DNS Professional services

Servisní a profylaktická podpora CyberVault řešení

Roční paušální služba expertní údržby a L3 podpory pro prostředí Nemocnice TGM Hodonín

Služba je určena pro již implementované řešení Dell CyberVault a navazuje na předchozí projekt Konzultace a implementace CyberVault řešení. Cílem služby je udržovat celé prostředí v podporovaném, bezpečném a provozně ověřeném stavu, omezit riziko provozních výpadků a zajistit, aby bylo řešení v případě bezpečnostního incidentu reálně použitelné pro obnovu dat.

Popis služby

CyberVault není jedno izolované zařízení, ale komplexní celek tvořený zálohovacím prostředím, trezorovým úložištěm, řídicími servery, bezpečnostními technologiemi, síťovou infrastrukturou a provozními postupy. Jednotlivé části musí být dlouhodobě udržovány v konzistentním a podporovaném stavu. Výpadek nebo nekonzistence jedné komponenty může v praxi znamenat nefunkčnost celého řetězce ve chvíli, kdy je jeho dostupnost nejkritičtější.

Služba je proto koncipována jako pravidelný expertní dohled a profylaktická údržba celého CyberVault řešení, nikoliv jako dílčí servis samostatných zařízení. DNS a.s. zajišťuje odbornou L3 podporu, kontrolu vazeb mezi komponentami, doporučení pro další údržbu, součinnost při incidentech a koordinaci komunikace s výrobci technologií.

Služba obsahuje:

- Roční paušální podporu již implementovaného CyberVault řešení.
- Pravidelnou kvartální profylaxi celého prostředí v rozsahu 4× ročně.
- Expertní L3 technický dohled nad řešením a jeho vzájemnými vazbami.
- Operativní součinnost při řešení eskalovaných incidentů a provozních problémů.
- Vyhodnocení doporučených aktualizací, firmware a patchů pro relevantní komponenty.
- Kontrolu provozní připravenosti řešení pro scénáře obnovy dat.
- Součinnost s Dell Technologies Support a s výrobcem datové diody.
- Odborné konzultace k provozu, údržbě a rozvoji CyberVault prostředí.
- Stručný servisní report po provedení profylaxe včetně doporučení dalších kroků.

Rozsah podporovaného prostředí

Služba se vztahuje na komponenty implementované v rámci CyberVault řešení, zejména na následující oblasti:

Oblast	Předmět údržby a kontroly
Dell PowerProtect Data Domain	Kontrola zdravotního stavu, kapacity, verzí, replikací a vazeb mezi produkční a trezorovou částí.
Cyber Recovery Manager	Kontrola konfigurace, úloh, Secure Copy procesů, dostupnosti a návaznosti na trezorové prostředí.

Servery a operační systémy	Kontrola provozního stavu řídicích a servisních serverů, včetně relevantních aktualizací a konfigurací.
Backup software a vazby na produkci	Ověření návaznosti zálohovací části řešení na CyberVault scénáře a doporučení úprav podle provozního stavu.
Networking a segmentace	Kontrola síťových vazeb, dostupnosti, základních konfiguračních souvislostí a dopadů změn na funkčnost řešení.
Data Diode	Kontrola funkčnosti, dostupnosti aktualizací, základní údržba a součinnost s výrobcem zařízení při řešení incidentů.
CyberSense analytika	Volitelně, pokud je součástí konkrétní implementace a je zahrnuta do sjednaného rozsahu služby. Kontrola funkčnosti, dostupnosti aktualizací, základní údržba a součinnost s výrobcem software při řešení incidentů.

Pravidelná profylaxe

Profylaktické práce jsou prováděny plánovaně, zpravidla čtvrtletně, po vzájemné dohodě s partnerem a zákazníkem. Jejich cílem je předcházet provozním problémům, včas identifikovat rizikové stavy a udržovat řešení v dlouhodobě podporovaném stavu.

- Kontrola funkčnosti a dostupnosti klíčových komponent CyberVault prostředí.
- Kontrola verzí software, firmware, hotfixů a dostupných doporučení výrobců.
- Analýza chybových logů a systémových událostí.
- Kontrola kapacitních parametrů a vytížení systémových zdrojů.
- Kontrola replikačních a Secure Copy úloh.
- Kontrola funkčnosti datové diody a souvisejících přenosových mechanismů.
- Vyhodnocení zjištění a návrh doporučených nápravných opatření.

