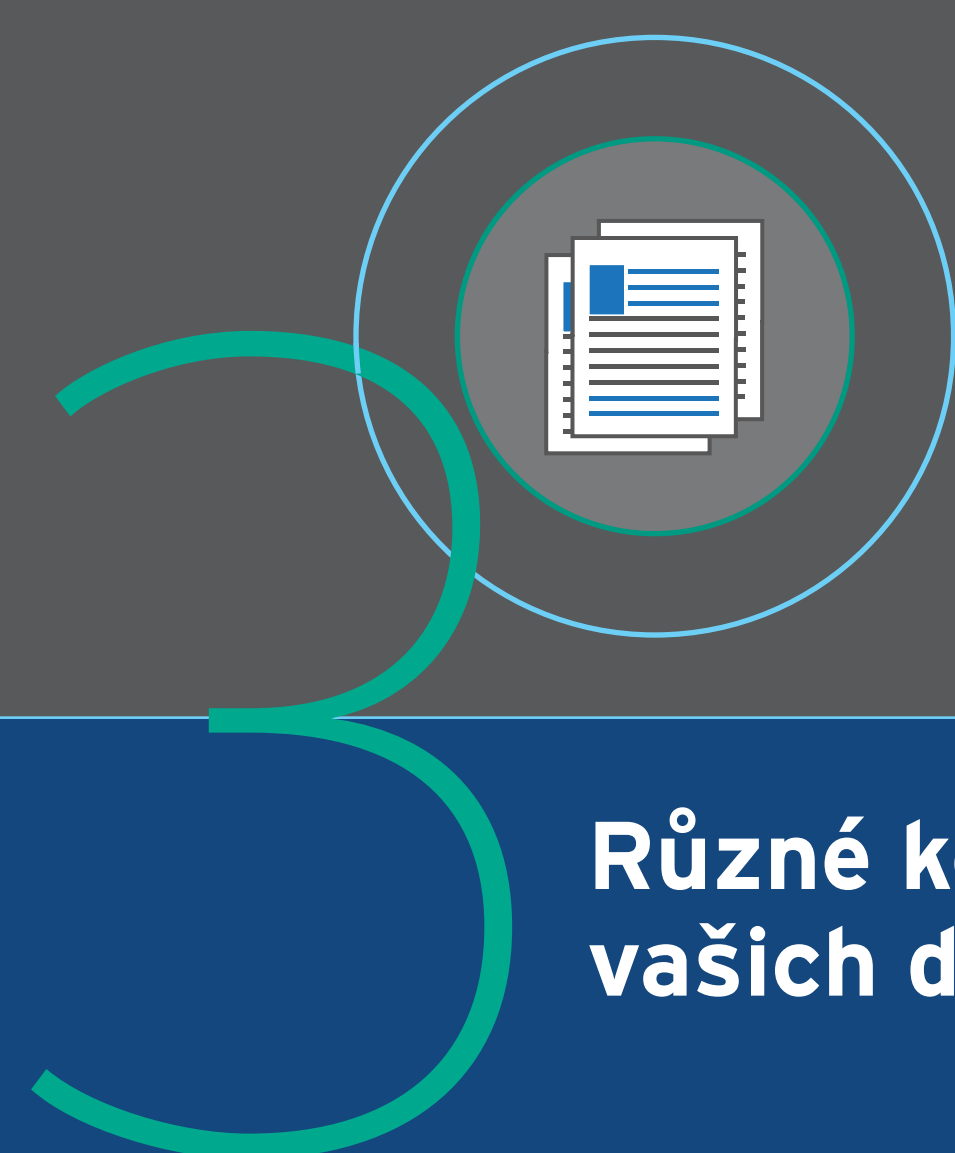


# STRATEGIE PRO ÚSPĚŠNOU OCHRANU DAT: 3-2-1-1-0

Pokud připravujete svou organizaci na prevenci kybernetických útoků, je také důležité přemýšlet o tom, jak se zotavit, pokud dojde k nejhoršímu scénáři. Pokyny pro dlouhodobé zálohování dat konzistentně nabízely strategii 3-2-1. Tedy tři kopie vašich dat. Dvě různá média a jedna kopie uložena mimo pracoviště. I tato strategie se dále vyvíjí. Zlatý standard je nyní 3-2-1-1-0 a zde je důvod, proč je nový přístup tak důležitý.

Gartner předpovídá, že nejméně **75 %** IT organizací bude do roku 2025 čelit jednomu nebo více útokům ransomwaru.

> [zdroj](#)



**Různé kopie vašich dat**



**Typy médií pro ukládání**



**Kopie, která je uložena offsite**



**Kopie, která je uložena offline**



**Zalohování bez chyb**

## PROČ 3 KOPIE?

Tři kopie vašich dat zahrnují vaše primární data plus dvě záložní kopie. Kromě jakékoli rychle obnovitelné záložní kopie by měly existovat také skutečné zálohy.

## PROČ ROZDÍLNÁ MÉDIA?

Tyto tři kopie by měly být uloženy alespoň na dvou různých typech paměťových médií. Vzhledem k tomu, že se tolik aplikací, dat a řešení úložiště přesouvá do cloudu, je důležité rozdělit úložiště mezi cloudová a místní úložiště.

## H2: PROČ OFFSITE?

To, jak jsou vaše cloudové zálohy uloženy, je často spojeno se strategií ochrany dat vašeho poskytovatele cloudu. Nejlepší je zajistit, aby byla kopie těchto dat prakticky izolovaná od produkční sítě. Při přípravě na přírodní katastrofy se ujistěte, že alespoň jedna záložní kopie se fyzicky nachází na jiném místě, než je hlavní záloha v případě hurikánu, povodně nebo jiné přírodní katastrofy.

## H2: PROČ OFFLINE?

Když má záloha fyzickou podobu, ransomware se k ní nemůže dostat. Tato kopie je oddělena od vaší sítě, kde se nachází ta primární. Pokud je primární kopie nebo místní záloha poškozena nebo ohrožena, lze offline zálohu použít k obnovení. Často se jedná o zálohu na datové pásce. Softwarové vzduchové mezery běžné při ukládání objektů jdou daleko, ale když se snažíte chránit data, nic nepřekoná fyzickou vzduchovou mezeru.

## H2: PROČ ŽÁDNÉ CHYBY?

Kopie 0 je záloha bez chyb, která je neměnná a nelze ji žádným způsobem změnit. Obvykle je držena offline a lze ji použít k zotavení po útoku ransomwaru. Aby bylo zajištěno zachování nulových chyb, mělo by být monitorování dat prováděno denně. Chyby musí být opraveny, jakmile jsou identifikovány.

**39 %** organizací SMB nemá plán, jak postupovat při kybernetickém útoku a úniku dat.

> [Zdroj](#)

Strategie zálohování 3-2-1-1-0 snižuje dopad každého bodu selhání. Vzhledem k tomu, že útoky ransomwaru neustále přibývají, plánujte dopředu, abyste se ujistili, že vaše strategie ochrany dat bude fungovat.

## DOZVĚDET SE VÍCE O ŘEŠENÍ IRON MOUNTAIN

**Úschova a záloha datových médií**  
Společnost Iron Mountain spojila své síly s předními poskytovateli cloudového zálohování Carbonite a Veeam, aby nabídla rozšířenou ochranu dat pro podniky všech velikostí.

- **Bezpečná likvidace a recyklace IT vybavení**