REPUBLIKA E SHQIPËRISË
AUTORITETI KOMBËTAR PËR SIGURINË KIBERNETIKE
DREJTORIA E ANALIZËS SË SIGURISË KIBERNETIKE

Situata aktuale e sulmeve kibernetike në aeroportet europiane

Versioni: 1.0
Datë: 22/09/2025

PËRMBAJTJA

Përmbledhje ekzekutive

Së fundmi, sektorit të aviacionit i është vënë re një përshpejtim i ndjeshëm i sulmeve kibernetike, me incidente të mëdha operative që prekin sisteme kritike si shërbimet e check-in, menaxhimin e bagazheve dhe ekranet e informacionit të fluturimeve. Ngjarjet e fundit që goditën aeroporte të mëdha evropiane nënvizojnë rrezikun e varësisë nga ofruesit e palëve të treta (Supply chain).

Gjatë ditëve 20-21 shtator 2025, një sulm kibernetik akoma i pakategorizuar, ka goditur sisteme që përdoren për check-in dhe dorëzimin e bagazheve, duke shkaktuar vonesa dhe anulime në aeroportet e mëdha evropiane, përfshirë *Heathrow* (Londër), *Zaventem* (Bruksel) dhe aeroportin e Berlinit. Sulmi ka prekur softuerin *Muse* të kompanisë *Collins Aerospace*, i cili ofron shërbime të desk-it të check-in për disa linja ajrore dhe aeroportet. Collins Aerospace [1](një njësi e grupit RTX) konfirmoi se po merret me një "incident të lidhur me sigurinë kibernetike" dhe po punonte për rikthimin e shërbimeve; autoritetet kombëtare të sigurisë kibernetike dhe forcat e rendit janë të përfshira në hetim. Aeroportet u janë drejtuar pasagjerëve që të verifikojnë statusin e fluturimeve përpara udhëtimit.

Në Aeroportin e Brukselit, sulmi kibernetik çoi në anulimin e rreth gjysmës së fluturimeve të planifikuara për një ditë, duke shkaktuar vonesa të gjata për qytetarët. Fluturimet u vonuan me orë të tëra dhe disa prej tyre u shtynë plotësisht.

[1] https://www.theguardian.com/business/2025/sep/21/delays-continue-at-heathrow-brussels-and-berlin-airports-after-alleged-cyber-attack

