Example projekt 2028–879 - Analýza firmy NUKIBator spol s.r.o

> Cílem tohoto dokumentu je provést základní analýzy a návrh doporučení k infrastruktuře společnosti NUKIBator spol s.r.o.
>
> Daný materiál vychází ze soustavy diskuzí s klientem a cílem je sepsat podle ideálního stavu, porovnat jej s aktuálním stavem
>
> a otevřít nad danou problematikou diskuze, které části lze formou outsourcingu zajistit k IT podpoře co nejdříve.

Podrobnosti k projektu:

```
Název projektu: 2028–879
Datum zadání: 16.01.2025 z ticketu číslo #202829174
Datum počátku projektu: 24.12.2024
Čas prvotní tvorby dokumentu: 24.12.2024 17:28
Zodpovědná osoba: Mgr.Radek Vymazal
```

1. Vyloučení zodpovědnosti

Tento dokument jsou autorizování číst pouze osoby oprávněné.

Materiál obsahuje citlivé informace o

vnitřní infrastruktuře společnosti NUKIBator s.r.o. Bez souhlasu vlastníků není povoleno materiál kopírovat,

ani nijak dále rozšiřovat třetím stranám.

2. Globální vize, širší kontext klienta

Společnost NUKIBator je obchodně-výrobní společnost s předmětem činnosti Myslivost. Se základním kapitálem 1 mil. korun a sídlem v Praze. Se svými počty okolo 110 koncových stanic i ročnímu obratu dle sbírky listin z obchodního rejstříku se svým profilem řadí do kategorie **středně** velkých podniků.

Danou informaci zmiňujeme, protože je to směrodatný faktor dle posuzování, jak by měla v dané kategorii vypadat infrastruktura, jaké jsou finanční možnosti dané společnosti a k tomuto budeme vztahovat posouzení aktuálního stavu s modelovým ideálním stavem.

Hned v úvodu si povíme, že podle článku modelové serverové struktury se svojí topologií společnost NUKIBator řadí do kategorie základní struktury, ale svými ekonomickými ukazateli můžeme společnost NUKIBator považovat že by měla spadat do kategorie minimálně HA-failover i s přihlédnutím k faktu, že mnoho elementů v síti (tedy až na jednotky) nejsou považovány za podnikově kritické.

2. Aktuální stav a jeho nedostatky

Aktuální infrastruktura velmi vyplývá z historického vývoje. Nese typické prvky málo konsolidovatelné infrastruktury.

s přihlédnutím k bodu výše vykazuje svojí topologií prvky poddimezované struktury, která nemá jednoznačnou strojovou i vývojovou filozofii, ale slouží dle diskuze s klientem dostatečně potřebám klienta k dnešnímu dni a s přihlédnutím k technickému vývoji dané doby, kdy se tento audit píše.

Naopak dle diskuze s klientem výhodou celé infrastruktury je, že se v ní nachází poměrně málo kriticky důležitých elementů, což byl pravděpodobně i důvod proč se historicky vedla infrastruktura k tomu, že některé jevy vycházející z tohoto faktu se objevili v ní.

> Máme-li shrnout bodovitě soustavu identifikovatelných bodů, tak dle významnosti je zde seřazujeme:

> 1. Licenční politika infrastruktury s využíváním Windows serverů.
> 2. Nedostatečná segmentace vnitřní sítě.

Pojďme si proto vyjmenovat tyto nedostatky, připodobněme je k ideálnímu modelu a otevřeme na závěr po shrnutí diskuzi, jak s danou problematiku dále pracovat.

2.1 Licenční politika Windows strojů

> Nejproblematičtější je je soustava nekonsolidovaných operačních systémů typu Windows server a jeho licencování.

Ideální stav

1. Všechny stroje mít na jedné verzi operačního systému, například Windows server standard 2024.
2. Všechny linuxové stroje mít na jedné jediné, nejnovější verzi operačního systému, například Debian 12/Ubuntu 24.04 LTS.
3. Mít pro dané prvky předchystané šablony pro tvorbu nových strojů (templates)
4. Mít pro danou soustavu strojů nachystanou orchestraci (Ansible) či pomocí GPO, je-li potřeba provést hromadně nějakou změnu či redeployment nějakého stroje. Filozofie - uchovávat infrastrukturní konfiguraci jako kód.

Aktuální stav

1. Přístupové CAL licence neodpovídají počtu Windows serverům. Jinými slovy máme-li 100 uživatelských přístupů a namixované prostředí různých Windows serveru (2022,2016,2012), měli bychom mít 100 CAL pro WS2022, 100 CAL pro 2016, 100 CAL pro 2012. Jedná se o rizikový prvek z pohledu potenciální hrozby auditu společnosti Microsoft.
2. Licence jsou mix několika verzí, některé nepodporované společnosti Microsoft z důvodu stáří. Vzhledem k tomu, že síť NUKIBator je jeden velký subnet, je to velmi rizikový prvek.

