DM. De Morgen

De Morgen WEBSITE 23/09/2025 - 03:00

Van check-in tot grenscontrole: waarom hack bij één toeleverancier Brussels Airport zo zwaar treft

Ook dinsdag zullen nog 10 procent van de vluchten vanuit Zaventem niet vertrekken. Drie dagen nadat een cyberaanval het check-insysteem lamlegde, is de situatie nog altijd niet onder controle. ‘Cybercriminelen weten: valt één systeem uit, dan ligt meteen de hele luchthaven plat.’

Dat het precies Collins Aerospace, de Amerikaanse leverancier van check-in- en bagagesoftware, is dat nu opnieuw getroffen wordt, roept vraagtekens op. In 2023 circuleerden al berichten dat het bedrijf slachtoffer was van ransomware. Toen bleef de impact beperkter en doken er geen gegevens op.

“Twee keer in zo’n korte tijd, dat zie je niet vaak”, merkt Geert Baudewijns van cybersecuritybedrijf Secutec op. “Het onderstreept dat dit soort aanvallen niet uitzonderlijk meer zijn, maar structureel. Al zien we de laatste jaren wel een stagnatie. Vooral grote bedrijven zijn nu veel beter beveiligd.”

De aanval begon vrijdagavond. Het gevolg was meteen voelbaar in verschillende Europese luchthavens, waaronder ook Londen, Dublin en Berlijn. Zaterdag moesten in Brussel 25 vertrekkende vluchten worden geschrapt, zondag 50. Voor maandag vroeg de luchthaven de helft van de 277 geplande vertrekken te annuleren, maar uiteindelijk bleven de gevolgen beperkt: 40 vluchten werden effectief geschrapt, naast tientallen vertragingen.

“We gebruiken alternatieve systemen, laptops en iPads, en online check-in waar mogelijk”, zegt woordvoerster Ihsane Chioua Lekhli van Brussels Airport. Passagiers krijgen het advies om de volgende dagen te controleren of hun vlucht niet geannuleerd is en om zeker op tijd te komen — twee uur voor Schengen- en drie uur voor niet-Schengen-vluchten. Lekhli: “We doen er alles aan om vluchten te laten doorgaan. Maar hoelang het nog duurt voordat alles weer normaal verloopt, is niet duidelijk.”

Voor reizigers is er doorgaans recht op terugbetaling of herboeking door de luchtvaartmaatschappijen, maar geen schadevergoeding omdat het hier gaat over overmacht.

Volgens Geert Baudewijns van Secutec zijn er maar twee uitwegen. “Back-ups zijn doorgaans gemaakt om één of twee servers te herstellen, niet honderden tegelijk. Dat kost vier tot zes uur per server. En keer je terug naar een moment vóór de aanval, dan bestaat het risico dat het virus gewoon opnieuw meekomt. Dat is dus niet opportuun.”

De andere optie is onderhandelen. Baudewijns heeft zelf al in naam van 550 bedrijven in de hele wereld zulke onderhandelingen gevoerd met cybercriminelen. “Je koopt de decryptiesleutels en kan opnieuw werken. Dat gebeurt vaker dan men denkt. Wij hebben wereldwijd al meer dan vijfhonderd van die onderhandelingen gevoerd. Het verloopt heel professioneel, via beveiligde kanalen. Geen smalltalk: zij zeggen wat ze willen, jij vraagt hoe het gefaciliteerd kan worden. De betalingen gebeuren altijd in bitcoin.”

Miljoenen euro’s schade

Volgens Baudewijns gaat het niet over een hacker in opdracht van een overheid. “Die wil onder de radar blijven en legt nooit een luchthaven plat. Dit is puur commercieel opportunisme. Zulke bendes hacken wereldwijd zo’n vijfhonderd bedrijven per maand. En dan reken je de amateurhackers nog niet mee. In België zien we gemiddeld twee gevallen per

week, waarvan één door een professionele groep. Voor een bedrijf als Collins schat ik dat het losgeld tussen vijf en tien miljoen dollar ligt."

Luchtvaartexpert Wouter Dewulf wijst op de complexiteit van de sector. "Je hebt maatschappijen, luchthavens, afhandelaars zoals Aviapartner, luchtverkeersleiding, schoonmaak, douane en politie. Als één speler uitvalt, kan de hele keten stilvallen. Die fysieke waardeketen is intussen volledig verbonden met IT-systemen. Hoe meer koppelingen, hoe groter de kans op een zwakke plek. Cybercriminelen weten dat: valt één systeem uit, dan ligt meteen de hele luchthaven plat."

Om de context te schetsen, vergelijkt Dewulf deze aanval met die op een koekjesfabriek. "Als daar de IT uitvalt, ligt de productie misschien een week stil. In de luchtvaart gaat het om tienduizenden reizigers per dag. Bagage die niet gelabeld raakt, mensen die niet ingecheckt raken: de impact is veel groter. En de schade loopt razendsnel op."

Volgens Dewulf kan de rekening enorm oplopen. "Een vliegtuig met 200 passagiers vertegenwoordigt makkelijk 30.000 euro aan verkochte tickets. Als tientallen vluchten wegvallen, spreek je over miljoenen euro's per dag. Tel daar extra personeel, herboekingen en hotelovernachtingen bij en je zit na enkele dagen in de tientallen miljoenen euro's aan economische schade op alle getroffen luchthavens tezamen. En dan hebben we het nog niet over de reputatieschade."

Collins werkt aan een geüpdatete versie van de software, maar het is onduidelijk wanneer die klaar zal zijn. Volgens Baudewijns zou er vrij snel een oplossing kunnen zijn, ofwel door alles opnieuw op te bouwen, ofwel via een deal. "In beide gevallen kost het tijd."

Voor Dewulf is de cyberaanval een wake-upcall. "De luchtvaart is een knooppunt waar tientallen spelers samenkomen, allemaal met hun eigen systemen en belangen. Dat maakt het waterdicht beveiligen bijna onmogelijk. Deze aanval toont hoe kwetsbaar de sector is en hoe groot de financiële en reputatieschade kan zijn. Ze zullen nu wel weer wakker geschoten zijn, maar het is kwestie van alert te blijven."

Dimitri Thijskens