

Zálohování do cloudu - efektivní způsob ochrany malé firmy před velkou katastrofou

14.8.2025 - | České Radiokomunikace

Ztráta dat může být pro firmu likvidační, a přitom jí lze snadno předejít. Podívejte se, co všechno cloudové zálohy poskytují, jak fungují a proč je rozumné je používat i v malých a středních firmách.

Na malém podnikání už dávno není nic malého. Malé a střední podniky, ač si to málokdo uvědomuje, hrají ve společnosti velice významnou ekonomickou i sociální roli. V Evropě tvoří více než 90 % všech podniků, na tvorbě HDP se podílejí 60 % a zaměstnávají přes 40 % obyvatel[1]. Vnímání rizik spojených se ztrátou, poškozením nebo zneužitím firemních dat jejich vedoucími manažery, zvláště pak manažery menších firem, však bývá často velmi rozporuplné. Představa, že „malým firmám se nic nemůže stát“, je ve skutečnosti mylná a nebezpečná.

To nejcennější, co firma může mít

V dnešní době jsou data často tím nejcennějším, co firma má. Stroje lze opravit, zaměstnance získat či vyškolit – ale ztracená data se ne vždy podaří obnovit. Možností, jak o ně přijít, je mnoho – od lidské chyby, úmyslného poškození či technické závady, přes krádež zařízení a kybernetický útok až po přírodní katastrofu. Bez ohledu na příčinu ztráta dat téměř vždy přináší nečekané náklady, ztrátu času a řadu komplikací. Připočteme-li narušenou důvěru klientů a partnerů, možné sankce a vysoké finanční ztráty z přerušeného provozu, může být pro menší podniky taková situace až likvidační.

Statistiky jsou neúprosné

Téměř 40 % malých podniků oznámilo po kybernetickém útoku významnou ztrátu dat. Výzkumy ukazují, že až 75 % malých a středních podniků by mělo značné potíže pokračovat v činnosti, kdyby se například staly terčem ransomwarového útoku[2]. A 51 % obětí ransomware raději rovnou zaplatilo masné výkupné[3], jen aby svoje data získaly zpět. Statistiky IBM a NASDAQ uvádějí, že po útoku ransomware 22 % malých firem skončí s podnikáním, a pokud je ztráta dlouhodobá zanikne 93 % firem, které přišly a svoje data[4]. Přesto mnozí i dál strkají hlavu do písku.

Zálohy nejsou všelék: proč testování a plán obnovy rozhodují

Mnoho malých a středních firem dnes už svá data nějakým způsobem zálohuje, ale jen zhruba polovina pravidelně testuje. Standardy ISO 22310 se v Česku implementují pomalu a 21 % firem, které alespoň zálohuje, nemá ani plán obnovy, ani pravidelné ověřování jeho funkčnosti[5]. Přitom právě plán obnovy (Disaster Recovery Plan) je klíčovou součástí strategie pro rychlou obnovu firemních dat a provozu klíčových systémů. Netestované zálohy navíc mohou být velice zrádné. Např. ransomware než požádá o výkupné, může týdny ba i měsíce šifrovat firemní data, aniž by si toho někdo všiml, a to včetně záloh. A zašifrované zálohy jsou k ničemu. Pokud jde o podíl malých firem, které mají alespoň základní strategii zálohování, například 3-2-1, čísla jsou bohužel stále alarmující.

Stáhnout data ještě neznamená zálohovat

Stáhnout jednou za čas data na přenosný disk uložený v šuplíku nebo na druhý server v serverovně rozhodně nestačí. Disk stejně jako záložní server se může pokazit. Ukládat data na sever na jiné pobočce je sice bezpečnější, ale ruku na srdce, kolik menších firem má pobočky technicky připravené k zálohování dat z centrály i z dalších lokalit? A kam zálohovat data ze záložní pobočky, a

kdo se v těch zálohách ještě dokáže vyznat?

Záloha má sloužit k plné obnově dat, pokud o ně firma přijde. Musí proto obsahovat nejenom pracovní data, ale i konfigurace systémů, obsahy a struktury databází, metadata a informace o přístupových právech. Důležité je mít rovněž zálohy firemních e-mailů, popř. dat z firemního intranetu a dalších součástí podnikového informačního systému. Jinak se může stát, a stává se, že firma sice má zálohu, ale zrekonstruovat z ní původní systém jednoduše nedokáže. Zálohování musí navíc být v souladu s požadavky GDPR.

