PŘÍPADOVÁ STUDIE
MALÉ UBYTOVACÍ ZAŘÍZENÍ

Relax Point Hynčice s.r.o.

Technické řešení

CYBEREE

POČÍTAČOVÁ SÍŤ

Původní počítačová síť byla založena na doméně Active Directory s jedním doménovým řadičem na Windows Server 2008. Group Policy nebylo prakticky nijak nakonfigurované a celé doménové prostředí sloužilo prakticky jen pro centrální ověřování uživatelů. Počítačové stanice byly počítače s Windows XP nebo Windows 7 připojené do domény. Doménový řadič současně sloužil i jako souborový server, tiskový server a server vzdálené plochy publikovaný přes standardní RDP protokol do celého internetu.

Cílem byla modernizace celého prostředí, zvýšení dostupnosti domény, vyřešení vzdáleného přístupu, provoz online rezervačního systému a zabezpečení celého prostředí.

Navržené řešení spočívalo v pořízení nového serveru, který by byl vhodný i pro potřeby virtualizace. Nezbytný byl upgrade stávajících počítačů, které byly z velké části provozované na Windows XP a nic novějšího nepodporovaly. A nasazení nového Active Directory forestu a domény, jelikož stávající byla značně zastaralá a vzhledem k nulové konfiguraci se prakticky jednalo jen o založení nových účtů. Upgrade by šel řešit přidáním nového řadiče, upgrade prostředí domény (FFL a DFL), vyčištěním, úpravou struktury objektů a konfigurace, ale v tomto případě bylo jednodušší začít zcela od nuly.

Pro nákup serveru padla volba na HPE ProLiant ML30 Gen10 / E-2124 / 32GB s Windows Server 2022 Standard, jelikož se jedná o naprosto dostatečné a cenově dostupné řešení pro malou firmu. Protože se jedná o ubytovací zařízení, počítače jsou využívány minimálně, nikoliv pro plnohodnotnou celodenní práci. Z důvodu úspory nákladů padla volba na repasované počítače DELL s 8 GB RAM, 256 SSD a podporou Windows 11.

Fyzický server slouží pouze pro účely virtualizace. Edice Standard operačního systému Windows Server 2022 umožňuje provoz dvou plnohodnotných instancí operačního systému Windows Server, tedy fyzický server + jeden virtuální server, případně dva virtuální servery, pokud se fyzický server používá pouze pro potřeby virtualizace.

Virtualizace je řešena pomocí Hyper-V, které je součást operačního systému Windows Server. Nad Hyper-V jsou provozovány dva virtuální servery – jeden jako doménový řadič se službou DNS a druhý jako terminálový server pro vzdálený přístup uživatelů. Třetí server je GNU/Linux a slouží pro provoz online rezervačního systému.

Active Directory

Active Directory byla nakonfigurována za účelem maximálně bezobslužného a bezúdržbového provozu s důrazem na zabezpečení. Maximum možných věcí je

automatizovaných a centrálně řízených pomocí Group Policy. Na koncových stanicích není potřeba žádná ruční konfigurace. Vše je řízeno centrálně pomocí Group Policy.

Z důvodu požadavku na maximální zabezpečení byl nasazen Tier model Active Directory, kde jsou striktně odděleny doménové řadiče a privilegované účty (Domain Admin / Schema Admin / Enterprise Admin), servery a serverové účty a uživatelské počítače s uživatelskými účty.

Vysoká dostupnost Active Directory je zajištěna pomocí druhého doménového řadiče umístěného v geograficky oddělené lokalitě (jiný objekt v rámci dané firmy). Z důvodu úspory financí byl pro druhý doménový řadič použit repasovaný hardware.

Terminálový server

Terminálový server slouží pro vzdálené přihlašování uživatelů. Vzdálený přístup je primárně potřeba kvůli účetnímu software, na který je potřeba mít přístup odkudkoliv.

Jedná se o Windows Server 2022 s rolí vzdáleného přístupu a brány vzdáleného přístupu. Nastavení vzdáleného přístupu je maximálně zabezpečeno, aby se zamezilo zneužití. Terminálový server navíc není dostupný z celého internetu, ale pouze z vybraných lokalit, navíc zabezpečen pomocí IPS/IDS na Unifi Dream Machine Pro (více viz níže) před různými typy síťových útoků.

INTERNÍ SÍŤ A SÍŤ PRO HOSTY

Připojení k internetu je v dnešní době velmi důležité. A to jak pro interní potřeby, tak u ubytovacích a stravovacích zařízení také pro potřeby hostů, kteří očekávají kvalitní Wi-Fi ve všech prostorech.

Interní síť byla původně řešena pomocí domácích switchů a Wi-Fi routerů TP-Link. Všechno bylo součást jedné sítě, jen Wi-Fi pro hosty měla vlastní SSID. Jako přístupové body sloužily taktéž Wi-Fi routery, jen zapojené do LAN portů tak, aby fungovaly jako přístupové body. Každý ubytovací objekt měl původně pouze jeden Wi-Fi přístupový bod, což znamenalo, že na některých pokojích byl signál velmi špatný a někde signál nebyl vůbec.

Všechny původně používané síťové prvky jsou určeny pro domácnosti, mají velmi omezené možnosti konfigurace, žádné možnosti centrální správy nebo dohledu a prakticky neexistující podporu.

Navržené řešení spočívalo v zakoupení síťových prvků Unifi od společnosti Ubiquiti. Síťové prvky Unifi jsou velmi populární a vhodné jak do domácností, tak i do malých až středních firem. To je také důvod, proč se na ně specializujeme a našim zákazníkům je doporučujeme.

