INTERNET CZ, a.s.

Forpsi Cloud

Fyzická bezpečnosť, kontinuita činností organizácie a obnova po havárii

14/04/2023

OBSAH

INTERNET CZ, a. s.
Ktiš 2, 384 03 Ktiš IČO: 26043319 DIČ: CZ26043319
https://www.forpsicloud.cz - https://www.forpsicloud.sk

1 UMIESTNENIE SYSTÉMU A KYBERNETICKÁ BEZPEČNOSŤ

Tri spracovateľské systémy používané na poskytovanie cloudových služieb skupiny Aruba sa nachádzajú v Taliansku, konkrétne v datacentroch "IT1" (Via Gobetti 96, Arezzo), "IT2" (Via Ramelli 8, Arezzo) a v datacentrách DCA a DCB "IT3" (Via San Clemente 53, Ponte San Pietro).

Obrázok 1 – Datacentrum IT1

Obrázok 2 – Datacentrum IT2

Obrázok 3 – Datacentrum IT3

Okrem datacentier v Taliansku disponuje spoločnosť Aruba Group medzinárodnou infraštruktúrnou sieťou na poskytovanie cloudových služieb, a to vlastných aj patriacich kvalifikovaným partnerom. Konkrétne sú to tieto:

- Datacentrum CZ1 v Ktiši v Českej republike patriace do medzinárodnej siete datacentier vo vlastníctve Organizácie.
- Datacentrum FR1 v Paríži, ktoré patrí do siete partnerských datacentier.
- Datacentrum DE1 vo Frankfurte patriace do siete partnerských datacentier.

- Datacentrum UK1 v Londýne patriace do siete partnerských datacentier.
- Datacentrum PL1 vo Varšave patriace do siete partnerských datacentier.

Obrázok 4 – Medzinárodná sieť datacentier cloudových služieb

Na splnenie prísnych noriem kvality sú všetky datacentrá certifikované podľa normy ISO 9001.

V ďalšej časti sú vysvetlené hlavné prijaté opatrenia fyzickej bezpečnosti.

1.1 Opis opatrení fyzickej bezpečnosti

Datacentrá sú certifikované podľa normy ISO 27001 a majú všetky hlavné prvky potrebné na zaručenie fyzickej bezpečnosti.

1.1.1 Tier 4*/Rating 4 a ISO 22237

Dátacentrá skupiny Aruba IT1 a IT3 spĺňajú najvyššiu úroveň normy ANSI/TIA 942-B-2017 (rating 4). Datacentrá A a B v areáli IT3 spĺňajú aj normu ISO 22237 (Data center facilities and infrastructures) týkajúcu sa zariadení a infraštruktúry dátových centier, ktorá je medzinárodnou normou pre celý životný cyklus dátového centra. Preukazuje schopnosť zabrániť prerušeniu poskytovania služieb aj v prípade závažných porúch, ktorá bola dosiahnutá prostredníctvom série dizajnových a implementačných opatrení, zohľadňujúcich všetky aspekty dátového centra: výber lokality, architektonické aspekty, fyzickú bezpečnosť, systémy protipožiarnej ochrany, elektrické systémy, mechanické systémy a dátovú sieť.

INTERNET CZ, a. s.
Ktiš 2, 384 03 Ktiš IČO: 26043319 DIČ: CZ26043319
https://www.forpsicloud.cz - https://www.forpsicloud.sk

Dátové centrá s ratingom 4 (predtým úrovne alebo TIER 4) využívajú redundantné komponenty, viacero napájacích ciest a chladiacich systémov.

Dátové centrá sú štruktúrované tak, aby zvládli poruchu v ktorejkoľvek časti zariadenia bez narušenia prevádzky a sú chránené proti udalostiam, ktoré ohrozujú hmotné prvky, vrátane prírodných katastrof (napr. požiar, povodeň, zemetrasenie atď.).

1.1.2 ISO/IEC 22237

Dátacentrá Aruba Group IT3 DCA a DCB sú certifikované podľa normy ISO/IEC 22237. Tieto centrá spĺňajú medzinárodnú normu pre dátacentrá vo všetkých fázach životného cyklu, od strategického plánu cez výstavbu až po prevádzku, v súlade s normami ANSI/TIA 942 (americká norma) a EN 50600 (európska norma). Takzvaný predpis " Data centre facilities and infrastructures" sa vzťahuje na sedem oblastí: Obecné koncepcie, Stavba budov, Distribúcia energie, Kontrola prostredia, Infraštruktúra telekomunikačnej kabeláže, Bezpečnostné systémy a Správa a prevádzkové informácie.