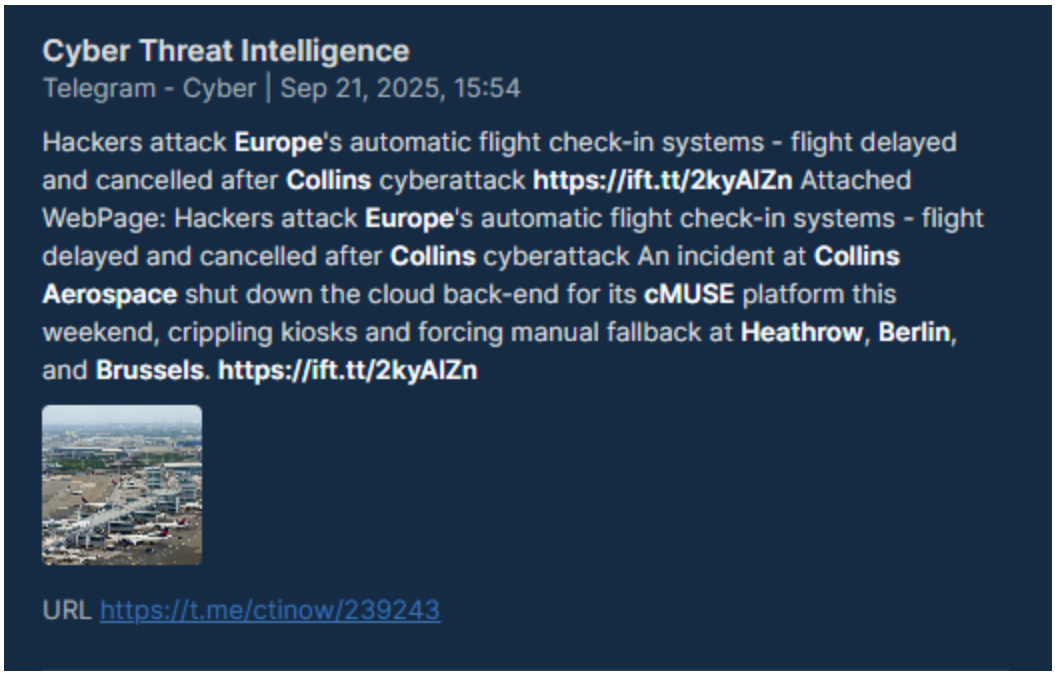

Figura 1: Informacione nga inteligjenca kibernetike

Në total, janë prekur disa aeroporte kryesore evropiane, duke shkaktuar një zinxhir vonesash dhe anulimesh që ndikuan qindra fluturime: sipas të dhënave të ndryshme mediatike, *Flightradar24* raportoi rreth 629 fluturime të prekura përgjatë valës së ndërprerjeve. Në *Heathrow(Londër)* u regjistruan vonesa në rreth 90% të mbi 350 fluturimeve me një mesatare rreth 34 minutash. Në Bruksel u anuluan 25 nisje të shtunën (datë 20 shtator), 50 të dielën (datë 21 shtator) dhe autoritetet i kërkuan linjave të anulojnë rreth 140 nisje për të hënën (përgjithësisht rreth gjysmës së nisjeve të planifikuara atë ditë).[2]

[2] https://www.independent.co.uk/news/uk/home-news/heathrow-brussels-berlin-airport-cyber-attack-delays-b2830693.html

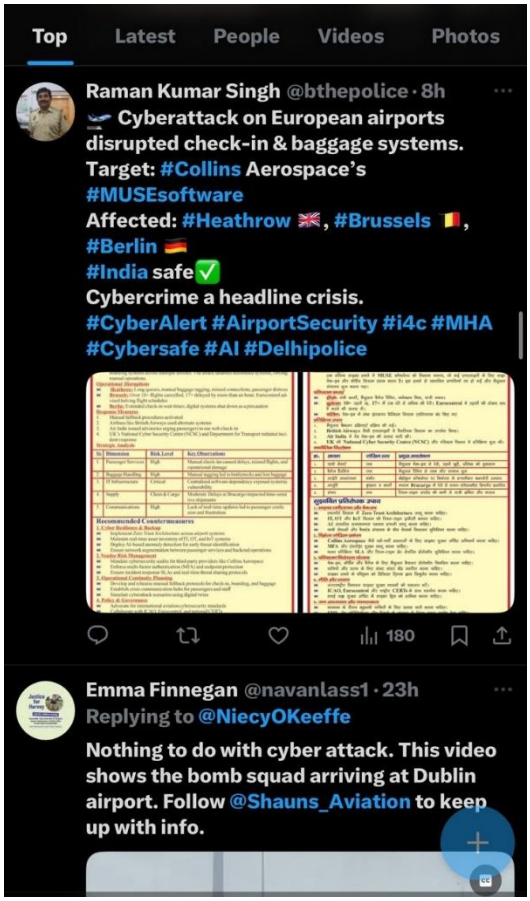

Figura 2: Komunikime në rrjetin X

Në të njëjtën periudhë, raporte të tjera treguan incidente kibernetike ndaj subjekteve në Rusi: ndërmarrje dhe faqe aeroportesh si *Pulkovo* (Shën Petersburg) dhe probleme operative të disa linja rajonale (Raporti i Recorded Future / The Record). Këto incidente janë raportuar si të ndara nga ngjarjet e Evropës perëndimore, por tregojnë një valë të zgjatur të sulmeve ndaj infrastrukturave të aeroporteve.

