INTERNET CZ, a.s.

Forpsi Cloud

Fyzická bezpečnost, kontinuita provozu a disaster recovery

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 UMÍSTĚNÍ SYSTÉMŮ A KYBERNETICKÁ BEZPEČNOST

Tři zpracovatelské systémy používané pro poskytování cloudových služeb Skupiny Aruba jsou umístěné v Itálii, konkrétně v datacentrech, „IT1“ (Via Gobetti 96, Arezzo), „IT2“ (Via Ramelli 8, Arezzo) a v DCA a DCB datacentrech „IT3“ (Via San Clemente 53, Ponte San Pietro).

Obrázek 1 – datacentrum IT1

Obrázek 2 – datacentrum IT2

Obrázek 3 – datacentrum IT3

Kromě italských datacenter využívá Skupina Aruba pro poskytování cloudových služeb mezinárodní sítě infrastruktur, a to jak ve svém vlastnictví, tak ve vlastnictví kvalifikovaných partnerů, konkrétně:

- Datatacentrum CZ1 v Ktiši (ČR), které patří do mezinárodní sítě datacenter vlastněných přímo organizací.
- Datatacentrum FR1 v Paříži (Francie), které patří do sítě partnerských datacenter.
- Datatacentrum DE1 ve Frankfurtu (Německo), které patří do sítě partnerských datacenter.

- Datatacentrum UK1 v Londýně (Velká Británie), které patří do sítě partnerských datacenter.
- Datatacentrum PL1 ve Varšavě (Polsko), které patří do sítě partnerských datacenter.

Obrázek 4 – Mezinárodní síť datacenter pro cloudové služby

Pro splnění přísných standardů kvality jsou všechna datacentra certifikovaná podle normy ISO 9001.
V další části naleznete vysvětlení, jaká byla přijata hlavní opatření fyzické bezpečnosti.

1.1 Popis opatření fyzické bezpečnosti

Datacentra jsou certifikovaná podle normy ISO 27001 a jsou v nich aplikována hlavní opatření potřebná k zajištění fyzické bezpečnosti.

1.1.1 Tier 4* / Rating 4 a ISO 22237

Datacentra skupiny Aruba IT1 a IT3 splňují nejvyšší úroveň standardu ANSI/TIA 942-B-2017 (rating 4). Datacentra A a B v areálu IT3 splňují také normu ISO 22237 (Data center facilities and infrastructures) týkající se zařízení a infrastruktury datacenter, což je mezinárodní standard pro celý životní cyklus datacentra. Dokazuje schopnost vyhnout se přerušení služeb i v případě závažných poruch, které bylo dosaženo díky řadě designových a implementačních opatření zohledňujících všechny aspekty datacentra: výběr místa, architektonické aspekty, fyzickou bezpečnost, protipožární systémy, elektrické systémy, mechanické systémy a datovou síť.

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

Datacentra s ratingem 4 (dříve úrovní, resp. TIER 4) využívá redundantní komponenty, více napájecích cest a systémů chlazení.

Datacentra jsou strukturovaná tak, aby přečkala poruchu v jakékoli části zařízení bez narušní provozu a jsou chráněná před událostmi ohrožujícími hmotné prvky, včetně přírodních katastrof (např. požár, povodně, zemětřesení atd.).

1.1.2 ISO/IEC 22237

Aruba Group datacentra IT3 DCA a DCB, jsou certifikována dle normy ISO/IEC 22237. Tato centra splňují mezinárodní standard pro datacentra ve všech fázích životního cyklu, od strategického plánu přes výstavbu až po provoz, a to v souladu s normami ANSI/TIA 942 (americký standard) a EN 50600 (evropský standard). Takzvané nařízení " Data centre facilities and infrastructures" pokrývá sedm oblastí: Obecné koncepty, Stavba budov, Distribuce elektřiny, Kontrola prostředí, Infrastruktura telekomunikační kabeláže, Bezpečnostní systémy a Správa a provozní informace.

1.1.3 Nepřetržitý monitoring

Všechna datacentra monitoruje technický tým 24 hodin denně, 365 dní v roce.

Partnerská datacentra také na dálku spravuje technický tým Skupiny Aruba v centru síťových operací NOC (Network Operations Center).

Kromě místních kontrolních opatření mají datacentra vlastněná skupinou systém řízení budov BMS (Building Management System), který umí v reálném čase upozorňovat na významné události a umožnit technikům na dálku spravovat všechny systémy.

1.1.4 Kontrola fyzického přístupu

Přístup do objektů je umožněný pouze tomu, kdo ho skutečně potřebuje, a to po přihlášení na recepci. Vstup do technických místností mají povolený pouze oprávněné osoby, poté co se identifikují průkazem a odpovídajícím kódem PIN.

V případě vlastních datacenter zahrnuje systém řízení přístupu možnost povolit a zakázat jednotlivé přístupové karty pro určité oblasti, časy a další kritéria, což zaručuje naprostou bezpečnost a snadný přístup.

V některých partnerských datacentrech, jako jsou FR1, DE1 a UK1, je zavedený biometrický systém řízení přístupu.

1.1.5 Systémy zabraňující vniknutí

Ve všech datacentrech jsou rozmístěné mříže, neprůstřelné sklo, pancéřované dveře a motorizované brány (pasivní systémy obrany proti vniknutí) a instalované systémy CCTV a VMD (aktivní systémy obrany proti vniknutí).

Kromě toho jsou ve všech prostorách datacenter instalované pohybové senzory, schopné zaznamenat přítomnost osob; v citlivých prostorách (datové sály, energetická centra, sklady) jsou také senzory, které detekují otevření dveří.

