Viacúrovňová bezpečnosť cloudovej platformy

Viacúrovňová bezpečnosť cloudovej platformy

Tomáš Hogh, Slovak Telekom, a.s.

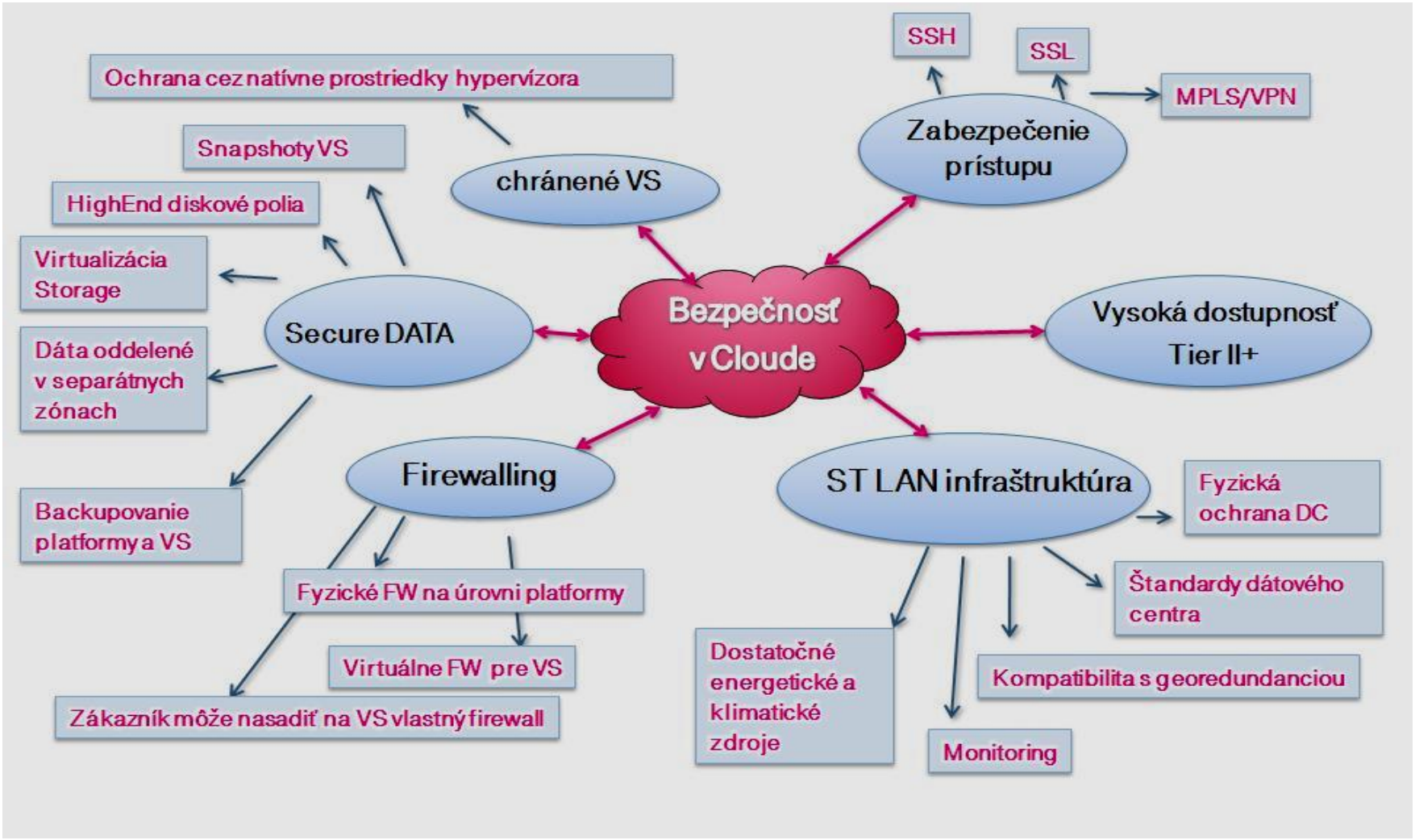
Úvod

- Najčastejšie otázky zákazníkov, firiem, organizácií sa dotýkajú bezpečnosti a celkovo obavy z cloudových riešení:
  - Je Cloud dostatočne bezpečný?
  - Na akých úrovniach?
  - Je dostatočne spoľahlivý?
  - Kde sú moje dáta / Kto tam má prístup?
  - Existuje pocit že organizácia sa zbavuje svojich citlivých dát?
  - Sú dodržané všetky legislatívne nariadenia/obmedzenia (uchovávanie a ochrana dát a informácií, ...)

