidente no tuvo lugar en sus propios sistemas, sino que la afectación se verifico en los servidores de SITA PSS. Firmas como Air New Zealand y Singapore Airlines señalaron que los datos exfiltrados son nombres de clientes, status en sus programas de viajero frecuente y número de membresía, además de en algunos casos sus preferencias al viajar, como asiento y comidas, pero que no se filtraron datos de contraseñas, reservaciones, información de contacto o tarjetas de crédito o débito.

Con todo, algunas empresas recomendaron a sus clientes cambiar sus credenciales de acceso a sus portales web, pese a que señalaron que esa información no es intercambiada con SITA.

Las líneas aéreas explicaron que la información afectada corresponde a datos de sus clientes de programas de viajero frecuente, y si bien, algunas líneas aéreas no son clientes directos del sistema de servicios al pasajero de SITA, si lo son de las alianzas Oneworld y Star Alliance, en donde comparten con SITA información de los viajeros frecuentes .

Latam Airlines, la aerolínea con más clientes en nuestro país, actualmente no pertenece a ninguna de estas alianzas, habiendo dejado de pertenecer a Oneworld en 2020, pero sin perjuicio de ellos las declaraciones consignan que en el incidente se habría tenido acceso a datos del año 2010 al 2019.

3. Recomendaciones

Junto con las mitigaciones y recomendaciones entregadas por SITA y las aerolíneas a los clientes afectados, el CSIRT de Gobierno solicita considerar otras medidas preventivas, como:

- Mantenerse al tanto de cualquier información proveniente de SITA o líneas aéreas en relación con la obtención de más detalles sobre el ataque realizado.
- Si se es miembro de programas de viajero frecuente de cualquiera de las aerolíneas que han reconocido ser afectadas, o de otras pertenecientes a Star Alliance o Oneworld, se recomienda cambiar las contraseñas con las que se está registrado en la plataforma de las empresas.

4. Enlaces

https://www.sita.aero/pressroom/

https://www.iata.org/en/pressroom/

CSIRT Gobierno de Chile

Firmado digitalmente por CSIRT Gobierno de Chile
Fecha: 2021.03.07 00:11:47 -03'00'