Wat zijn luchthiaten en zijn ze effectieve strategieën voor databeveiliging?

Dit is onderdeel van een serie over luchthiaten en veerkrachtarchitecturen. Lees deel twee: Bent u, zonder een gelaagde back-uparchitectuur, echt veerkrachtig?

Ransomware-aanvallers zijn meedogenloze opportunisten, maar dat betekent niet dat we hun werk gemakkelijker moeten maken.

Pak de aanval op de backoffices van Colonial Pipelines aan. De kritieke gas- en brandstofinfrastructuur was meer dan *vier dagen* offline. Uit een onderzoek bleek dat grote tekortkomingen in de beveiliging het “redelijk eenvoudig” maakten om in te breken.

We moeten het leven voor hackers zo moeilijk mogelijk maken. Gelukkig is er een arsenaal aan technologieën en architectuurparadigma’s om dat te doen. Een van deze benaderingen wordt “**luchthiaten**” genoemd, maar zijn ze een zilveren opsommingsteken voor cyberveerkracht?

Wat is een luchtkloof?

Is een luchtkloof een must-have, marketinglingo, of beide? Laten we eens kijken.

Traditioneel was een luchtkloof fysiek, met behulp van tape-gebaseerde back-ups of offsite systemen, gescheiden door nul fysieke connectiviteit. Beheerders maken een verbinding tussen het productiesysteem en het air-gapped systeem, zoals een drawbridge. De brug gaat omlaag wanneer data worden overgedragen en gaat vervolgens de rest van de tijd weer omhoog.

Vandaag de dag evolueert de definitie en het concept van “luchthiaten” voorbij de traditionele “fysieke netwerkisolatie” om een waardevol onderdeel te zijn van een effectieve, efficiënte databeveiligingsstrategie. Moderne luchthiaten richten zich meer op **logische scheiding**, voornamelijk met netwerkcontroles. In wezen zijn het topologieën voor netwerkontwerp die productie- en back-upnetwerken scheiden. Sommige leveranciers hebben het concept aangepast in:

- **“Virtuele” luchtgaten.** Deze werden voor het eerst geïntroduceerd door leveranciers die zich wilden richten op logische netwerkscheiding en een

dubbele set infrastructuur wilden verkopen met Write Once, Read Many (WORM)-mogelijkheden. Het netwerk tussen locaties zou periodiek openen en sluiten. Dit werd geleverd via uitgebreid advies en Professional Services.

- **“Operationele” luchtspleet.** Toen de “virtuele luchtkloof” een lastige ontvangst van klanten had (d.w.z. lage verkoop), werden operationele luchthiaten gecreëerd in een poging om de infrastructuurkosten te verlagen en extra automatisering toe te voegen rond de installatie en het onderhoud.

In de kern vertrouwen beide benaderingen meestal op WORM-mogelijkheden die zijn gebouwd voor wettelijke en compliancevereisten.*

Het doel van een luchtkloof is om kritieke data te isoleren van lokale netwerken en productiegebieden die kwetsbaarder zijn voor aanvallen. Door regelmatig data vanuit het productienetwerk toe te staan, worden back-ups regelmatig bijgewerkt, maar de twee zijden zijn niet altijd verbonden. Deze intervallen kunnen eenmaal per dag of op een bepaalde frequentie plaatsvinden.

De belofte van de luchtkloof

Het idee is dat zonder een open verbinding tussen de twee locaties, bedreigingen theoretisch geen brug oversteken. En zonder Rekennodes zijn air-gapped systemen nog minder toegankelijk. Sommige aanbieders van dataopslag noemen deze air-gapped recovery-kluizen als een moderne innovatie om data veilig te houden. Een zogenaamde luchtkloof kan zelfs iets eenvoudigs en programmatischs zijn, zoals een firewall.

Over het algemeen kunnen luchthiaten een **betere bescherming bieden door:**

- Biedt meer beveiliging dan traditionele back-uparchitectuur.
- Beperken van de mogelijkheid voor malware om zich te verspreiden.
- Meer werk creëren voor hackers om air-gapped data te krijgen.
- De kans op herstel van een aanval verbeteren

En na de aanval kunnen luchthiaten ook nuttig zijn voor het herstellen van compromisloze data. Maar er is meer om rekening mee te houden.

De realiteit van luchthiaten

Er zijn een paar problemen die u moet overwegen bij luchthiaten. De eerste is toegankelijkheid. Na een aanval, wanneer elke seconde telt, heeft een air-gapped kluis niet alleen data moeilijk toegankelijk gemaakt voor hackers – het is ook moeilijk voor u om toegang te krijgen. De tweede is het werk dat nodig is om luchtgaten te behouden. Hoe groter een luchtkloof wordt met complexe scripts, hoe meer zorg en voeding het vereist om operationeel en effectief te blijven.

Andere problemen:

- Ze zijn niet 100% immuun voor aanvallen.
- Ze kunnen duur zijn om te implementeren en te bedienen, en moeilijk te beheren en te onderhouden.
- Ze zijn niet superschaalbaar en kunnen langzamer grote hoeveelheden data herstellen.
- Ze lossen geen interne bedreigingen of gecompromitteerde inloggegevens van opslag- of back-upbeheerders op.
- Het herstel van grote bestandsvolumes duurt te lang wanneer u moet voldoen aan strenge RPO's – en het classificeren van die data voor gelaagd herstel kost tijd en moeite.