Jako router/gateway slouží Unifi Dream Machine Pro s 8 RJ45 LAN porty, jedním RJ45 WAN portem a dvěma 10 Gbit SFP+ porty použitelnými pro LAN i WAN. Jako switche slouží řada USW Lite (5, 8 nebo 16 portů včetně napájení PoE). Jako přístupové body slouží AC Long Range.

Všechny síťové prvky mají centrální správu pomocí webové konzole nebo mobilní aplikace, pokročilé možnosti konfigurace, monitoringu a pravidelné aktualizace.

Obrázek 1 - Přehled a statistiky síťového provozu na Unifi Dream Machine Pro

Type	Name	Application	Status	IP Address	Uplink	Parent Device
	Relax	Network	Online		GbE	CETIN a.s.
	hospudka-kancelar-s...	Network	Up to date		GbE	Relax Port 1
	skola-switch-5p	Network	Up to date		GbE	hospudka-kancelar-...
	penzion-switch-5p	Network	Up to date		GbE	skola-switch-5p Por...
	domecek	Network	Up to date		GbE	hospudka-kancelar-...
	penzion-prizemi	Network	Up to date		FE	penzion-switch-5p ...
	penzion-patro	Network	Up to date		GbE	penzion-switch-5p ...
	hospudka-kancelar	Network	Up to date		FE	hospudka-kancelar-...
	skola-prizemi	Network	Up to date		GbE	skola-switch-5p Por...
	skola-patro	Network	Up to date		FE	skola-switch-5p Por...

Obrázek 2 - Seznam aktivních síťových prvků Unifi a jejich stav

ODDĚLENÍ SÍTĚ PRO HOSTY OD INTERNÍ SÍTĚ

Síť byla rozdělena do 3 virtuálních sítí (VLAN). Jedna síť slouží pro interní potřeby – tam jsou zapojeny počítače zaměstnanců, servery nebo například tiskárny. Druhá síť slouží pro „internet věcí" (IoT), tedy všechny možné chytré krabičky a spotřebiče připojené k internetu. Třetí síť slouží pro hosty.

Interní síť má plný přístup do internetu a zařízení mezi sebou mohou komunikovat. Jako DNS se v interní síti používají výhradně doménové řadiče. Interní síť je tvořena jak pomocí LAN (servery, počítače, některé tiskárny), tak pomocí interní Wi-Fi (mobilní telefony, tablety, notebooky, některé tiskárny) s RADIUS ověřováním napojeným na doménu Active Directory.

Síť pro internet věcí je z bezpečnostních důvodů oddělená. Osobně nevěřím těmto chytrým zařízením a tomu, že neobsahují zranitelnosti a nemohou být zneužity. Proto tato síť je izolovaná jak od ostatních sítí, tak i jednotlivá zařízení v rámci sítě jsou navzájem izolovaná a nevidí na sebe. Možný je pouze přístup do internetu. Tato síť běží jak po LAN (některé IoT zařízení jsou připojeny LAN kabelem), tak i po Wi-Fi. Ověřování je pomocí hesla (WPA2-PSK) s omezením pouze na vybrané MAC adresy.

Síť pro hosty je opět izolovaná od ostatních sítí a také zařízení mezi sebou na sebe nevidí. Síť pro hosty běží pouze na Wi-Fi (LAN připojení není hostům poskytováno). Na připojení k internetu jsou aplikována omezení, jako například omezení rychlosti pro jednotlivá připojená zařízení, blokování nelegálního obsahu, P2P sítí a také blokování stránek pro dospělé (na Wi-Fi se připojují i děti). Rychlost pro hosty je výrazně omezena, protože na Wi-Fi se může připojit prakticky kdokoliv – heslo není žádné tajemství, ale je vylepené na

dveřích všech objektů. Ubytovaní hosté ale dostávají speciální vouchery, které jim zajistí výrazně rychlejší připojení k internetu po dobu jejich pobytu.

Díky instalaci nových přístupových bodů a dalších síťových prvků je zajištěn plný centrální a vzdálený management celé sítě. Nové přístupové body v jednotlivých objektech jsou umístěny tak, že celé objekty včetně všech pokojů mají výborné pokrytí Wi-Fi signálem, a tedy rychlý a spolehlivý internet pro hosty i zaměstnance.

KAMEROVÝ SYSTÉM

Protože se v ubytovacích a stravovacích objektech pohybuje velké množství lidí a v minulosti docházelo k různým větším či menším krádežím nebo vandalismu, doporučili jsme instalaci kamerového systému do společných prostor.

Unifi Dream Machine Pro, které je použité jako hlavní router a gateway, má i slot na jeden pevný disk a umí sloužit jako záznamové zařízení pro bezpečnostní kamery Unifi. Po diskuzi jsme vzhledem k požadavkům doporučili kamery G5 Bullet a G5 Dome. Tyto kamery představují velmi kvalitní, ale přitom cenově dostupné řešení.

Kamerový systém je plně integrovaný do centrálního managementu Unifi, nabízí široké možnosti konfigurace, má detekci pohybu, lidí i aut a záznamy se ukládají lokálně za vyměnitelný pevný disk. Obraz z kamer lze v reálném čase i zpětně v historii sledovat jak pomocí aplikace pro mobilní telefony, tak i pomocí webového prohlížeče.

Z mého pohledu se jedná o vhodné řešení za rozumnou cenu. Ukládání záznamu lokálně na pevný disk vidím jako velkou výhodu jak z pohledu nákladů (cloudové ukládání záznamu bývá placené, navíc s omezenou délkou záznamu), tak i z pohledu ochrany soukromí, protože záznamy se drží lokálně na vlastním zařízení v objektu dané firmy.