Zálohování do cloudu

Zálohování do cloudu je ideálním řešením právě pro malé a střední firmy. Zálohy se ukládají přes bezpečné a šifrované spojení na vzdálené cloudové servery poskytovatele cloudových služeb. Bezpečnost a dostupnost záloh pak leží na jeho bedrech. Zálohy jsou dostupné odkudkoliv bez nutnosti fyzického přístupu k zálohovacím zařízením, což mimo jiné umožňuje třeba po povodni nebo požáru obnovit firemní IT i v jiném místě, než bylo původně umístěno, a výrazně tak urychlit oživení celého provozu firmy. K dalším přednostem cloudového zálohování patří zejména:

možnost automatizace záloh, která snižuje riziko, že někdo zapomene zálohu vytvořit a uložit, možnost zvětšit objem zálohovaných dat bez investic do vlastního nového hardwaru, rychlejší, spolehlivější a asistovaná obnova, redundance, většina solidních poskytovatelů zálohuje svoje cloudová data v dalších geograficky oddělených lokalitách a prakticky tak eliminuje možnost ztráty nebo poškození zálohy.

Přechod k zálohování do cloudu většinou není nijak komplikovaný. Vzdálené cloudové úložiště se bez nějakých zásadních změn prostě připojí do prostředí klienta. Specialisté poskytovatele mohou pomoci i s přípravou strategie a plánu obnovení provozu po havárii, katastrofě nebo incidentu, navrhnou a připraví zálohování tak, aby obnova byla spolehlivá, co nejjednodušší a nejrychlejší. Klient se tak zbaví nejen starostí se zálohováním, ale může si být jist, že v i případě té nejhorší katastrofy se jeho byznys nadlouho nezastaví.

Zálohování a obnova dat v cloudu CRA

Jednoduché, rychlé, plně integrované a finančně nijak náročné cloudové zálohování a obnova dat využívající zálohovací software Veeam Backup & Replication a Microsoft 365 Cloud Backup, poskytuje jistotu v okamžicích, kdy o budoucnosti firmy mohou doslova rozhodovat minuty. Zálohovat a obnovit lze nejenom určitá data, ale třeba i rovnou celý firemní IT provoz. Veškerá data, jak aktuálně používaná, tak i uložená, jsou šifrována a neopustí Českou republiku.

Zajištění dostupnosti kritických infrastrukturních prvků dosahuje až 99,999 %, což jinými slovy znamená, že celkový maximální roční výpadek služeb nepřesáhne 5 minut. Unikátní cloudová platforma VIRTIX poskytuje snadné ovládání a nastavování všech cloudových služeb. CRA disponují všemi nezbytnými certifikacemi a jejich specialisté pomohou i s návrhem a přípravou řešení Disaster Recovery a Business Continuity plánů.

Veeam Cloud Connect, Microsoft 365 Cloud Backup nebo jenom virtuální NAS? Veeam Cloud Connect představuje snadné, efektivní a plně integrované cloudové zálohování. Vzdálené cloudové úložiště si klient jednoduše připojí ke své infrastruktuře a může začít zálohovat. Nevyžaduje žádné změny firemní IT architektury a obnova se provádí přímo z uživatelského rozhraní na straně klienta, který tak má všechno pod absolutní kontrolou.

Zálohování v prostředí Microsoft 365 zamezí ztrátě dat, ať už je způsobí lidská chyba nebo kybernetický útok, a zajistí rychlou obnovu e-mailů, souborů a sad Microsoft 365 nebo Office 365. I

zde má uživatel plnou kontrolu nad zálohovanými položkami.

Virtuální síťové úložiště, NAS, nabízí jednoduchý přístup přímo prostřednictvím protokolů NFS a CIFS, silné zabezpečení a samozřejmě podporu Active Directory a LDAP.

Ochrana je vždy levnější, než řešení následků

Platí to obecně – a zálohování není výjimkou. Ignorování rizik, víra, že „mně se to stát nemůže“, nebo pouhé stěžování si na cenu ještě nikdy nikoho před ztrátou dat neochránily. Efektivní, spolehlivé a promyšleně navržené cloudové zálohování však ano.

Podívejte se na web nebo si přijďte o zálohování nezávazně popovídat.

Kontaktujte nás

[1]
https://single-market-economy.ec.europa.eu/system/files/2023-08/Annual%20Report%20on%20European%20SMEs%202023_FINAL.pdf

[2] <https://www.sciencedirect.com/science/article/pii/S0167404824001275>

[3] <https://www.strongdm.com/blog/small-business-cyber-security-statistics>

[4] <https://www.comimpex.cz/blog/co-je-dobre-vedet-a-co-nepodcenit-u-zalohovani-dat>

[5] <https://fpvmv.umb.sk/data/page/umb.sk/24334/bezpecnostne-forum-2024.pdf>

<https://www.cra.cz/tiskove-centrum/cloud/zalohovani-do-cloudu-efektivni-zpusob-ochrany-male-firmy-pred-velkou-katastrofou>