**Czytaj lub słuchaj artykuł online**

Zeskanuj kod QR, aby otworzyć artykuł na XO.PL

Źródło artykułu:

**https://xo.pl/it-na-wesolo-data-recovery**

DANE I ICH OCHRONA

# Odzyskiwanie danych, czyli archeolog szukający zaginionych dokumentów

Centralny Magazyn Dokumentów imienia Pana Kierownika przetrwał pożar. A właściwie — firma przetrwała dzięki **kopii zapasowej** spod skarpetek księgowej. **RAID** odbudowano, **backupy** poukładano, a kierownik uroczyście ogłosił koniec wszystkich problemów z danymi. Następnego ranka z jego gabinetu dobiegł krzyk, który przestraszył nawet drukarkę. Witamy w archeologii cyfrowej: odzyskiwaniu danych.

## Rozdział pierwszy: kierownik usunął coś bardzo ważnego

— PANIE FRANKU! ZNIKNĄŁ MI PLIK!
— Jaki plik?
— BARDZO WAŻNY!
— Jak się nazywał?
— „NOWY DOKUMENT (OSTATECZNY) (OSTATECZNY 2)”.
— Gdzie był zapisany?
— Na pulpicie.
— A co pan robił, zanim zniknął?
— PporządKI! USUNĄŁEM WSZYSTKO, CO WYGLĄDAŁO NA NIEPOTRZEBNE!
— Sprawdzimy kosz.
— WYNOSIŁEM ŚMIECI! KOSZ TEŻ OPRÓŻNIŁEM!

🤣🤣🤣

**Odzyskiwanie danych** to próba przywrócenia dostępu do informacji, które zostały skasowane, uszkodzone, utracone albo stały się niedostępne. Czasami wystarczy kliknąć „Przywróć” w koszu. Czasami potrzebujemy **backupu**. A czasami mamy do czynienia z uszkodzonym sprzętem, gdzie każda nieprzemyślana operacja może pogorszyć sytuację.

Ważna różnica: **odtworzenie z backupu** polega na sięgnięciu po wcześniej przygotowaną kopię. **Odzyskiwanie z nośnika** próbuje uratować to, co jeszcze pozostało na dysku lub innym urządzeniu. Pierwsze jest zwykle bardziej przewidywalne. Drugie nie daje gwarancji.

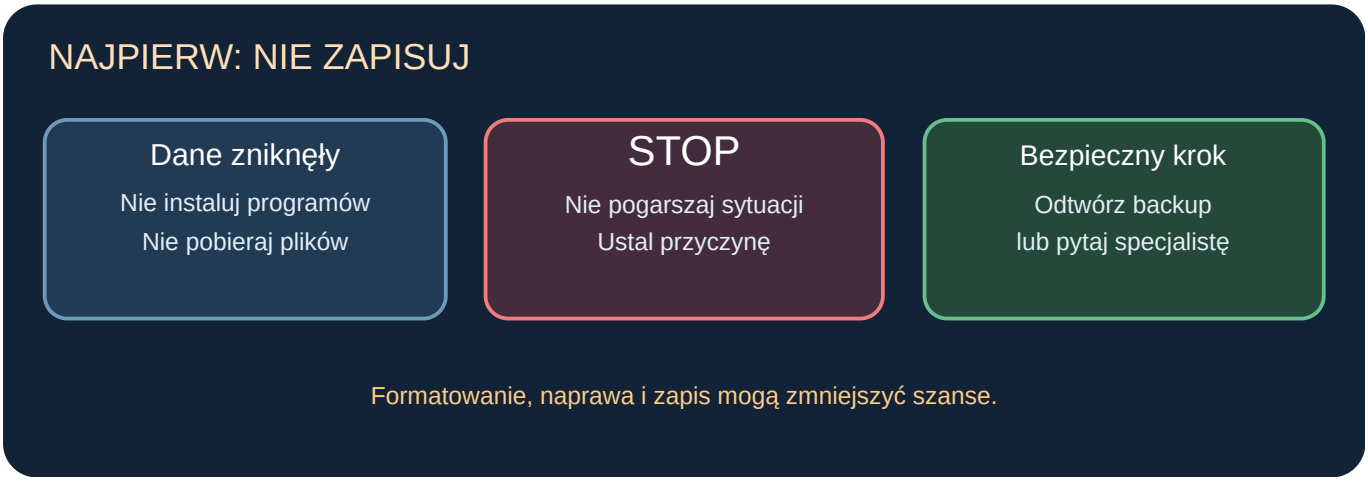
## Rozdział drugi: najdroższe trzy słowa — „już naprawiłem”

