Aruba Cloud Solution

# Fizikai biztonság, üzletmenet-folytonosság és katasztrófa utáni helyreállítás

2023.04.14.

# TARTALOMJEGYZÉK





**BlazeArts Kft.**
1096 Budapest, Thaly Kálmán utca 39. cégjegyzékszám: 01-09-389087
adószám: 12539833-2-43 közösségi adószám: HU12539833
https://www.arubacloud.hu

# 1 TÁROLÁSI RENDSZEREK ÉS KIBERBIZTONSÁG

Olaszországban az Aruba Csoport felhőalapú szolgáltatásainak nyújtásához használt összes adatfeldolgozó rendszer Arezzo két adatközpontjában, az „IT1”-ben és az „IT2”-ben található a Via Gobetti 96 és a Via Ramelli 8 alatt, valamint az „IT3” DCA és DCB adatközpontjaiban Ponte San Pietro-ban (BG) a Via San Clemente 53-ban.

*1. ábra 1 – Adatközpont IT1*

*2. ábra 2 – Adatközpont IT2*

*3. ábra – Adatközpont IT3*

Az olaszországi adatközpontok mellett a felhőszolgáltatások nyújtásához az Aruba Csoport egy nemzetközi infrastruktúra-hálózatot vesz igénybe, amely egyrészt saját tulajdonú, másrészt minősített partnerek tulajdonában van:

- CZ1 adatközpont Csehországban, Ktišben, amely a Csoport tulajdonában lévő nemzetközi adatközpont hálózathoz tartozik;
- FR1 adatközpont Párizsban, Franciaországban, amely a partner adatközpontok hálózatához tartozik;
- DE1 adatközpont Frankfurtban, Németországban, amely a partner adatközpontok hálózatához tartozik;



**BlazeArts Kft.**
1096 Budapest, Thaly Kálmán utca 39. cégjegyzékszám: 01-09-389087
adószám: 12539833-2-43 közösségi adószám: HU12539833
https://www.arubacloud.hu

- UK1 adatközpont Londonban, amely a partner adatközpontok hálózatához tartozik;
- PL1 adatközpont Varsóban, Lengyelországban, amely a partner adatközpontok hálózatához tartozik.


*4. ábra – Nemzetközi Felhőszolgáltatási Adatközpont Hálózat*

A szigorú minőségi szabványoknak való megfelelés végett minden adatközpont ISO 9001 tanúsítvánnyal rendelkezik.

A következő részben ismertetjük az elfogadott főbb fizikai biztonsági intézkedéseket.

## 1.1 A fizikai biztonsági intézkedések leírása

Az ISO 27001 tanúsítvány mellett az adatközpontok a fizikai biztonság garantálásához szükséges összes fő funkcióval rendelkeznek.

### 1.1.1 Tier 4*/Rating 4

Az Aruba Csoport IT1 és IT3 DCA és DCB adatközpontjai megfelelnek az ANSI TIA 942-B-2017 legmagasabb szintű szabványának (Rating 4). Ez azt mutatja, hogy még súlyos hibák (hibatűrés) esetén is el lehet kerülni a szolgáltatások megszakadását, és ez egy sor tervezési és végrehajtási intézkedésnek köszönhető, amelyek az adatközpont minden aspektusára kiterjednek: a helyszín kiválasztására, az építészeti szempontokra, a fizikai biztonságra, a tűzoltó rendszerekre, az elektromos rendszerre, a mechanikai rendszerre és az adathálózatra.



**BlazeArts Kft.**
1096 Budapest, Thaly Kálmán utca 39. cégjegyzékszám: 01-09-389087
adószám: 12539833-2-43 közösségi adószám: HU12539833
https://www.arubacloud.hu

A Rating 4 (korábban Tier 4) adatközpont redundáns komponensekkel rendelkezik, amelyek folyamatosan működnek, valamint több ellátási útvonalat és hardveres hűtőrendszert is tartalmaz.

Az adatközpontok kialakításuknak köszönhetően üzemszünet nélkül ellenállnak a létesítmény bármely részében fellépő hibának, és védve vannak a fizikai eseményektől, beleértve a természeti katasztrófákat (pl. tűz, árvíz, földrengés stb.) is.

### 1.1.2 ISO/IEC 22237

Az Aruba Csoport IT3 DCA és DCB adatközpontjai ISO/IEC 22237 tanúsítvánnyal rendelkeznek és teljes életciklusuk során megfelelnek az adatközpontokra vonatkozó nemzetközi standardnak, a stratégiai koncepciótól a felépítésig és üzemeltetésig, összhangban az ANSI/TIA 942 (amerikai) és EN 50600 (európai) szabványokkal. Az úgynevezett „Adatközpont létesítmények és infrastruktúrák” szabályozás hét területet fed le: általános fogalmak, épületépítés, áramelosztás, környezetvédelem, távközlési kábelezési infrastruktúra, biztonsági rendszerek és menedzsment és üzemeltetési információk.