Expertní technická podpora

V rámci služby je poskytována expertní podpora úrovně L3. DNS a.s. vstupuje do řešení jako odborná eskalace pro partnera nebo zákazníka, zejména v případech, kdy je potřeba hlubší znalost architektury CyberVault řešení, jeho konfigurace a vazeb mezi jednotlivými komponentami.

- Diagnostika eskalovaných incidentů a nestandardního chování prostředí.
- Analýza příčin problémů a návrh nápravných opatření.
- Součinnost při komunikaci s Dell Technologies Support.
- Součinnost při komunikaci s výrobcem datové diody.
- Konzultace při plánování aktualizací, změn a obnovovacích scénářů.
- Doporučení pro minimalizaci rizik ovlivňujících obnovitelnost dat.

Doplňkové služby (volitelné):

- Změna architektury CyberVault řešení.
- Testovací obnova vybraných systémů nebo aplikací nad rámec běžné kontroly připravenosti.
- Aktualizace nebo rozšíření technické dokumentace nad rámec servisního reportu.

Vymezení služby

Služba představuje expertní servisní a profylaktickou podporu řešení. Nejedná se o provozní HelpDesk, Service Desk ani službu nepřetržité hotline pro koncové uživatele.

- Služba nezahrnuje L1/L2 HelpDesk ani přijímání požadavků od koncových uživatelů zákazníka.
- Služba nezahrnuje garantovanou 24×7 hotline.
- Služba nenahrazuje výrobní podporu Dell Technologies ani podporu výrobců třetích stran.
- Služba nezahrnuje dodávku hardware, software, licencí ani servisních kontraktů výrobců.
- Služba nezahrnuje rozsáhlé projektové změny, migrace, redesign prostředí ani obnovu produkčních systémů jako garantovaný výsledek.
- Služba nezahrnuje zásahy do systémů a služeb, které nebyly součástí implementovaného CyberVault řešení.

Součinnost příjemce služby

Pro úspěšné doručení služby je nutná součinnost partnera a zákazníka. Během poskytování služby může být příjemce služby požádán zejména o zajištění vzdáleného přístupu, platných přístupových údajů, souhlasu se servisním oknem, dostupnosti administrátorů, informací o provedených změnách, přístupu k relevantním logům a součinnosti při komunikaci s výrobci.

V případě neposkytnutí potřebné součinnosti, nedostupnosti prostředí nebo změn provedených mimo dohodnutý postup nemusí být možné garantovat dokončení plánovaných činností v původně sjednaném rozsahu. Čas strávený nad rámec sjednané služby může být řešen formou Engineer time.

Způsob doručení služby

- Služba je poskytována primárně vzdáleně, pokud není pro konkrétní činnost dohodnuto jinak.
- Služba je doručována v pracovní dny, v čase od 8:00 do 17:00.
- Služba je doručována konzultantem s odpovídající odborností a zkušenostmi v oblasti Dell Data Protection a CyberVault řešení.
- Každá kvartální profylaxe je ukončena stručným servisním reportem s popisem provedených činností a doporučených návazných kroků.
- Služba je platná v rámci České republiky.

Přínosy služby

- Pravidelné ověřování stavu řešení chránícího kritická data zákazníka.
- Snížení rizika výpadku způsobeného zastaralými verzemi, chybovou konfigurací nebo nekonzistencí mezi komponentami.
- Rychlejší řešení eskalovaných incidentů díky znalosti konkrétního prostředí.
- Lepší připravenost řešení pro obnovu dat po kybernetickém incidentu.
- Jednoznačné vymezení role DNS jako expertní L3 podpory vůči partnerovi a zákazníkovi.
- Nižší administrativní zátěž oproti opakovanému objednávání jednotlivých zásahů.

Poznámka: Konkrétní rozsah služby, periodicita profylaxí, reakční režim a cena budou potvrzeny v obchodní nabídce a případné smluvní dokumentaci.