— Co pan zrobił po usunięciu pliku? — pyta Franek.
— ZAINSTALOWAŁEM PIĘĆ PROGRAMÓW DO ODZYSKIWANIA!
— Na którym dysku?
— NA TYM, Z KTÓREGO ZNIKNĄŁ PLIK!
— A potem?
— POBRAŁEM FILM INSTRUKTAŻOWY!
— Też na ten dysk?
— A GDZIE MIAŁEM GO POBRAĆ?!
— ...
— PANIE FRANKU, NIECH PAN NIE PATRZY NA MNIE JAK NA AWARIĘ SPRZĘTOWĄ!

🤣🤣

Przy podejrzeniu przypadkowego usunięcia danych najważniejsze jest **ograniczenie dalszego zapisu** na urządzeniu. Nie instalujemy odruchowo nowych programów, nie pobieramy plików na ten sam dysk, nie formatujemy go i nie uruchamiamy napraw tylko dlatego, że komputer je proponuje. Nowy zapis może nadpisać dane, których właśnie szukamy.

Jeśli dysk wykazuje objawy fizycznej awarii — stuka, znika z systemu, zwalnia w nietypowy sposób albo zgłasza narastające błędy — **przerywamy jego używanie**. Powtarzane uruchamianie i skanowanie uszkodzonego mechanicznie dysku może zmniejszyć szanse na odzyskanie danych. Przy naprawdę ważnych danych lepiej zasięgnąć opinii specjalistycznego laboratorium niż eksperymentować.




**Wyjątek od odruchu „wyłącz wszystko”:** sytuacje takie jak aktywne **szyfrowanie** ransomware, zaszyfrowane woluminy czy systemy firmowe mogą wymagać odrębnej procedury reagowania. Nie ma jednej komendy dobrej na każde zdarzenie. Jeśli nie wiesz, co się dzieje, nie wykonuj kolejnych operacji „na próbę” — najpierw ustal, czy problem dotyczy usunięcia, awarii sprzętu, uszkodzenia systemu plików czy incydentu bezpieczeństwa.

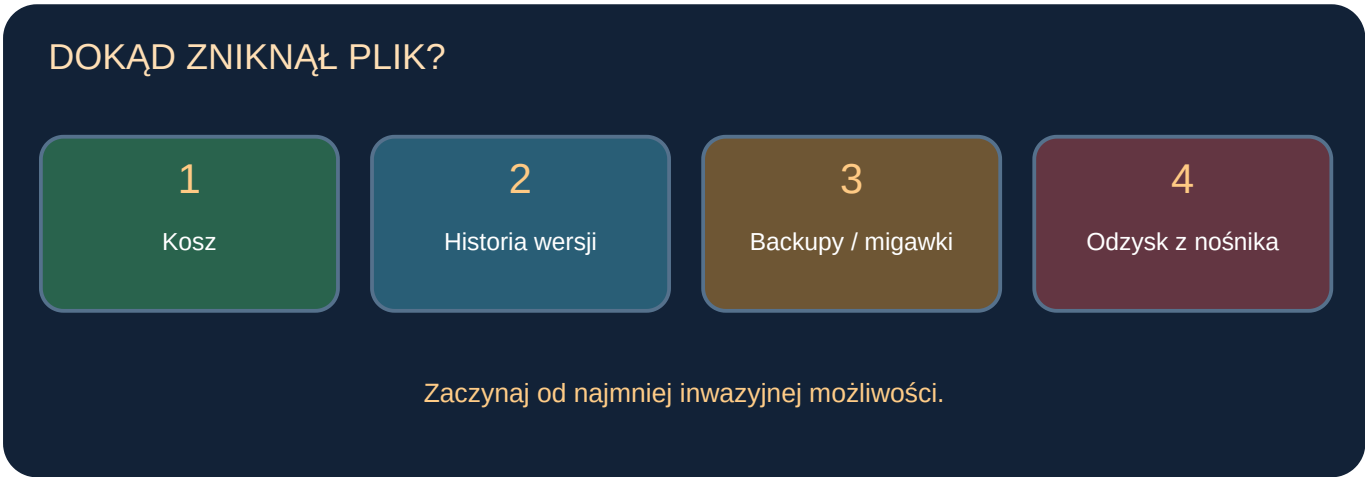
## Rozdział trzeci: najpierw szuflady, potem wykopaliska