Air-gapped beveiligingsstrategieën kunnen ook de problemen van **betrouwbaarheid** en **snelheid** niet volledig aanpakken – de twee belangrijkste factoren voor succesvol herstel. Wat is dan een allround air-gapped oplossing die eenvoud, betrouwbaarheid *en* snelheid aanpakt?

Pure's aanpak van luchtkloof

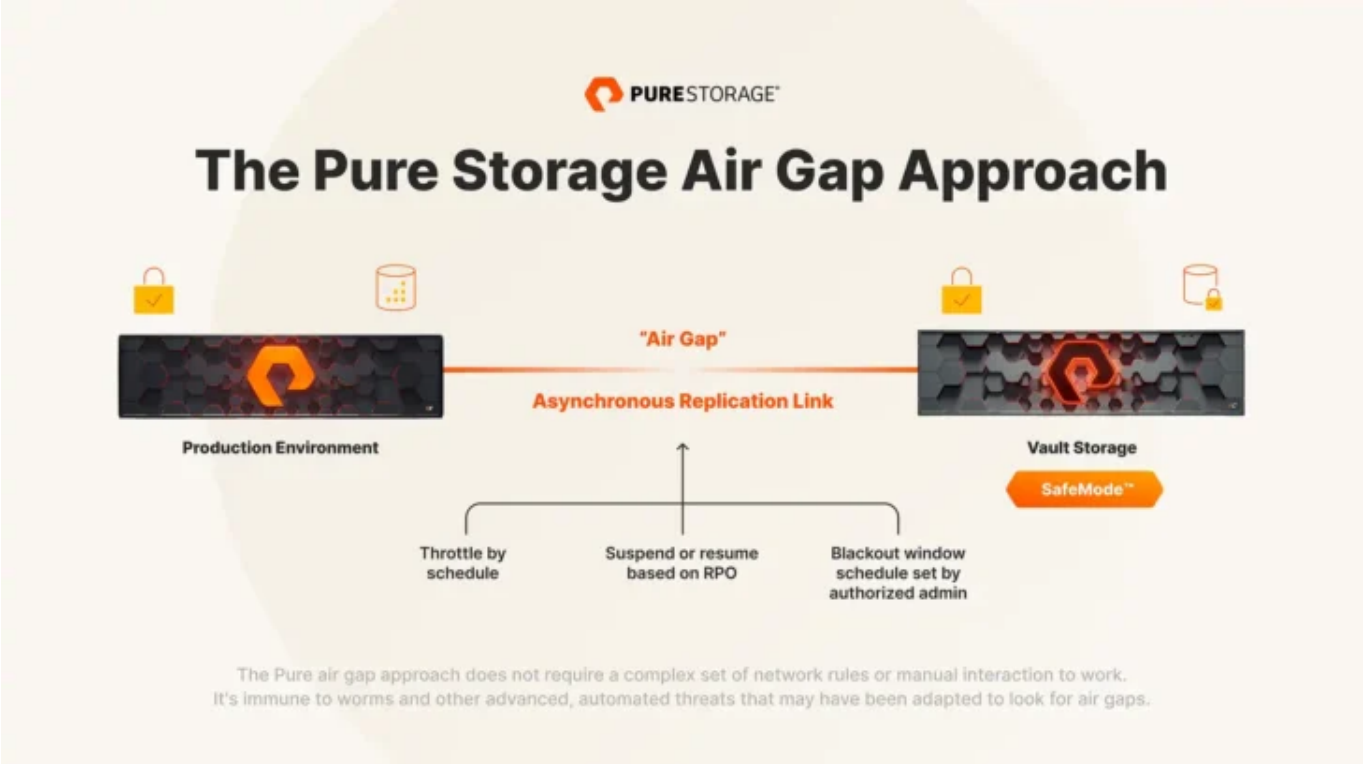
Onze moderne kijk op de virtuele luchtkloof is een implementatie op een hoger niveau die alle voordelen van een air-gapped databunker biedt, maar met een belangrijk verschil: het is **eenvoudiger EN sneller**.

Dit is hoe het werkt:

De SafeMode™-functie van Pure Storage is de sleutel. SafeMode creëert een veilige enclave, waaruit snapshots niet kunnen worden verwijderd – of het nu handmatig door een mens of door een programmatische aanpak is. Daarnaast is er nog een extra menselijk element. Om snapshots handmatig uit te roeien, heeft de oplossing van Pure **realtime, interactieve ondersteuning nodig**, waardoor een extra beschermingslaag wordt toegevoegd.

Dan is er de eenvoud. Ingebouwde automatisering en vooraf ingestelde timers zorgen voor gemoedsrust zonder het extra werk dat nodig is om programmatische of fysieke luchthiaten te handhaven.

Tot slot is het verdrietig, maar waar: tenzij uw dataherstel snel genoeg is om grote organisatie-, reputatie- en financiële impact te voorkomen, is al het werk dat u hebt gedaan rond bescherming waardeloos. Ongeacht het platform of de onderliggende technologie (bijv. pointer-gebaseerde snapshots of toonaangevende verwerkingscapaciteit), Pure kan herstelsnelheden leveren die uw bedrijf niet laten wachten.



Deel 2: Bunkered, gelaagde back-uparchitecturen

---

1. https://www.nytimes.com/2021/05/10/us/politics/pipeline-hack-darkside.html

*Pure-producten ondersteunen geen WORM-mogelijkheden.