AIRNITE

ZERO DAY

NUMÉRO 07/2026 · SÉCURITÉ INFORMATIQUE

L’enregistrement au stylo : ce que nous apprend l’attaque contre le logiciel aéroportuaire MUSE

En septembre 2025, un rançongiciel chez un prestataire a paralysé le logiciel d’enregistrement de plusieurs aéroports européens. Les passagers ont été enregistrés à la main. Les leçons sur la dépendance aux prestataires.

Publié le: 21 novembre 2026 Temps de lecture: 6 min Auteur: Rédaction Airnite

SOFTWARE. SECURITY. CODE.

// LA SITUATION EN CHIFFRES

19/09/2025
incident détecté
selon la déclaration de RTX à la SEC américaine

Rançongiciel
type d'incident
sur des systèmes supportant MUSE (RTX, formulaire 8-K)

manuel
enregistrement dans les aéroports
les clients sont passés en mode de secours ou manuel (RTX)

non significatif
impact financier pour RTX
selon sa propre évaluation dans le 8-K du 24/09/2025

En septembre 2025, des compagnies aériennes ont dû passer en mode manuel dans plusieurs aéroports européens, dont Bruxelles, Berlin et Londres-Heathrow. Des vols ont été retardés ou annulés. La cause ne se trouvait pas dans les aéroports eux-mêmes, mais chez un prestataire.

// Que s'est-il passé ?

Selon une déclaration à l'autorité boursière américaine SEC, le groupe **RTX**, propriétaire de Collins Aerospace, a constaté le **19 septembre 2025** un incident de cybersécurité impliquant un **rançongiciel** sur des systèmes supportant son logiciel de traitement des passagers **MUSE**. MUSE permet à plusieurs compagnies de partager les comptoirs d'enregistrement et les portes d'embarquement, y compris le traitement des bagages.

RTX écrit que ses clients sont passés en **mode de secours ou manuel** et ont subi des retards et des annulations. L'entreprise a activé son plan de réponse aux incidents et informé les autorités judiciaires nationales et internationales. Selon l'agence Reuters, les aéroports touchés comprenaient Londres-Heathrow, Bruxelles et Berlin ; l'agence européenne de cybersécurité ENISA aurait confirmé qu'il s'agissait d'un rançongiciel.

// Comment fonctionne l'attaque ?

Un rançongiciel chiffre les systèmes et les rend inutilisables ; les auteurs exigent souvent une rançon pour le déchiffrement ou menacent de publier des données volées. RTX n'a pas indiqué dans sa déclaration qui se trouvait derrière l'incident ni comment les attaquants étaient entrés ; des chercheurs comme Acronis jugent l'attribution ouverte.

Un détail de la déclaration de RTX retient l'attention : les systèmes MUSE des aéroports fonctionnent **en dehors du réseau d'entreprise de RTX**, sur des réseaux propres aux clients. L'incident a donc frappé une plateforme spécialisée dont dépendent de nombreux clients en même temps. Si elle tombe, tous les utilisateurs tombent à la fois – un risque de concentration typique.

// Qui est concerné ?

Les aéroports et compagnies utilisant MUSE étaient touchés, et avec eux leurs passagers. Sur le plan financier, RTX qualifie l'incident de **non significatif** pour le groupe dans sa déclaration. Pour les clients, c'était autre chose : ils ont dû basculer en urgence sur le papier et le travail manuel.

Ce schéma concerne toute entreprise qui confie des processus essentiels à un prestataire : caisses, gestion des stocks, comptabilité, prise de rendez-vous, logistique. Votre propre informatique peut être parfaitement protégée – si le prestataire tombe, l'activité s'arrête quand même. La nouvelle législation NIS2 vise

expressément ces risques liés à la chaîne d'approvisionnement.

// Que faire maintenant ?

La principale leçon de l'incident MUSE : un mode dégradé ne fonctionne que s'il est préparé. Les aéroports ont pu continuer parce que des procédures manuelles existaient. Les entreprises doivent savoir quels systèmes externes sont critiques pour elles, comment travailler sans eux et combien de temps cela tient. Cela inclut des documents d'urgence sur papier, des procédures exercées et des accords clairs avec le prestataire. La check-list ci-dessous résume les étapes.

// Comment Airnite vous aide-t-il ?

En **conseil**, Airnite établit avec vous l'inventaire de vos prestataires critiques et un plan d'urgence opérationnel. En **formation** et lors d'exercices, vos équipes s'entraînent au mode dégradé avant d'en avoir besoin. Avec des **tests d'intrusion**, nous vérifions les connexions entre votre réseau et les systèmes de vos prestataires.

> Remarque : les informations sur les aéroports et l'ENISA proviennent de dépêches d'agence ; nous n'avons pas pu consulter directement les déclarations des aéroports. État de la recherche : 21 novembre 2026.

Check-list : ce qu'il faut faire maintenant

[+] Lister tous les prestataires et plateformes logicielles sans lesquels votre activité s'arrête, et évaluer leur importance.

[+] Définir un mode dégradé pour chaque service critique : comment continuer à travailler un à trois jours sans lui ?

[+] Conserver les documents d'urgence (listes, formulaires, contacts) hors ligne et à portée de main – aussi sur papier.

[+] Encadrer contractuellement avec les prestataires les standards de sécurité, l'obligation de signaler les incidents et les délais de reprise.

[+] Exercer le mode dégradé au moins une fois par an avec toutes les équipes concernées.

[+] Préparer la communication : qui informe clients, collaborateurs et autorités, par quels canaux ?

Comment Airnite vous aide

- Conseil – Un regard extérieur sur vos projets.
- Formations – Votre équipe apprend nos outils et méthodes.
- Tests d'intrusion et sécurité – Attaques contrôlées avec rapport clair et plan d'action.

Que se passe-t-il si votre principal prestataire tombe en panne ?

Airnite analyse avec vous quels systèmes externes sont critiques pour votre activité, comment une panne vous toucherait et à quoi peut ressembler un mode dégradé. Nous vérifions les exigences de sécurité dans les contrats et répétons la crise avec votre équipe – avant qu'elle ne survienne.

Demander un premier échange · Écrire un e-mail · Par WhatsApp

Contact

Des questions sur cet article ? Écrivez-nous sur WhatsApp : +49 174 6834842

Lire en ligne: https://airnite.de/fr/magazine/collins-aerospace-muse-aeroports-ransomware/

Sources

Chaque fait de cet article repose sur les sources ci-dessous. Les sources primaires sont signalées.

1. **RTX Corporation · Form 8-K (Item 8.01), SEC EDGAR** · 24/09/2025 (événement du 19/09/2025) · SOURCE PRIMAIRE
   Source primaire : rançongiciel sur MUSE, fonctionnement manuel chez les clients, retards et annulations, pas d'impact financier significatif
   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
   Agence de presse : aéroports touchés, confirmation du rançongiciel par l'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
   Recherche en sécurité : analyse, questions ouvertes sur l'attribution
   https://www.acronis.com/en-us/tru/posts/arincs-common-use-passenger-processing-system-muse-disruption-impacts-flights-across-europe/

Information éditoriale générale, sans conseil juridique ni examen individuel de vos systèmes. État : date de publication.

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