— PANIE KIEROWNIKU, SPRAWDZIŁ PAN KOSZ?
— OPRÓŻNIONY!
— Historię wersji dokumentu?
— JAKĄ HISTORIĘ?! PRZECIEŻ TO NIE LEKCJA HISTORII!

— Kosz w usłudze chmurowej?
— TAM TEŻ JEST KOSZ?!
— **Backup** z wczoraj?
— ...
— Panie kierowniku?
— PROSZĘ MI POWIEDZIEĆ, ŻE NIE MUSZĘ ZNOWU PROSIĆ KSIĘGOWEJ O SKARPETKI!

🤣🤣

Najpierw sprawdzamy **najmniej inwazyjne możliwości**: kosz systemowy i kosz aplikacji, historię wersji dokumentu, mechanizmy przywracania w chmurze, automatyczne zapisy programów, **kopie zapasowe** i dostępne migawki. Pamiętaj, że czas przechowywania wersji oraz skasowanych plików zależy od usługi i jej konfiguracji.




To ważne także dlatego, że próby odzysku bezpośrednio z nośnika są bardziej ryzykowne i czasochłonne. Jeżeli dokument bezpiecznie czeka w historii wersji sprzed godziny, nie ma powodu urządzać archeologicznych wykopalisk na SSD.

## Rozdział czwarty: usunięty plik nie zawsze znika od razu

— PANIE FRANKU, SKORO USUNĄŁEM PLIK, TO GDZIE ON JEST?!
— Zależy od systemu plików i rodzaju dysku.
— JA PYTAM O PLIK, NIE O FILOZOFIĘ!
— W wielu sytuacjach po usunięciu znika przede wszystkim informacja, jak do niego dotrzeć. Część danych może jeszcze pozostać w komórkach lub sektorach.
— TO PROSZĘ JE ZAWOŁAĆ!
— Problem w tym, że inne dane mogą zająć ich miejsce.
— TO NIECH PAN POSTAWI TABLICZKĘ „ZAJĘTE”!

🤣🤣

W uproszczeniu: usunięcie pliku często oznacza zmianę informacji organizujących dane, a nie natychmiastowe wymazanie każdej zapisanej cząstki. Ale **nie daje to gwarancji odzyskania**. Na wynik wpływają m.in. system plików, stan urządzenia, późniejsze zapisy, **szyfrowanie**, migawki i mechanizmy obsługi wolnej przestrzeni.

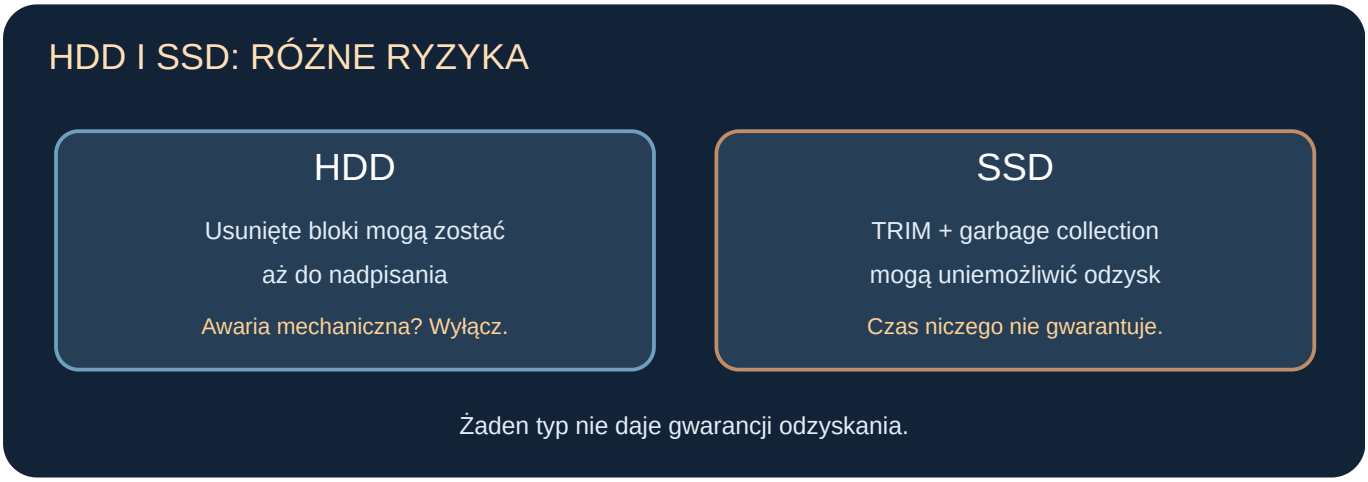
Przy odzyskiwaniu mogą przetrwać fragmenty pliku bez jego oryginalnej nazwy, ścieżki czy struktury katalogów. Program może znaleźć zdjęcie, ale nie wiedzieć już, że leżało w katalogu „Wakacje 2014”. Dlatego cudowna lista „100% odzyskanych plików” niewiele znaczy, dopóki nie sprawdzimy, czy pliki są kompletne i otwierają się prawidłowo.

