Bezpečnost zákazníka DC

Mgr. František Princ

CRA Security 2022
18. 10. 2022

WEB4U

Společnost Web4U s.r.o.

- na trhu od roku 2003
- registrátor domén
- poskytovatel webhostingu & mailhostingu
- široké portfolio serverových služeb
- desítky tisíc spokojených zákazníků
- zákazníkem ČRa od roku 2017
- od léta 2022 patří společnost do nadnárodní skupiny Miss Group

Datová centra

- 2 hlavní datová centra - CRa DC Tower a T-Mobile THP
- DC Tower - primární lokalita (2017) - většina služeb
- T-Mobile THP - záložní lokalita, HA služby, síťová redundance
- “externí” DC CRa Strahov - mimo AS (monitoring, VoIP, ...)
- neveřejná lokalita - umístění sekundární zálohy pro DR

WEB4U

Stěhování (příprava)

- v letech 2016-17 nabídka od ČRa, později konkurenční od TTC
- prohlídky obou datových center, hodiny schůzek a konzultací
- hlavní kritérium - fyzická bezpečnost, kterou zákazník neovlivní a musí se plně spolehnout na provozovatele DC
- Q2 2017 rozhodnuto o stěhování do DC Tower vč. celé pobočky
- další hodiny konzultací s odborníky ČRa na datová centra
  - `layout racku, napájení serverů, optimalizace chlazení`

WEB4U

Stěhování (realizace)

- 11/2017 - předání a finální osazení racků
  - napájení, lokální propoje
- 12/2017 - oživení lokality na síťové úrovni
  - propoje se stávající sítí, nové propoje k partnerům (NIX, Vodafone, ČRa), úprava routingu
  - aktivace prvních serverů (hypervizorů) – stěhování VM live po síti
- 1-2/2018 - stěhování fyzických serverů
  - dedikované a managed vlastními silami
  - housing ve spolupráci s jednotlivými zákazníky
- 2/2018 - stěhování kanceláří, skladu a zaměstnanců

WEB4U

Stěhování (shrnutí)

- původní plán - hromadné stěhování odbornou firmou
  - zamítnuto kvůli dlouhé odstávce všeho najednou
- zvolen transport v cyklech po ~5 fyzických serverech
  - v původním DC jeden administrátor vypínal a nakládal
  - 1 kolega zajišťoval bezpečný převoz
  - v cílovém DC 2 kolegové oživovali navezený HW
- průběh 2x 4 noci (23 - 5)
- zbytek kolegů zajišťoval běžný provoz + přípravu pro další noc
- sklad a kancelář - jednodenní akce pro většinu kolegů

WEB4U

Stěhování (bezpečnost)

- Mnoho nových rizik - servery (a data) opouští bezpečný přístav DC
  - poškození HW (manipulace, autonehoda, změna teploty)
  - poškození/ztráta dat - disky v RAID, ale ve stejném serveru
  - riziko krádeže HW mimo bezpečný perimetr DC
  - rizika při manipulaci s cizím HW (serverhousing)
- Výsledek
  - žádný problém s HW
  - několik serverů nenaběhlo chybou konfigurace ze strany zákazníka
  - námi spravované servery bez problému
  - virtuální servery putovaly do nového DC bezpečně po síti

WEB4U

Fyzická rizika z pohledu zákazníka DC

- neoprávněný přístup do DC, sálu, racku
  - neoprávněná manipulace se servery (odpojení, přístup ke konzoli, boot z USB zařízení a spuštění čehokoli)
  - krádež HW, tedy i dat
  - zásah do síťové infrastruktury
    - odposlech
    - přerušení nebo omezení provozu
  - neoprávněné umístění HW pro následné zneužití (opět odposlech, pozdější útok)
- výpadek napájení
- přerušení komunikačních tras
- požár a další “živelné” pohromy

Fyzická rizika - serverhousing

- specifická služba z hlediska fyzické bezpečnosti
- vyhrazené racky pouze pro housing
- přístup zákazníka do sdíleného racku
  - minimalizace asistence technika (COVID) = samostatný přístup
  - přístupová práva, proškolení, dohled
  - odpovědnost zákazníka

WEB4U

Kanceláře

- umístění přímo v budově DC Tower
  - zabezpečení v rámci standardů ČRa
  - zabezpečená chodba pouze pro Web4U
  - nadstandardní konektivita přímo z DC (mimo náš AS)
- sklad
  - záložní HW
  - adekvátní prostor pro montáž
  - velká flexibilita při manipulaci HW v DC

