

Případová studie:

Zabezpečení a zálohování firemní sítě s 50 počítači

1. Úvod

Tato případová studie představuje komplexní řešení pro zabezpečení a zálohování firemní sítě s 50 počítači. Cílem je ochránit data před kybernetickými hrozbami, jako je ransomware, ztráta dat a narušení provozu. Studie zahrnuje analýzu aktuální situace, návrh řešení, jeho implementaci, testování a dlouhodobou údržbu.

2. Analýza aktuální situace

Byly identifikovány následující slabiny:

- Chybějící centrální zálohovací systém
- Absence automatických záloh a pravidelného testování
- Bez segmentace sítě, což zvyšuje riziko šíření škodlivého software
- Uživatelská přístupová práva, která nejsou dostatečně omezená

3. Návrh řešení

Navržené řešení zahrnuje:

- NAS zařízení Synology DS1524+ nebo QNAP TS-453D
- Profesionální zálohovací software (Veeam Backup nebo Acronis Cyber Protect)
- Segmentaci sítě pomocí VLAN
- Automatické zálohy na NAS, do cloudu a na externí HDD
- Šifrování dat a monitorování stavu záloh

4. Implementace

Implementace zahrnovala instalaci NAS zařízení, konfiguraci zálohovacího softwaru, segmentaci sítě a zavedení cloudových záloh. Byly nastaveny zálohovací politiky a provedeno testování.

5. Testování a monitorování

Testování zahrnovalo obnovu dat z lokálních i cloudových záloh, kontrolu přístupů a simulaci výpadků. Pravidelné monitorování zajistilo průběžnou kontrolu záloh.

6. Dlouhodobá údržba

Zahrnuje pravidelné aktualizace, testování obnovy, auditů bezpečnosti a školení zaměstnanců.

7. Náklady a časová náročnost

Orientační náklady na řešení:

- NAS Synology DS1522+: 18 500 – 21 800 Kč
- Zálohovací software Veeam: 10 000 – 15 000 Kč ročně
- Acronis Cyber Protect: 4 000 – 6 000 Kč ročně na zařízení
- Pevné disky: 12 000 – 15 000 Kč
- Cloudové úložiště: 100 – 200 Kč měsíčně za TB
- Doba implementace: 8 – 11 pracovních dnů

8. Výhody navrhovaného řešení

- Zvýšená ochrana dat před ransomwarem a jinými hrozbami.
- Snadná správa a rychlá obnova dat v případě výpadku.
- Přizpůsobitelné řešení pro různé firemní potřeby.
- Kombinace lokálních a cloudových záloh pro vyšší bezpečnost.
- Průběžné monitorování a jednoduchá správa.

9. Časté dotazy (FAQ)

Jak často by měly být zálohy prováděny?

Doporučujeme denní inkrementální zálohy a týdenní plné zálohy.

Jaké jsou výhody cloudového zálohování?

Cloudová záloha chrání data před fyzickými hrozbami, jako je požár nebo krádež.

Je nutné školit zaměstnance?

Ano, zaměstnanci by měli být proškoleni o kybernetické bezpečnosti a postupech obnovy dat.

Kontaktujte nás

Helpio je váš spolehlivý partner pro IT outsourcing. Kontaktujte nás a společně navrhujeme řešení, které bude odpovídat vašim potřebám. Zajistíme bezpečnost vašich dat a plynulý chod vaší firmy.