## Rozdział piąty: HDD kontra SSD — wielka niespodzianka kierownika

— KUPIŁEM NOWOCZESNE SSD! TERAZ DANE BĘDZIE ŁATWIEJ ODZYSKAĆ!
— Niekoniecznie.
— JAK TO NIEKONIECZNIE?!
— Dyski SSD często obsługują TRIM i wewnętrzne porządkowanie pamięci.
— CO ROBI TRIM?!
— Informuje urządzenie, że określone bloki nie są już potrzebne. W połączeniu z działaniem kontrolera może to uniemożliwić późniejszy odzysk.
— TO JA WYDAŁEM WIĘCEJ PIENIĘDZY, ŻEBY PLIK ZNIKNĄŁ DOKŁADNIEJ?!

🤣🤣

Na tradycyjnym **HDD** dane po usunięciu mogą przez pewien czas pozostawać w sektorach, dopóki coś ich nie nadpisze. Nie ma jednak gwarancji ani bezpiecznego „okna czasowego”. Na **SSD** polecenia **TRIM**, wewnętrzna obsługa pamięci i garbage collection mogą sprawić, że odzyskanie usuniętych danych będzie znacznie trudniejsze, a czasami niemożliwe. Zależy to również od systemu, kontrolera i konfiguracji.




SSD to świetny nośnik do normalnej pracy. Właśnie dlatego jednak **backup jest ważniejszy niż wiara w późniejsze odzyskanie skasowanych plików**. Podobnie jest z **szyfrowaniem**: przy utracie niezbędnych kluczy dane mogą być matematycznie nieosiągalne mimo fizycznego istnienia pamięci.

## Rozdział szósty: dysk stuka, a kierownik go przekonuje

Z serwerowni dochodzi regularne „klik, klik, klik”.

— PANIE FRANKU! DYSK MI STUKA!
— Proszę go wyłączyć i nie uruchamiać ponownie.
— ALE MOŻE JAK GO JESZCZE TRZY RAZY WŁĄCZĘ, TO SIĘ ROZMYŚLI?!
— To nie negocjacje, panie kierowniku.
— A JAK GO LEKKO POSTUKAM Z DRUGIEJ STRONY?!

— Tym bardziej nie.
— TO MOŻE WŁOŻYĆ GO DO ZAMRAŻARKI?!
— Nie. Żadnych domowych eksperymentów.

🤣🤣

Przy podejrzeniu **uszkodzenia mechanicznego HDD** ryzykowne są kolejne uruchomienia, długie skany i improwizowane metody w rodzaju zamrażania, potrząsania lub otwierania obudowy. Uszkodzenia głowic, powierzchni talerzy lub elektroniki nie naprawia się zaklęciem z forum internetowego. W profesjonalnych laboratoriach stosuje się specjalistyczny sprzęt oraz kontrolowane warunki, ale nawet tam odzysk nie jest zawsze możliwy.