Bezpečnosť z pohľadu rôznych úrovní

- Bezpečnosť zákazníckych dát musí byť riešená na viacerých úrovniach
  - Berieme do úvahy kvalitatívnu úroveň jednotlivých súčastí Cloudu (napr. dátové centrum, HW infraštruktúru, hypervízory, atď.)
  - Bezpečnosť má byť riešená aj na úrovni sietí, diskových polí, serverov, VS, príp. samotných prenášaných dát, vrátane logickej separácie zákazníkov
- Čo zahrňujeme pod pojem bezpečný Cloud?
  - Parametre a bezpečnosť Dátového centra
  - LAN / SAN infraštruktúra
  - Firewalling
  - Servery, diskové polia, sieťové prvky
  - Virtuálna infraštruktúra
  - Bezpečné prostredie / Secure DATA
  - Samoobslužbý portál pre zákazníka
  - Konektivita – možnosti pripojenia zákazníka do Cloudu
  - Legislatíva / Dôveryhodnosť poskytovateľa / SLA

Úrovne bezpečnosti TelekomCloudu



Parametre a bezpečnosť Dátového centra

- Dátové centrum len pre interné systémy a technológie
- Dostatočné kvalitatívne parametre Dátového centra
- Vysoká dostupnosť dátového centra (99,9)
- Nezávislé optické trasy do dátového centra
- Dostatočné energetické a klimat. zdroje a kapacity
- Priemyselný stackovateľný cooling
- Systém detekcie požiaru, dymu až na úroveň jednotlivých stojanov
- Dvojokruhová napájacia sústava (nezávislé el.pripojenie)
- Záložné zdroje napájania - UPS, Motorgenerátor, ...

- Viacúrovňová fyzická ochrana DC + manažment vstupov + logovanie vstupov
- Kamerový a dohľadový systém DC
- Monitoring zdrojov (elektrina, klíma)
- Vlastná trafostanica

LAN / SAN Infraštruktúra

- Redundantná sieťová infraštruktúra na primárnej lokalite
- Pripravenosť na georedundanciu
- LAN aj SAN infraštruktúra vybudovaná na zariadeniach (HighEnd/Enterprise) od renomovaných výrobcov (Cisco, Fortinet, Arbor)
- Dodržané štandardy dátového centra (zálohované napájanie, enviro-prostredie, dostatok sieťových interfejsov,)
- Kapacitný manažment
- Monitoring / logovanie / Dohľadovaná služba = 24/7
- Jednoduchá a rýchla rozširovateľnosť sieťových zdrojov
- Diskové polia primárne pripájané cez manažovanú SAN sieť

Servery, diskové polia, sieťové prvky

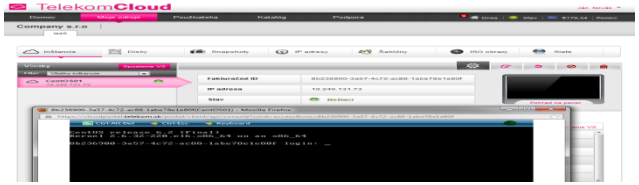
- Riešenie dizajnované tak, aby zabezpečovalo možnosť dynamického škálovania (Plug&EasyConf&Play)
- Redundantná HW infraštruktúra
- Pre vysokú výkonnosť, škálovateľnosť a dostupnosť dát využívané diskové polia HighEnd/Enterprise úrovne (Hitachi VSP, spoľahlivosť -> 99,999%)
- Vypočtový výkon dodáva IBM BladeCenter H infraštruktúra
- IBM pásková knižnica využívaná pre backup platformy
- Sieťové prvky od renomovaných výrobcov cisco Nexus / FORTINET
- SAN a LAN infraštruktúra s vysokou priepustnosťou a s možnosťou rozšírenia
- HW zdroje monitorované kapacitným manažmentom
- Systémový monitoring fyzickej HW platformy
- Cloud z pohľadu HW nezávislý od výrobcu **(NO Vendor Lock)**

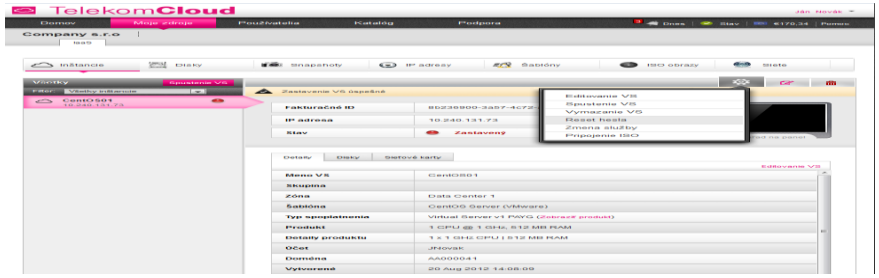
Bezpečné prostredie / Secure DATA

- Multiering Storage / dáta oddelené v separátnych zónach
- Viacstupňový backup
  - Zálohovanie celej platformy (platform backup), Virtual server backup, konfigurácií komponentov riešenia, zákaznícke zálohovanie
  - Zákazník môže sám inicializovať vlastné zálohovanie pomocou samoobslužného portálu (manuálny/automatický + jednorázový/pravideľný).
- Secure Testing - Testovanie na oddelenej platforme emulujúcej produkčné prostredie
- Bezpečné updat-y, upgrad-y, simulácia zákazníckych updatov (minimalizácia výskytu chýb)
- Real-time monitoring (voľných/obsadených) zdrojov (virtuálnych/fyzických) (pozor iba zdrojov, nie OS, dát, a pod.)
- Monitoring previazaný s alarm systémom
- Kapacitný manažment – v prípade míňajúcich sa fyzických/virtuánych zdrojov, systém upozorňuje na nutné rozšírenie (možnosť nastavénia prahových hodnôt)
- Centralizovaný manažment riešenia – jednoduchšia/efektívnejšia kontrola a riadenie zdrojov (napr. realizácia zákazníckych požiadaviek na zmenu služby, alebo riešenie nežiaducich udalostí)
- Logovanie činností Cloud platformy (Zákazník/Provider)
- Bezpečný transfer dát (bezpečná komunikácia prostredníctvom SSL, klient VPN, S2S VPN, prípadne MPLS/BCN služba)

