IRON MOUNTAIN®

TWOJA SKUTECZNA STRATEGIA OCHRONY DANYCH: 3-2-1-1-0

Przygotowując swoją organizację do zapobiegania cyberatakom, należy zastanowić się, jak powrócić do normalnego funkcjonowania w przypadku najgorszego scenariusza.

W długoterminowych zaleceniach dotyczących tworzenia kopii zapasowych dotychczas konsekwentnie proponowano strategię 3-2-1 – czyli trzy kopie danych na dwóch różnych nośnikach z jedną kopią przechowywaną poza siedzibą firmy. Ale to się zmienia. Rekomendowanym standardem jest teraz 3-2-1-1-0 i oto dlaczego ta strategia jest tak ważna.

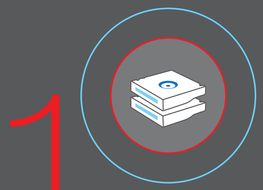
Gartner przewiduje, że do 2025 r. co najmniej **75%** organizacji IT stanie w obliczu co najmniej jednego ataku ransomware.

› *Źródło*

3 **Różne kopie Twoich danych**

2 **Różne typy nośników do przechowywania**

1 **Kopia przechowywana poza siedzibą firmy**



1 **Kopia przechowywana offline**

0 **Kopia zapasowa bez błędów**

DLACZEGO 3 KOPIE?

Trzy kopie Twoich danych obejmują materiały pierwotne oraz dwie kopie zapasowe. Oprócz kopii awaryjnej, z której można szybko odzyskać dane, powinny istnieć również prawdziwe kopie zapasowe oparte o zdywersyfikowaną politykę dostępności.

DLACZEGO RÓŻNE NOŚNIKI?

Trzy kopie powinny być przechowywane na co najmniej dwóch różnych rodzajach nośników pamięci. Przy tak wielu aplikacjach, danych i rozwiązaniach, ważne jest zróżnicowanie między chmurą a rozwiązaniami on-premises.

39% małych i średnich firm nie ma planu dotyczącego reagowania na cyberataki i naruszenia bezpieczeństwa danych

› *Źródło*

DLACZEGO POZA?

Sposób przechowywania kopii zapasowych w chmurze jest często powiązany ze strategią ochrony danych dostawcy usług w chmurze. Najlepiej upewnić się, że kopia tych danych jest oddzielona od sieci. Przygotowując się na klęskę żywiołową, musisz mieć pewność, że przynajmniej jedna kopia zapasowa pozostanie fizycznie poza główną siedzibą firmy i zostanie przeniesiona w inne miejsce na wypadek huraganu, tornada lub innej klęski żywiołowej.

DLACZEGO OFFLINE?

Gdy kopia zapasowa jest fizycznie odizolowana, oprogramowanie ransomware nie ma do niej dostępu. Twoja kopia zapasowa jest oddzielona od sieci, w której przechowywane są dane. Jeśli kopia podstawowa lub lokalna kopia zapasowa jest uszkodzona lub naruszona, kopia zapasowa offline może zostać użyta do przywrócenia danych. Często jest to kopia zapasowa na taśmie. Izolacja w oprogramowaniu odpowiedzialnym za przechowywanie danych jest stosowana od dawna, ale nic nie jest skuteczniejsze od fizycznego odseparowania nośnika.

DLACZEGO BEZ BŁĘDÓW?

Kopia 0 to bezbłędna kopia zapasowa, która jest stała i nie można jej w żaden sposób zmienić. Zazwyczaj jest przechowywana w trybie offline i może być użyta do odzyskania danych po ataku ransomware. Aby utrzymać brak błędów, monitorowanie danych powinno być wykonywane codziennie, a błędy naprawiane, gdy tylko zostaną zidentyfikowane.

Strategia tworzenia kopii zapasowych 3-2-1-1-0 zmniejsza wpływ pojedynczej awarii. W obliczu rosnącej liczby ataków ransomware planuj z wyprzedzeniem i upewnij się, że Twoja strategia ochrony danych zapewnia Ci bezpieczeństwo.

0801 800 802
IRONMOUNTAIN.PL