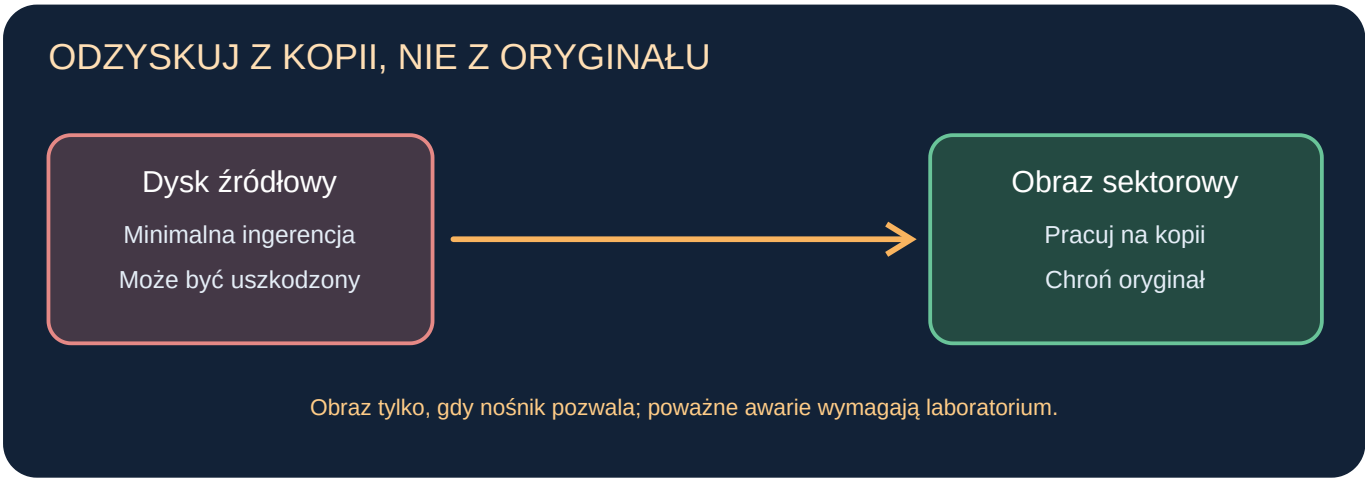
Inaczej wygląda sytuacja, gdy problem dotyczy tylko błędnej partycji lub systemu plików na sprawnym urządzeniu. Najpierw trzeba jednak **rozpoznać, z którą sytuacją mamy do czynienia**.

## Rozdział siódmy: najpierw obraz, potem eksperymenty

— PANIE FRANKU, ZNALAZŁEM PROGRAM NAPRAWIAJĄCY WSZYSTKO!
— Nie uruchamiajmy go na jedynym egzemplarzu danych.
— TO NA CZYM?!
— Jeżeli stan nośnika pozwala, najpierw wykonujemy możliwie wierną kopię sektorową albo obraz urządzenia na innym, sprawnym nośniku.
— A PO CO?!
— Żeby prowadzić dalszą analizę na kopii i chronić oryginał.
— CZYLI ROBIMY **BACKUP** DYSKU, KTÓRY JUŻ SIĘ PSUJE?!
— W określonych sytuacjach — tak, ale ostrożnie i nie zawsze samodzielnie.
— PANOWIE, JA CHYBA ZACZYNAM ROZUMIEĆ, DLACZEGO WY MACIE TYLE DYSKÓW!

🤣🤣

W odzyskiwaniu danych często stosuje się **obraz sektorowy** — kopię zawartości nośnika, wykorzystywaną do dalszej analizy bez ingerencji w oryginał. Nie należy mylić jej ze zwykłym kopiowaniem widocznych plików. Praca na obrazie pozwala ograniczać ryzyko, że nieudana próba naprawy zniszczy jedyną dostępną wersję danych.



Jednak **nie każdy uszkodzony dysk należy samodzielnie obrazować**. Jeśli urządzenie ma poważne problemy fizyczne, nawet odczyt może je dobijać. Wtedy decyzję o dalszych krokach powinien podejmować specjalista. A jeśli nośnik jest stabilny, trzeba szczególnie uważać, by nie pomylić dysku źródłowego z docelowym — zapisanie obrazu w złym kierunku może nieodwracalnie zniszczyć dane.