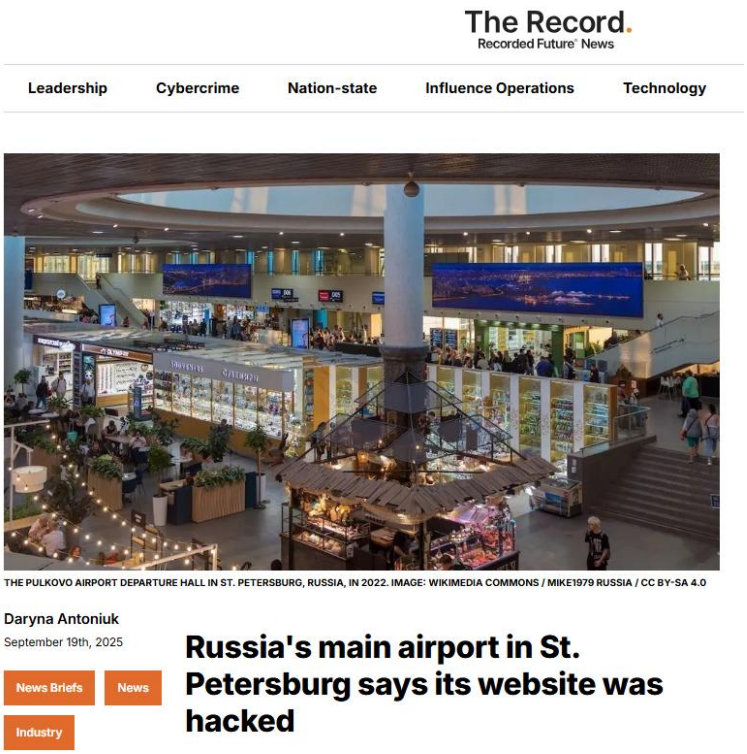

Figura 3: Ngjarjet në Rusi

Sa e prekshme mund të jetë Shqipëria?

Shqipëria si vend i vogël me një infrastrukturë aeroportuale të centralizuar (Rinas/Tiranë kryesisht, plus aeroporti i Kukësit dhe porte të tjera të vogla) nuk është imun ndaj efekteve të këtyre ngjarjeve. Ndikimi konkret varet nga dy faktorë kryesorë:
Përdorimi i të njëjtave palë të treta/furnitorë — Nëse operatorët shqiptarë (aeroportet ose linjat ajrore që fluturojnë në/së nga Shqipëria) përdorin të njëjtat zgjidhje që u goditën (ose softuerë të ngjashëm të palëve të treta), rreziku për ndërprerje lokale rritet.

Aeroportet më të vogla kanë burime njerëzore dhe procese manuale të kufizuara; një ndërprerje e sistemeve të check-in mund të shkaktojë bllokime të vazhdueshme, veçanërisht kur ka fluturime ndërkombëtare të koordinuara me linja të mëdha. Gjithashtu kapacitetet në fushën e sigurisë kibernetike janë të limituara. Po ashtu dhe mjetet teknologjike duhet të jenë nga më të avancuarat deri në aplikimin e parimit Zero Trust për të mos u prekur ndaj sulmeve *Supply Chain.*

Për Shqipërinë, prioritet është verifikimi i furnitorëve, përgatitja e procedurave të reagimit ndaj incidenteve kibernetike, forcimi i koordinimit kombëtar për menaxhim incidentesh, raportimi i incidenteve drejt Autoritetit Kombëtar për Sigurinë Kibernetike.

Referenca

1. https://www.cnbc.com/amp/2025/09/21/what-we-know-about-the-cyberattack-that-hit-major-european-airports.html
2. https://www.bbc.com/news/articles/cwy88857llno.amp
https://www.theguardian.com/business/2025/sep/21/delays-continue-at-heathrow-brussels-and-

berlin-airports-after-alleged-cyber-attack
3. https://www.balkanweb.com/aeroportet-ne-berlin-dhe-bruksel-goditen-nga-nje-sulm-kibernetik/#gsc.tab=0
4. https://therecord.media/russia-krasavia-airline-disrupted-suspected-cyberattack
   https://therecord.media/russia-pulkovo-airport-st-petersburg-website-hacked
5. https://euronews.al/sulmi-kibernetik-prek-aeroportin-e-brukselit-anulohen-disa-fluturime/
6. https://www.independent.co.uk/news/uk/home-news/heathrow-brussels-berlin-airport-cyber-attack-delays-b2830693.html