1.1.6 Protipožární, protipovodňový a protiseismický systém budov

Všechna datacentra odpovídají protiseismickým normám. Kromě toho jsou budovy opatřeny automatickými systémy detekce požáru a hasicími systémy s inertním plynem, které jsou neškodné pro lidi a IT systémy, a dále systémy detekce povodní.

Ve všech patrech budov jsou k dispozici senzory požární detekce, stejně jako senzory, které detekují únik kapaliny.

Budovy jsou umístěné v rovinatých oblastech a na místech, kde proběhl průzkum úrovně terénu.

1.1.7 Záložní klimatizační systémy

Klimatizační systém pro datové sály a technologické systémy je tvořený několika redundantními moduly, aby byl i v případě více současných poruch zajištěn provoz.

Klimatizační systém je chráněný zdrojem nepřerušovaného napájení (UPS) s bateriemi a nouzovými generátory elektřiny pro zaručení kontinuity provozu.

1.1.8 Napájení a záloha napájecího centra

Skupina Aruba používá pouze servery a zařízení s duálním napájením. Pro výstup z každého napájecího centra jsou k dispozici spínače STS (Static Transfer Switch), které jsou schopné zaručit kontinuitu napájení pro obě přítomné linky a také zajistit, aby nadále fungovaly servery a zařízení, která nemají duální napájení.

Napájecí zdroj pro servery je díky dvěma samostatným napájecím centrům kompletně zálohovaný. Každé napájecí centrum má kapacitu zásobovat všechny datové místnosti ve vlastních datacentrech, a to i při plném zatížení, a je vybavené systémy UPS s dvojitou konverzí a extrémně vysokou energetickou účinností (2 N + 1 záloha pro IT1, IT2 a IT3 a 2 N pro CZ1).

Napájecí systémy v partnerských datacentrech jsou také zcela zálohované a vybavené systémy UPS s dvojitou konverzí.

Podrobnější informace o technických charakteristikách analyzovaných datacenter najdete na webové stránce: „Vlastní datacentra“.

2 KONTINUITA PROVOZU A DISASTER RECOVERY

2.1 Úvod

Cílem této kapitoly je popsat zavedený postup obnovy po havárii a zajištění kontinuity provozu a jeho implementaci ve vztahu k poskytování cloud služeb v rámci Skupiny Aruba.

Provoz všech společností a jejich související činnosti je silně závislý na dostupnosti zařízení a zdrojů určených pro podpůrné procesy. Obecně se dopad nedostupnosti služby zvyšuje, protože přerušení pokračuje exponenciálně, a v krátké době může dojít k trvalému ohrožení provozu společnosti.

Pro zajištění kontinuity podnikových procesů je nesmírně důležité chránit všechny zdroje, které přispívají k poskytování nejzásadnějších služeb: informace, lidi a infrastrukturu, technologie, komunikační sítě atd.

Skupina Aruba se rozhodla zavést program řízení kontinuity provozu, který analyzuje a řídí dopad určitých scénářů katastrof na procesy a následně identifikuje řešení obnovy pro podporu kontinuity provozu.

Tato řešení se týkají obnovy základních služeb z perspektivy organizace, logistiky a IT.

2.2 Plán kontinuity provozu

Plán kontinuity provozu (Business Continuity Plan, dále jen „BCP“) je soubor pravidel a postupů, které – předvídáním jednoho nebo více scénářů, které by mohly přerušit běžný provoz kteréhokoli organizovaného systému – definují odpovědnosti, stanoví činnosti a poskytují nástroje pro řízení přerušení a navrácení systému do dostatečného stavu provozu.

Účelem BCP je zajistit, aby kritické procesy byly obnoveny v rámci přijatelných a předem stanovených termínů.

Celé produkční prostředí související s cloudovými službami je chráněné BCP společnosti, přičemž každoročně jsou naplánované testy kontinuity provozu.

Úlohou tohoto plánu je poskytnout pokyny Skupině Aruba, pokud jde o řízení a zmírnění veškerých rizik zjištěných použitím metodiky „Řízení rizik v oblasti bezpečnosti informací“, která je podrobně popsaná v příslušné kapitole.

BCP také definuje a uvádí seznamy opatření, která mají být přijatá před stavem nouze, během něj a po něm, aby se zajistila kontinuita provozu. Poskytuje doporučení a, pokud je to možné, podrobné pokyny pro zajištění kontinuity zásadních služeb Skupiny Aruba v případě nežádoucích událostí, které můžou na různě dlouhou dobu přerušit IT systémy.

2.3 Disaster recovery

Prostředí cloudu se skládá z infrastruktury několika datacenter, jejíž služby jsou propojené zabezpečenou sítí IPSEC s vysokou šířkou pásma.

Každé datacentrum poskytuje řadu typů služeb:

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

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

- Cloud Monitoring
- Cloud Backup

Každé datacentrum má také strukturu tvořenou následujícími základními servery:

- 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

Struktura s více datacentry má přirozené dispozice zotavit se po havárii, protože v principu jsou všechna datacentra na sobě nezávislá.

Je důležité zdůraznit skutečnost, že virtualizované zákaznické servery nepodléhají geografickému zotavení po havárii (Disaster Recovery), protože samotní zákazníci mají k dispozici všechny potřebné nástroje pro vybudování na míru vytvořených systémů a postupů pro zotavení po havárii (Disaster Recovery).

HISTORIE VERZÍ

VERZE 1.1 K 14/04/2023	***POPIS ZMĚN: Vloženo: ISO/IEC 22237 certifikace a IT3 Campus s odkazem na DCA a DCB; aktualizovaný seznam poskytovaných Cloudových Služeb.***

VERZE 1.0 K 01/01/2022	***POPIS ZMĚN: První vydání***

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