AIRNITE

ZERO DAY

NÚMERO 07/2026 · SEGURIDAD INFORMÁTICA

Facturación con boli y lista: lo que enseña el ataque al software aeroportuario MUSE

En septiembre de 2025, un incidente de ransomware en un proveedor paralizó el software de facturación de varios aeropuertos europeos. Los pasajeros se facturaron a mano. Qué enseña sobre la dependencia de los proveedores.

Publicado: 21 de noviembre de 2026 Tiempo de lectura: 6 min Autor: Redacción de Airnite

SOFTWARE. SECURITY. CODE.

// LA SITUACIÓN EN CIFRAS

19/09/2025
incidente detectado
según la comunicación de RTX a la SEC de EE. UU.

Ransomware
tipo de incidente
en sistemas que dan soporte a MUSE (RTX, formulario 8-K)

manual
facturación en aeropuertos
los clientes pasaron a procesos de respaldo o manuales (RTX)

no significativo
impacto financiero para RTX
según su propia valoración en el 8-K del 24/09/2025

En septiembre de 2025, las aerolíneas de varios aeropuertos europeos, entre ellos Bruselas, Berlín y Londres-Heathrow, tuvieron que pasar al modo manual. Hubo vuelos retrasados y cancelados. La causa no estaba en los propios aeropuertos, sino en un proveedor.

// ¿Qué ha pasado?

Según una comunicación a la autoridad bursátil estadounidense SEC, el grupo **RTX**, propietario de Collins Aerospace, detectó el **19 de septiembre de 2025** un incidente de ciberseguridad con **ransomware** en sistemas que dan soporte a su software de procesamiento de pasajeros **MUSE**. MUSE permite que varias aerolíneas compartan mostradores de facturación y puertas de embarque, incluida la gestión de equipajes.

RTX escribe que sus clientes pasaron a **procesos de respaldo o manuales** y sufrieron retrasos y cancelaciones. La empresa activó su plan de respuesta a incidentes e informó a las autoridades policiales nacionales e internacionales. Según la agencia Reuters, entre los aeropuertos afectados estaban Londres-Heathrow, Bruselas y Berlín; la agencia europea de ciberseguridad ENISA confirmó, según esa información, que se trataba de ransomware.

// ¿Cómo funciona el ataque?

El ransomware cifra los sistemas y los deja inservibles; los autores suelen exigir un rescate por descifrarlos o amenazan con publicar datos robados. RTX no indicó en su comunicación quién estaba detrás ni cómo entraron los atacantes; investigadores como Acronis consideran la autoría sin aclarar.

Un dato de la comunicación de RTX llama la atención: los sistemas MUSE de los aeropuertos funcionan **fuera de la red corporativa de RTX**, en redes propias de cada cliente. El incidente afectó, por tanto, a una plataforma especializada de la que dependen muchos clientes a la vez. Si cae, caen todos los usuarios al mismo tiempo: un riesgo de concentración clásico.

// ¿A quién afecta?

Afectó a los aeropuertos y aerolíneas que usan MUSE y, con ellos, a sus pasajeros. En lo financiero, RTX califica el incidente en su comunicación como **no significativo** para el grupo. Para los clientes fue distinto: tuvieron que pasar con urgencia al papel y al trabajo manual.

El patrón vale para cualquier empresa que externalice procesos clave en un proveedor: cajas, gestión de stock, contabilidad, reserva de citas, logística. Su propia informática puede estar perfectamente protegida: si el proveedor cae, la actividad se detiene igual. La nueva legislación NIS2 aborda expresamente estos riesgos de la cadena de suministro.

// ¿Qué hay que hacer ahora?

La principal lección del incidente MUSE: un modo de emergencia solo funciona si está preparado. Los aeropuertos pudieron seguir trabajando porque existían procedimientos manuales. Las empresas deben saber qué sistemas externos son críticos para ellas, cómo trabajar sin ellos y cuánto tiempo aguantarían. Eso incluye documentación de emergencia en papel, procedimientos ensayados y acuerdos claros con el proveedor. La lista de control de abajo resume los pasos.

// ¿Cómo ayuda Airnite?

En la **consultoría**, Airnite elabora con usted un inventario de sus proveedores críticos y un plan de emergencia práctico. En la **formación** y los simulacros, sus equipos ensayan el modo de emergencia antes de necesitarlo. Con **pruebas de penetración** revisamos las conexiones entre su red y los sistemas de sus proveedores.

> Nota: los datos sobre aeropuertos concretos y sobre ENISA proceden de informaciones de agencia; no pudimos consultar directamente los comunicados de los aeropuertos. Estado de la investigación: 21 de noviembre de 2026.

Lista de control: qué hacer ahora

[+] Enumere todos los proveedores y plataformas de software sin los que su actividad se detiene y valore su importancia.

[+] Defina un modo de emergencia para cada servicio crítico: ¿cómo seguiría trabajando de uno a tres días sin él?

[+] Guarde la documentación de emergencia (listas, formularios, contactos) sin conexión y a mano, también en papel.

[+] Acuerde por contrato con los proveedores estándares de seguridad, obligación de notificar incidentes y tiempos de recuperación.

[+] Ensaye el modo de emergencia al menos una vez al año con todos los equipos implicados.

[+] Prepare la comunicación: quién informa a clientes, plantilla y autoridades, y por qué canales.

Cómo ayuda Airnite

- Consultoría – Una mirada externa sobre sus planes y proyectos.
- Formación – Su equipo aprende nuestras herramientas y procesos.
- Pruebas de penetración y seguridad – Ataques controlados con un informe claro y un plan de medidas.

¿Qué pasa si falla su proveedor más importante?

Airnite analiza con usted qué sistemas externos son críticos para su actividad, cómo le afectaría una caída y cómo puede ser un modo de emergencia. Revisamos los requisitos de seguridad de los contratos y ensayamos la crisis con su equipo antes de que ocurra.

Solicitar una primera conversación · Escribir un correo · Por WhatsApp

Contacto

¿Preguntas sobre este artículo? Escríbanos por WhatsApp: +49 174 6834842

Leer en línea: https://airnite.de/es/revista/collins-aerospace-muse-aeropuertos-ransomware/

Fuentes

Cada dato de este artículo se basa en las fuentes indicadas a continuación. Las fuentes primarias están señaladas.

1. **RTX Corporation · Form 8-K (Item 8.01), SEC EDGAR** · 24/09/2025 (hecho del 19/09/2025) · FUENTE PRIMARIA
   Fuente primaria: ransomware en MUSE, funcionamiento manual en los clientes, retrasos y cancelaciones, sin impacto financiero significativo
   https://www.sec.gov/Archives/edgar/data/101829/000010182925000036/rtx-20250919.htm
2. **Insurance Journal (Reuters) · Europe Air Travel Snarls Continue After Cyberattack** · 22/09/2025
   Agencia de noticias: aeropuertos afectados, confirmación del ransomware por ENISA
   https://www.insurancejournal.com/news/international/2025/09/22/839936.htm
3. **Acronis Threat Research Unit · ARINC's MUSE disruption impacts flights across Europe** · 2025
   Investigación de seguridad: análisis, autoría sin aclarar
   https://www.acronis.com/en-us/tru/posts/arincs-common-use-passenger-processing-system-muse-disruption-impacts-flights-across-europe/

Información editorial general, no constituye asesoramiento jurídico ni una evaluación de sus sistemas concretos. Vigencia: fecha de publicación.

Airnite GmbH · Am Waldbach 7 · 77654 Offenburg · airnite.de