1.1.3 Monitorovanie 24 hodín denne

Všetky datacentrá monitoruje technický tím 24 hodín denne, 365 dní v roku.

Partnerské datacentrá sú tiež spravované na diaľku technickým tímom spoločnosti Aruba Group v NOC (Network Operations Center).

Okrem miestnych kontrolných opatrení sú vlastné datacentrá vybavené systémom BMS (Building Management System), ktorý je schopný v reálnom čase informovať o významných problémoch a umožňuje technickému spravovať všetky systémy na diaľku.

1.1.4 Kontrola fyzického prístupu

Prístup do budov je umožnený len tým, ktorí ho skutočne potrebujú, a to po prihlásení sa na recepcii, pričom vstup do technických miestností je povolený len oprávneným pracovníkom po preukázaní sa preukazom a príslušným PIN kódom.

V prípade vlastných datacentier systém kontroly prístupu zahŕňa možnosť povoliť a zakázať používanie osobných vstupných kariet pre konkrétne oblasti, časy a iné kritériá, čo zaručuje úplnú bezpečnosť a jednoduchosť prístupu.

V niektorých partnerských datacentier, ako sú FR1, DE1 a UK1, je zavedený biometrický systém kontroly prístupu.

1.1.5 Systémy proti vniknutiu

Vo všetkých datacentrách sú nainštalované mreže, nepriestrelné sklo, pancierové dvere a motorizované brány (pasívne systémy proti vniknutiu), systémy CCTV a VMD (aktívne systémy proti vniknutiu).

INTERNET CZ, a. s.
Ktiš 2, 384 03 Ktiš IČO: 26043319 DIČ: CZ26043319
https://www.forpsicloud.cz - https://www.forpsicloud.sk

Okrem toho sú vo všetkých priestoroch datacentier nainštalované snímače pohybu, ktoré sú schopné zistiť prítomnosť osôb. V citlivých priestoroch (dátové miestnosti, centrá napájania, sklady) sa nachádzajú aj snímače, ktoré zisťujú otvorenie dverí.

1.1.6 Stavebný protipožiarny, protipovodňový a protiseizmický systém

Všetky datacentrá spĺňajú protiseizmické predpisy. Okrem toho máme automatické systémy detekcie požiaru a hasenia inertným plynom, ktoré sú neškodné pre ľudí a IT systémy, ako aj systémy detekcie záplav.

Na všetkých poschodiach budov sa nachádzajú senzory na detekciu požiaru, ako aj senzory na detekciu úniku kvapalín.

Budovy sa tiež nachádzajú v rovinatých oblastiach a v polohách, ktoré boli preskúmané vzhľadom na úroveň terénu.

1.1.7 Záložné klimatizačné systémy

Klimatizačný systém pre dátové miestnosti a technologické systémy sa skladá z viacerých redundantných modulov, aby sa zabezpečila jeho funkčnosť aj v prípade viacerých súčasných porúch.

Klimatizačný systém je chránený UPS s batériami a núdzovými generátormi elektrickej energie, aby sa zaručila nepretržitosť prevádzky.

1.1.8 Redundantné záložné generátory a napájacie centrum

Aruba Group používa iba servery a zariadenia s dvojicou napájacích zdrojov. Každé napájacie centrum je zálohované STS zariadeniami (Static Transfer Switch), ktoré zaisťujú nepretržitý prívod energie aj pre zariadenia používajúce iba jeden napájací zdroj.

Všetko napájanie serverov je kompletne redundantné vďaka dvom oddeleným napájacím centrám. Každé z týchto centier má kapacitu na napájanie všetkých 10 dátových sál pri plnej záťaži a je vybavené UPS s dvojitou konverziou a vysokou energetickou účinnosťou (2N + 1 redundancia pre datacentrá IT1, IT2 a IT3 a 2 N pre datacentrum CZ1).

Napájacie systémy v partnerských datacentrách sú tiež kompletne redundantné a vybavené systémami UPS s dvojitou konverziou.

Podrobnejšie informácie o technických charakteristikách analyzovaných datacentier nájdete na stránke: Naše datacentrá.

2 KONTINUITA ČINNOSTÍ ORGANIZÁCIE A OBNOVA PO HAVÁRII

2.1 Úvod

Cieľom tejto kapitoly je opísať zavedený postup obnovy po havárii a kontinuity činností s cieľom zabezpečiť jeho implementáciu v súvislosti so službami Aruba Group Cloud.