Samoobslužbý portál pre zákazníka

- Zákazník sám kontroluje / riadi / monitoruje virtuálnu infraštruktúru prostredníctvom Samoobslužného (Self service) portálu
  - Nástroj manažmentu , bezpečnosti (FW), ale aj dôvery (zákazník má prehľaď a svojich zdrojoch)
  - Umožňuje zákazníkom priamu správu a konfiguráciu pridelených zdrojov (VS, VS+OS, disky, siete, Virtual firewall, ...)
  - Každý zákazník má vlastný Virtuálny firewall s plnou administráciou
  - Monitoring stavu zriadených služieb z pohľadu zákazníka (prehľad VS, diskových kapacít, dátovej prevádzky, virtuálnych sietí, ...)
  - Systémové hlásenia
  - Logovanie činností na virtuálnych zdrojoch
  - Plná podpora Role-based administrácie (aj z pohľadu zákazníka)
  - Dostupnosť Command Line rozhrania so šifrovanou komunikáciou cez SSH
  - Power managment
  - Management snapshotov
  - Šifrovaná komunikácia klient-portál





https://cloudportal.telekom.sk/portal/

Konektivita – možnosti pripojenia do Cloudu

- Vysokokvalitné sieťové prepojenie medzi zákazníkom a dátovým centrom
- Prepojenie garantovaným a bezpečným pripojením MPLS VPN, resp. MetroEthernet (BCN) ku cloudu
- Dedikovaný (garantovaný) prepoj z Cloudu do verejného internetu
- Zdieľaný prepoj s verejnou sieťou ku cloudu
- Kombinácie predchádzajúcich pripojení (s dôrazom na bezpečnosť)

Doplnkové služby s pridanou hodnotou

- „Network Protector“ - nástroj, ktorý umožňuje identifikáciu a ochranu pred útokmi na životne dôležité IT zdroje. Je schopný čeliť DoS (Denial of Service) a DDoS (Distributed Denial of Service) útokom.
- „Analyze NET“ – riešenie, ktoré zlepšuje sieťový monitoring a zjednodušuje správu aplikácií poskytnutím celkovej viditeľnosti siete a aplikačných závislostí. Zabezpečí viditeľnosť do detailnej úrovne sieťových vrstiev a vnorenie sa do problémových oblastí siete alebo aplikácii.
- Mobile Device Management – platforma, ktorá poskytuje možnosť zabezpečenia, konfigurácie, kontroly a centrálneho riadenia vašich inteligentných mobilných zariadení – smartphonov a tabletov. Zariadenia sú pod kontrolou, dáta v nich sú zabezpečené pred stratou a zneužitím.

MobileIron®

Legislatíva / Dôveryhodnosť providera / SLA

- Provider musí spĺňať legislatívne požiadavky, audity, certifikáty a systémy riadenia kvality platné v SR a EU (technologické, bezpečnostné, ISO, ochrana dát, informácií)
- Vysoká kvalita a dostupnosť služieb - silný a stabilný technologický partner
- Dáta na Slovensku
- Cloud platforma neobsahuje žiadne osobné/ citlivé údaje o zákazníkov (iba číslený identifikátor naviazaný na billing)
- Dátové centra ST spĺňajú prísne medzinárodné kritéria a sú na najvyšších technologických úrovniach
- Zmluvne potvrdené a definované SLA (výkonnosť, latencie, dostupnosť, reakčné časy, ochrana informácií)

Záver

- *Je Cloud dostatočne bezpečný? A na akých úrovniach?*
- *Je dostatočne spoľahlivý?*
- *Existuje pocit že organizácia sa zbavuje svojich citlivých dát?*
- *Sú dodržané všetky legislatívne nariadenia/obmedzenia (uchovávanie a ochrana dát a informácií, ...)*
- *Kde sú moje dáta / Kto tam má prístup?*

Odpovede – Argumenty – Fakty

- Objasnenie technologickej kvality riešenia, úrovne cloudu
- Vysvetlenie modelu služby a jeho prínosov pre organizáciu (odbremenenie od starostlivosti o HW, licencií, upgradeov – možnosť sústrediť sa na svoj Core biznis/aplikácie)
- Garancia spoľahlivosti (kvalita a úroveň poskytovania služieb / SLA)
- Provider s preukázateľnými splnenými legislatívnymi podmienkami, auditmi
- Dáta sú stále a výhradne pod kontrolou a vo vlastníctve zákazníka
- Dáta na Slovensku / v chránených priestoroch Providera / Garancia bezpečnosti

Ďakujem za pozornosť