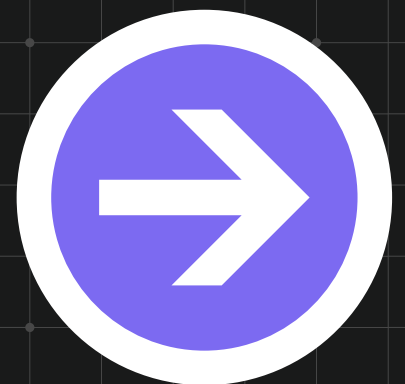


European Airports Cyberattack:

What You Need to Know



www.getastra.com

SWIPE

What Happened?

On September 19, 2025, a cyberattack targeted the MUSE system used across several airports. The system is responsible for check-in desks, boarding gates, and baggage operations. Its sudden outage forced airlines and airports to scramble, leading to widespread service interruptions.

www.getastra.com

SWIPE

Impacted Airports & Passengers

Airports in Heathrow, Brussels, Berlin, and Dublin were among the worst affected. With electronic check-in and baggage drop unavailable, staff had to revert to manual processes. Passengers experienced delays ranging from 30 to 90 minutes, and in some cases, flights were cancelled altogether.

The Weak Link: MUSE

MUSE, or the Multi-User System Environment, is a common-use platform shared across multiple airlines and terminals. This efficiency comes with a cost: it creates a single point of failure. When MUSE was compromised, the effects cascaded across all dependent airports simultaneously, amplifying the disruption.

Why It Matters ?

The incident highlights the hidden risks of supply chain dependencies in aviation. Airports are critical infrastructure, and under regulations like the EU's NIS2 directive, such disruptions raise questions about resilience. The attack revealed how over-reliance on third parties, insufficient redundancy, and lack of robust contingency planning can cause both operational and reputational damage.

How it happened?

The exact technical details of the attack have not been disclosed yet, but reports confirm it was a cyber-related disruption targeting Collins Aerospace's MUSE system. Since MUSE is a centralized, common-use platform for check-in and boarding, attackers only needed to compromise this one system to create a cascading impact across multiple airports.

Experts suggest it could have been caused by malware, ransomware, or even a supply chain compromise within the software or its supporting infrastructure.

Astra Security

This case is a strong reminder that third-party systems are part of an organization's attack surface. Security leaders must build resilience by ensuring backup systems and manual fallbacks are ready to go. Regular red-team exercises and supply chain risk assessments can help prepare for such incidents. Ultimately, this attack reinforces the fact that organizational security is only as strong as its weakest vendor.