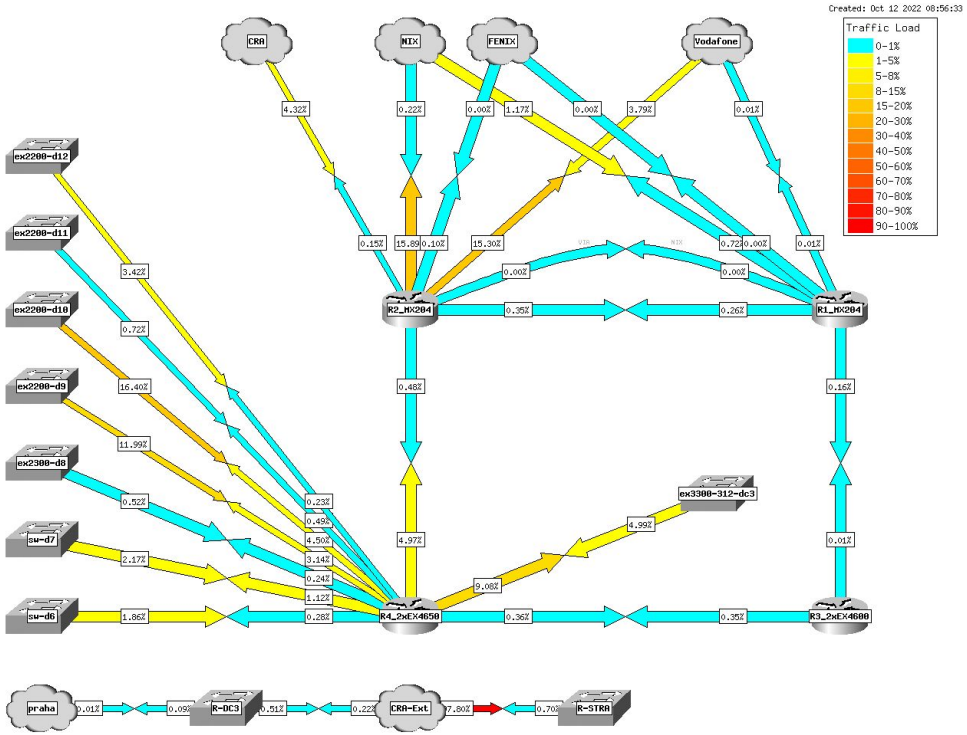
COVID

- nová situace pro všechny - ze dne na den plošný home office
- na DC maximálně 1 zaměstnanec (senior admin)
- povinné testování pro přístup do objektů
- minimalizace kontaktů = omezení asistence remote hands
- některé změny ve fungování firmy jsou trvalé

WEB4U

Síťová infrastruktura

- zdvojování
  - routery
  - switche
  - linky
- oddělení lokalit
- out-of-band management
- uzavřená síť pro IPMI



WEB4U

Síťová infrastruktura - výpadky

- HW výpadek síťového prvku
  - dojezd technika prodlužuje dobu výpadku
  - řešeno zdvojením všeho, co dává smysl
  - náhradní HW buď skladem nebo u dodavatele v rámci supportu
- porucha linky
  - ne vše můžeme ovlivnit - např. překopnutí optického kabelu
  - zdvojení
- odříznutí konfigurační chybou
  - out-of-band management
  - verzování konfigurace = rychlý návrat zpět

WEB4U

Síťová infrastruktura - útoky

- DDoS
  - frekvence i síla rostou
  - ochrana na tranzitních linkách nestačí
  - nutné komplexní řešení
    - tlusté linky a lokální mitigace
    - externí ochrana
- kradení adres (MAC, IP)
  - ochrana na více úrovních (access switche, hypervizory, …)
  - segmentace sítě

Monitoring

- nezbytná součást provozu
- odhalí mnoho bezpečnostních problémů, ale **ne všechny**
- spolehlivost je klíčová
  - `aktivní zasílání alertů`
  - `eskalace pro případ selhání člověka nebo techniky`
  - `monitoring monitoringu :)`
- nutno doplnit o logování, archivaci a analýzu

WEB4U

Zálohování obecně

Všichni ví, že zálohovat se musí, ale ...

- funguje zálohování?
- lze ze zálohy obnovit?
- jak dlouho to bude trvat?
- co když přijdeme o zálohovací pole (havárie, zlý úmysl, ...)?
- data mohou uniknout i ze záloh, je jich tam dokonce více

WEB4U

Zálohování - DR

- DR záloha zálohy
  - inspirováno případem českého poskytovatele z r. 2020
  - zálohujeme zálohy (více instancí)
  - umístění mimo naše provozní DC
  - striktně omezený přístup zaměstnanců (nikdo se nesmí dostat všude)
  - nedostupnost po síti
  - šifrování
  - kvalitní dokumentace - nepoužívané věci z lidské paměti mizí

WEB4U

Závěr

- Bezpečnostní posun v posledních letech
  - stěhování do DC Tower
  - dokončení změn na síťové infrastruktuře
  - externí monitoring
  - zavedení záloh pro DR
  - procesy vzniklé v covidové době
  - nezávislé penetrační testy ze strany nového majitele

WEB4U