Podnikanie všetkých spoločností a s ním spojené činnosti sú do veľkej miery závislé od dostupnosti zariadení a zdrojov určených na podporné procesy. Vo všeobecnosti sa vplyv nedostupnosti služby exponenciálne zvyšuje, keď prerušenie pokračuje, a v krátkom čase môže dôjsť k trvalému ohrozeniu schopnosti spoločnosti fungovať.

Na zabezpečenie kontinuity obchodných procesov je mimoriadne dôležité chrániť všetky zdroje, ktoré prispievajú k poskytovaniu najdôležitejších služieb: informácie, ľudí a infraštruktúru, technológie, komunikačné siete atď.

Spoločnosť Aruba Group sa rozhodla zaviesť program riadenia kontinuity činností organizácie s cieľom analyzovať a riadiť vplyv určitých katastrofických scenárov na prevádzku a následne určiť riešenia obnovy na podporu kontinuity činností.

Tieto riešenia riešia obnovu základných služieb z organizačného, logistického a IT hľadiska.

2.2 Plán kontinuity činností organizácie

Plán kontinuity činností organizácie (angl. Business Continuity Plan, ďalej len „BCP“) je súbor pravidiel a postupov, ktoré – predvídaním jedného alebo viacerých scenárov, ktoré by mohli prerušiť normálnu prevádzku akéhokoľvek organizovaného systému – vymedzujú zodpovednosti, stanovujú činnosti a poskytujú nástroje na riadenie prerušenia a vrátenia systému do dostatočného stavu prevádzky.

Účelom BCP je zabezpečiť, aby kritické procesy boli obnovené v rámci tolerovateľných a vopred stanovených termínov.

Celé produkčné prostredie súvisiace s cloudovými službami je chránené plánom BCP, pričom sa každý rok vykonávajú testy kontinuity činností organizácie v rámci infraštruktúry.

Úlohou tohto plánu je poskytnúť usmernenia pre spoločnosť Aruba, pokiaľ ide o riadenie a zmierňovanie rizík identifikovaných použitím metodiky „Riadenie rizík informačnej bezpečnosti“, ktorá je podrobne opísaná v príslušnej kapitole.

BCP tiež definuje a uvádza opatrenia, ktoré sa majú uskutočniť pred, počas a po núdzovej situácii, aby sa zabezpečila kontinuita činností. Poskytuje odporúčania a, ak je to možné, podrobné pokyny na zaručenie kontinuity kritických služieb spoločnosti Aruba Group v prípadoch nežiaducich udalostí, ktoré môžu na určitý čas prerušiť IT systémy.

2.3 Obnova po havárii

Cloudové prostredie pozostáva z infraštruktúry viacerých datacentier, ktorých služby sú prepojené bezpečnou sieťou IPSEC s vysokým vlnovým rozsahom.

Každé datacentrum poskytuje množstvo druhov služieb vrátane týchto:

- Cloud Computing
- Database as a Service
- Virtual Private Cloud – VPC

- Cloud Object Storage
- Domain Center
- Cloud Monitoring
- Cloud Backup

Každé dátacentrum má tiež štruktúru pozostávajúcu z týchto základných serverov:

- 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

Je navrhnutá ako štruktúra s viacerými datacentrami a je prirodzene predurčená na obnovu po havárii, pretože všetky datacentrá sú na sebe logicky nezávislé.

Je dôležité zdôrazniť skutočnosť, že virtualizované počítače zákazníkov nepodliehajú geografickej obnove po havárii, pretože zákazníci majú k dispozícii všetky potrebné nástroje na vytvorenie systémov a postupov obnovy po havárii na mieru.

INTERNET CZ, a. s.
Ktiš 2, 384 03 Ktiš IČO: 26043319 DIČ: CZ26043319
https://www.forpsicloud.cz - https://www.forpsicloud.sk

HISTÓRIA VERZIÍ

VERZIA **1.1** K 14/04/2023	***OPIS ZMIEN: Pridané: certifikácia ISO/IEC 22237 a IT3 Campus s odkazom na DCA a DCB; aktualizovaný zoznam poskytovaných cloudových služieb.***
VERZIA **1.0** K 01/01/2022	***OPIS ZMIEN: Prvé vydanie***

INTERNET CZ, a. s.
Ktiš 2, 384 03 Ktiš IČO: 26043319 DIČ: CZ26043319
https://www.forpsicloud.cz - https://www.forpsicloud.sk