### 1.1.3 24 órás felügyelet

Az összes adatközpontot az év 365 napján, a nap 24 órájában műszaki csapat felügyeli.

A partner adatközpontokat az Aruba Csoport NOC (Network Operations Center) műszaki csapata távolról is irányítja.

A helyi ellenőrző intézkedések mellett a saját adatközpontok BMS (Building Management System) épületkezelési rendszerrel rendelkeznek, amely képes valós idejű riasztásokat generálni a jelentős eseményekről, és lehetővé teszi a távoli technikusok számára az összes rendszer kezelését.



### 1.1.4 A fizikai hozzáférés ellenőrzése

Az épületekbe csak azok léphetnek be, akiknek ténylegesen szükségük van rá, a recepción történő bejelentkezéssel, a technikai helyiségekbe való belépés pedig csak az arra jogosult személyek számára engedélyezett, a belépőkártyával és a megfelelő PIN-KÓDDAL történő azonosítást követően.

Saját tulajdonú adatközpontjai esetében a beléptető rendszer lehetővé teszi az egyedi húzókártyák engedélyezését és letiltását bizonyos területeken, időpontokban és egyéb kritériumoknak megfelelően, garantálva a teljes biztonságot és a könnyű hozzáférést.

Egyes partner adatközpontokban, mint például az FR1, a DE1 és az UK1 központokban biometrikus beléptető rendszer működik.

### 1.1.5 Behatolásgátló rendszerek

Az összes adatközpontban rácsok, golyóálló üveg, páncélozott ajtók és motoros kapuk (passzív behatolásgátló rendszerek) vannak telepítve, valamint CCTV és VMD rendszereket (aktív behatolásgátló rendszerek) alkalmazunk.

Emellett mozgásérzékelőket telepítettünk az adatközpontok minden területére, amelyek képesek érzékelni az emberek jelenlétét; az érzékeny területeken (adatszobák, áramközpontok, raktárak) is vannak olyan érzékelők, amelyek érzékelik az ajtók nyitását.

### 1.1.6 Tűz- és árvízvédelemmel ellátott, antiszeizmikus épületrendszer

Az adatközpontok eleget tesznek az antiszeizmikus előírásoknak. Emellett az emberekre és az informatikai rendszerekre ártalmatlan automatikus tűzjelző és inert gázzal oltó, valamint árvízjelző rendszerekkel vannak felszerelve. A tűzérzékelők és a folyadékszivárgást észlelő érzékelők az épületek minden emeletén jelen vannak.

### 1.1.7 Redundáns légkondicionáló rendszerek

Az adatszobák és a technológiai rendszerek légkondicionáló rendszere több redundáns modulból áll annak érdekében, hogy több egyidejű meghibásodás esetén is működőképes maradjon.

A légkondicionáló rendszert akkumulátorokkal és vészhelyzeti áramfejlesztőkkel ellátott szünetmentes tápegységek védik a szolgáltatás folyamatosságának biztosítása érdekében.

### 1.1.8 Áramellátó Központ tápellátása és redundanciája

Az Aruba Csoport csak kettős tápellátással rendelkező szervereket és berendezéseket használ. Minden egyes áramellátó központ kimenetéhez STS (statikus átviteli kapcsoló) eszközök állnak rendelkezésre, amelyek garantálják az áramellátás folyamatosságát mindkét jelenlévő vezeték számára, és biztosítják, hogy a kettős tápellátással nem rendelkező szerverek és berendezések továbbra is működjenek.

A két különálló áramellátó központnak köszönhetően a szerverek tápellátása teljes mértékben redundáns. Minden áramellátó központ képes ellátni a saját adatközpontjainak összes adatszobáját, még teljes terhelés mellett is, és kettős konverziós UPS rendszerekkel van felszerelve, rendkívül magas energiahatékonysággal (2N + 1 redundancia az IT1, IT2 és IT3 és 2N a CZ1 esetében).

A partner adatközpontok áramellátó rendszerei szintén teljesen redundánsak, és kettős konverziós UPS rendszerekkel vannak felszerelve.

Az adatközpontok műszaki jellemzőivel kapcsolatos további részletekért kérjük, tekintsd meg az alábbi weboldalt: „Adatközpontjaink”.



# 2 ÜZLETMENET-FOLYTONOSSÁG ÉS KATASZTRÓFA UTÁNI HELYREÁLLÍTÁS

## 2.1 Bevezetés

Ennek a fejezetnek az a célja, hogy leírja a katasztrófa utáni elhárítási és üzletmenet-folytonossági eljárást, amely biztosítja annak végrehajtását az Aruba Csoport felhőalapú szolgáltatásaival kapcsolatban.

Az összes vállalat üzleti tevékenysége és a kapcsolódó tevékenységek nagymértékben függnek a támogató folyamatokra szánt eszközök és erőforrások rendelkezésre állásától. Általánosságban elmondható, hogy a szolgáltatás elérhetetlenségének hatása egyre nagyobb, ahogy a megszakítás exponenciálisan folytatódik, és vállalat működési képessége rövid időn belül tartósan veszélybe kerülhet.