Návrh řešení

1. Zakoupit potřebný počet nejnovějších Windows server licencí. Zvážit, zdali ekonomicky bude lepší nakoupit několik Standard, anebo naopak bude výhodnější finančně datacenter.
2. Zakoupit potřebný počet CAL pro přístupy na servery.
3. Zakoupit potřebný počet RDS CAL (Je možné, že tento bod nebude potřeba, pokud aktuální RDS CAL jsou na nejnovější verzi OS či verzi OS, která se zvolí jako primární).
4. Zanalyzovat, zdali by některé SW byla komplikace migrovat, pokud ano, identifikovat, naleznout úzká hrdla práce.
5. Provést migraci ze starých OS na nové OS.

Daný výše uvedený postup je jen jeden izolovaný jev, jak uvidíme později, má to závislost na aktuální segmentací sítě spolu s potenciální HA strukturou.

2.2 Nedostatečná segmentace vnitřní sítě

> Segmentace vnitřní topologie není realizována.

Ideální stav

Existuje centrální prvek (ideálně v redundanci), který slouží jako centrální firewall. Může to být Mikrotik, Sophos, FortiGate. Zde se nachází inicializace VLAN. Z tohoto prvku vedou VLANs do switche. Zde se může (anebo nemusí) udělat inter-VLAN routing (dle toho jak výkonný by byl firewall).

Určitá suma běžně se vyskytujících VLAN může být:

1. Mgmt VLAN pro management vnitřních prvků
2. LAN pro zaměstnance.
3. VLAN pro ostatní prvky.
4. Tiskárny.
5. Virtuální stroje.
6. Virtuální stroje s omezeným přístupem (DMZ).

7. Kamery.
8. Stroje ve výrobě.
9. Wifi pro hosty.
10. VPN adresace.

Segmentace je firemně specifická, obecně při počtu 100 a více zaměstnanců readresace dává smysl z bezpečnostího hlediska i z adresního hlediska a to i za cenu zvýšení komplexity sítě. Dalším benefitem je segmentace na úrovni poboček. Naprosté minimum je mít alespoň jednu management VLANu.

Aktuální stav

Absence VLAN struktury v síti je naprosto zásadní a z našeho pohledu a další kritický prvek v infrastruktuře. Musíme brát v potaz, že:

- Na některé VM mají přístup dodavatelé třetích stran zvenčí.
- V jednolitém subnetu jsou různé průmyslové stroje, které ne vždy jsou v nejaktuálnějším stavu.
- Koncový uživatelé mají přístupy všude, včetně na prvky core infrastruktury a jejich management.
- Některé VM mají zastaralé verze OS.
- Je otevřeno pro přístup zvenčí služba IIS (webové služby), která smřuje do vnitřního subnetu, kde jsou opět prvky kritické infrastruktury (firewall, core switche, servery)
- Riziko kybernetických útoků roste exponenciálně v čase.
- Každý den jsou objeveny nové zranitelnosti v jinak funkčních systémech.
- Aktuální struktura postrádá i základní management VLANu.
- Nejsou zohledněny adresace například pro ILO(BMC, KVM, iDRac).

V některých topologiích je i možné dedikovat jednu veřejnou adresu pro odchozí traffic z Guest WiFi. Vzhledem k počtu volných veřejných adres, je to doporučené, ne nezbytně nutné.

Zde dodáváme, že jsme se nedívali do detailu na další skladby prvků, ale samozřejmostí by měla být u switchů:

1. Jejich redundance, jedná-li se o část core struktury napříč ve firmě.
2. Monolitost (jeden výrobce po celé struktuře). Případně duplikace dvou různých výrobců vzájemně kompatibilních.
3. Bezpečnostní opatření proti smyčkám či prevence nežádoucímu přístupu do vnitřní sítě.
4. Eliminace nemanagovatelných switchů ve struktuře dále od core struktury.

Literatura

- Cisco tips
- FortiNet lib

3. Shrnutí a návrh řešení

Na základě získaných poznatků jsme identifikovali úzká hrdla a nejrizikovější komponenty vně sítě. Po celou dobu jsme hovořili o ideálním stavu a porovnali jej s aktuálním stavem. Nyní je potřeba otevřít k diskuzi možné řešení, jak provést zarovnání technologických dluhů a různých nedostatků.

Navrhujeme dle úvodního mailu se zaměřit na jadernou sturkturu a tedy řešit i následující formu zlepšení, nedostatků vně sítě, konsolidací, kterou rozdělujeme na:

1. Hardware
2. Software
3. Realizace

a tak dále...