AIRNITE

ZERO DAY

ISSUE 07/2026 · IT SECURITY

Check-in with pen and list: what the attack on the MUSE airport software teaches

In September 2025, a ransomware incident at a service provider crippled the check-in software of several European airports. Passengers were checked in by hand. What companies can learn about dependence on service providers.

Published: 21 November 2026 Reading time: 6 min Author: Airnite editorial team

SOFTWARE. SECURITY. CODE.

// THE SITUATION IN NUMBERS

19 Sep 2025
incident detected
according to RTX's filing with the US SEC

Ransomware
type of incident
on systems supporting MUSE (RTX, Form 8-K)

manual
check-in at airports
customers switched to back-up or manual processes (RTX)

not material
financial impact on RTX
according to its own assessment in the 8-K of 24 Sep 2025

In September 2025, airlines at several European airports, including Brussels, Berlin and London Heathrow, had to switch to manual operation. Flights were delayed or cancelled. The cause did not lie with the airports themselves but with a service provider.

// What happened?

According to a filing with the US Securities and Exchange Commission, **RTX**, the group that owns Collins Aerospace, became aware on **19 September 2025** of a cyber security incident involving **ransomware** on systems that support its **MUSE** passenger processing software. MUSE allows several airlines to share check-in desks and gates at airports, including baggage handling.

RTX writes that customers switched to **back-up or manual processes** and experienced delays and cancellations. The company activated its incident response plan and notified law enforcement at home and abroad. According to the news agency Reuters, the affected airports included London Heathrow, Brussels and Berlin; the EU cyber security agency ENISA reportedly confirmed that ransomware was involved.

// How does the attack work?

Ransomware encrypts systems and renders them unusable; the perpetrators often demand a ransom for decryption or threaten to publish stolen data. RTX did not disclose in its filing who was behind this incident or how the attackers got in; security researchers such as Acronis describe the attribution as open.

One detail of the RTX filing stands out: the MUSE systems at the airports run **outside the RTX corporate network**, on customer-specific networks. The incident therefore hit a specialised platform on which many customers depend at the same time. If it fails, all users fail at once – a classic concentration risk.

// Who is affected?

Airports and airlines using MUSE were affected, and with them their passengers. Financially, RTX classifies the incident in its filing as **not material** to the group. For the customers it looked different: they had to switch to paper and manual work at short notice.

The pattern applies to every company that outsources core processes to a service provider: point-of-sale systems, inventory management, accounting, appointment booking, logistics. Your own IT can be perfectly protected – if the provider fails, operations still stop. The new NIS2 legislation explicitly addresses exactly these supply chain risks.

// What should you do now?

The most important lesson from the MUSE incident: a fallback mode only works if it is prepared. The airports could keep operating because manual processes existed. Companies should know which external systems are critical to them, how they would work without them and how long that would last. This includes emergency documents on paper, rehearsed procedures and clear agreements with the service provider. The checklist below sums up the steps.

// How does Airnite help?

In **consulting**, Airnite works with you to create an overview of your critical service providers and a practical emergency plan. In **training** and exercises, your teams rehearse the fallback mode before it is needed. With **penetration tests**, we check the connections between your network and your service providers' systems.

> Note: information on individual airports and ENISA comes from news agency reports; we were unable to view the airports' own statements directly. Research status: 21 November 2026.

Checklist: what to do now

[+] List all service providers and software platforms without which your operations stop, and assess their importance.

[+] Define a fallback mode for each critical service: how do you keep working for one to three days without it?

[+] Keep emergency documents (lists, forms, contact details) offline and to hand – on paper too.

[+] Agree contractually with service providers on security standards, incident notification duties and recovery times.

[+] Rehearse the fallback mode at least once a year with all teams involved.

[+] Prepare communications: who informs customers, staff and authorities, and through which channels?

How Airnite helps

- Consulting – An outside view of your plans and projects.
- Training – Your team learns our tools and processes.
- Penetration Testing & Security – Controlled attacks with a clear report and action plan.

What happens if your most important service provider fails?

Airnite works with you to analyse which external systems are critical to your operations, how an outage would hit you and what a fallback mode can look like. We check contracts for security requirements and rehearse the emergency with your team – before it happens.

Request an initial call · Send an email · Via WhatsApp

Contact

Questions about this article? Message us on WhatsApp: +49 174 6834842

Read online: https://airnite.de/en/magazine/collins-aerospace-muse-airports-ransomware/

Sources

Every fact in this article is based on the sources below. Primary sources are marked.

1. **RTX Corporation · Form 8-K (Item 8.01), SEC EDGAR** · 24 Sep 2025 (event 19 Sep 2025) · PRIMARY SOURCE
   Primary source: ransomware incident at MUSE, manual operation at customers, delays and cancellations, no material financial impact
   https://www.sec.gov/Archives/edgar/data/101829/000010182925000036/rtx-20250919.htm
2. **Insurance Journal (Reuters) · Europe Air Travel Snarls Continue After Cyberattack** · 22 Sep 2025
   News agency: affected airports, ENISA confirmation of ransomware
   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
   Security research: assessment, open questions on attribution
   https://www.acronis.com/en-us/tru/posts/arincs-common-use-passenger-processing-system-muse-disruption-impacts-flights-across-europe/

General editorial information, not legal advice and not an assessment of your individual systems. Status: date of publication.

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