Az üzleti folyamatok folytonosságának biztosítása érdekében rendkívül fontos minden olyan erőforrás védelme, amely hozzájárul a legkritikusabb szolgáltatások nyújtásához: adatok, emberek és infrastruktúra, technológiák, kommunikációs hálózatok stb.

Az Aruba Csoport úgy döntött, hogy bevezet egy üzletmenet-folytonossági menedzsment programot, hogy elemezze és kezelje bizonyos katasztrófa-forgatókönyvek hatását a működésre, és következésképpen azonosítsa az üzletmenet-folytonosságot támogató helyreállítási megoldásokat.

Ezek a megoldások az alapvető szolgáltatások helyreállítását célozzák szervezeti, logisztikai és informatikai szempontból.

## 2.2 Üzletmenet-folytonossági terv

Az Üzletmenet-folytonossági terv (röviden a Terv) olyan szabályok és eljárások összessége, amely – egy vagy több olyan forgatókönyv előrejelzésével, amely bármely szervezett rendszer rendes működését megszakíthatja – meghatározza a felelősségi köröket, a tevékenységeket, és biztosítja a szolgáltatás megszakadás kezeléséhez és a rendszer megfelelő működési állapotba való visszaállításához szükséges eszközöket.



A Terv célja annak biztosítása, hogy a kritikus folyamatok elfogadható és előre meghatározott határidőkön belül helyreálljanak.

A felhőalapú szolgáltatásokhoz kapcsolódó teljes termelési környezetet a vállalat Terve védi az infrastruktúra üzletmenet-folytonossági tesztjeivel, amelyek évente elvégzésre kerülnek.

A Terv célja, hogy iránymutatást adjon az Aruba Csoport számára az „Információbiztonsági kockázatkezelés” módszertan alkalmazásával azonosított kockázatok kezelésére és mérséklésére vonatkozóan, amelyet a vonatkozó fejezet ismertet részletesen.

A Terv meghatározza és felsorolja azokat az intézkedéseket is, amelyeket vészhelyzet előtt, alatt és után kell megtenni a szolgáltatás folyamatosságának biztosítása érdekében. Ajánlásokat tesz, és ahol lehetséges, lépésről lépésre utasításokat ad az Aruba Csoport kritikus szolgáltatásai folyamatosságának garantálására olyan nemkívánatos események esetén, amelyek bármilyen ideig megszakíthatják az informatikai rendszereket.

## 2.3 Katasztrófa utáni helyreállítás

A felhőkörnyezet egy több adatközpontú infrastruktúrából áll, amelynek szolgáltatásait egy nagy sávszélességű, biztonságos IPSEC hálózat köti össze.

Az egyes adatközpontok többféle szolgáltatást nyújtanak, többek között:

- Cloud Computing
- Jelastic Cloud
- Database as a Service
- Virtual Private Cloud – VPC
- Cloud Object Storage
- Domain Center
- Cloud Monitoring
- Cloud Backup

Minden adatközpont felépítése a következő alapgépekből áll:

- Domain Controller
- LVS Balancer
- Front-End
- WCF (Microsoft Webservice)
- Provisioning
- Accounting and billing
- Database
- Hypervisor hosts
- Cloud Storage hosts
- Cloud Monitoring hosts
- Private Cloud hosts
- Cloud backup hosts



**BlazeArts Kft.**
1096 Budapest, Thaly Kálmán utca 39. cégjegyzékszám: 01-09-389087
adószám: 12539833-2-43 közösségi adószám: HU12539833
https://www.arubacloud.hu

A struktúrát több adatközpontra tervezték, eleve fel van készítve a Disaster Recovery biztosítására, mivel az összes adatközpont logisztikailag független egymástól.

Fontos kiemelni, hogy a virtualizált ügyfélgépek nem tartalmazzák a katasztrófa utáni helyreállítás biztosítását, mivel maguk az ügyfelek minden szükséges eszközzel rendelkeznek saját katasztrófa utáni helyreállítási rendszerek és eljárások létrehozásához.



**BlazeArts Kft.**
1096 Budapest, Thaly Kálmán utca 39. cégjegyzékszám: 01-09-389087
adószám: 12539833-2-43 közösségi adószám: HU12539833
https://www.arubacloud.hu

# VERZIÓTÖRTÉNET

| | |
|---|---|
| **VERZIÓ**<br>**1.1**<br>14/04/2023 | ***VÁLTOZÁS JELLEGE: Beillesztve: ISO/IEC 22237 tanúsítvány és az IT3 kampusz DCA és DCB adatközpontjaira hivatkozás; a cloud szolgáltatások listája frissítve.*** |

| | |
|---|---|
| **VERZIÓ**<br>**1.0**<br>01/01/2022 | ***VÁLTOZÁS JELLEGE: Első kiadás*** |



**BlazeArts Kft.**
1096 Budapest, Thaly Kálmán utca 39. cégjegyzékszám: 01-09-389087
adószám: 12539833-2-43 közösségi adószám: HU12539833
https://www.arubacloud.hu