## Rozdział ósmy: „napraw dysk” to nie zawsze dobra rada

— KOMPUTER MÓWI, ŻEBY NAPRAWIĆ SYSTEM PLIKÓW!
— Zanim to zrobimy, zabezpieczmy dane i sprawdźmy przyczynę.
— ALE PRZECIEŻ JEST PRZYCISK „NAPRAW”!
— Niektóre narzędzia poprawiają spójność struktury kosztem odrzucenia uszkodzonych wpisów.
— CZYLI NAPRAWIĄ DYSK, A PLIK ZOSTAWIĄ W LESIE?!
— To możliwy scenariusz.
— PANOWIE! PROSZĘ NATYCHMIAST USUNĄĆ PRZYCISK „NAPRAW”!

🤣🤣

Narzędzia takie jak **CHKDSK**, **fsck** czy podobne mechanizmy mają za zadanie przywrócić spójność systemu plików. To nie jest to samo co maksymalizowanie szans na odzyskanie każdej utraconej informacji. Operacje naprawcze mogą modyfikować metadane, odłączać uszkodzone fragmenty katalogów albo usuwać niepoprawne odniesienia.

Gdy zależy nam na odzyskaniu danych, bezpieczniejszy porządek to zazwyczaj: **zatrzymać niepotrzebny zapis, ustalić typ uszkodzenia, zabezpieczyć oryginał lub jego obraz, a dopiero później rozważać naprawę**. Nie uruchamiamy destrukcyjnych operacji w ciemno.

## Rozdział dziewiąty: RAID wraca jak zły sen

— PANIE FRANKU! ALE MY PRZECIEŻ MAMY **RAID**!
— Tak, panie kierowniku.
— TO NIECH ON ODZYSKA PLIK!
— **RAID** może pomóc przetrwać określone awarie dysków. Nie cofa automatycznie logicznego usunięcia danych.
— TO PO CO JA MAM **RAID**?!
— Żeby przy części awarii sprzętowych usługa nadal działała.
— A COFA USUNIĘCIE PLIKU NA WSZYSTKICH DYSKACH?!
— Nie, zmiana zwykle trafia do całej macierzy.
— CZY MY JUŻ O TYM NIE ROZMAWIALIŚMY PRZED POŻAREM?!
— Rozmawialiśmy.

🤣🤣

**RAID to nie backup.** To ważne również podczas odzyskiwania. Awaria jednego dysku w odpowiedniej konfiguracji **RAID** może być obsłużona przez mechanizm nadmiarowości. Ale przypadkowe usunięcie, zaszyfrowanie plików, nadpisanie bazy czy błąd aplikacji nie zostają magicznie cofnięte.

Co więcej, odzyskiwanie uszkodzonej macierzy **RAID** bywa trudniejsze niż odzyskiwanie jednego dysku, bo znaczenie mają kolejność nośników, metadane, układ pasków, poziom **RAID** i stan każdego elementu. Nie inicjalizujemy ponownie macierzy ani nie wykonujemy pochopnych przebudów, jeśli zależy nam na utraconych danych.

## Rozdział dziesiąty: backup kontra odzysk — dwie drużyny ratunkowe

Księgowa podnosi rękę.

— A może po prostu odtworzyć dokument z wczorajszego **backupu**?
— ALE JA CHCĘ DZISIEJSZĄ WERSJĘ! — protestuje kierownik.
— Wersja z wczoraj jest sprawdzona. Dzisiejszą możemy spróbować znaleźć w historii edycji.
— A JEŚLI NIE MA?!
— Wtedy oceniamy, ile pracy rzeczywiście utracono i czy odzysk z nośnika ma sens.
— CZYLI **BACKUP** TO PLAN A, A ARCHEOLOG TO PLAN B?!
— Zwykle dokładnie tak.

🤣🤣

Jeżeli istnieje **sprawdzony backup**, jest często najprostszą i bezpieczniejszą drogą. Trzeba tylko zwrócić uwagę na datę kopii i nie nadpisać przypadkowo innych, nowszych danych podczas przywracania. Warto czasem odtworzyć pliki do osobnego folderu, porównać wersje i dopiero potem zdecydować, którą zachować.

Inaczej postępujemy z **bazami danych** i aplikacjami: pojedynczy plik wyciągnięty z działającego systemu nie zawsze jest spójny. Mogą być potrzebne transakcyjne **backupy**, dzienniki zmian, właściwa kolejność odzyskiwania i sprawdzenie zgodności danych. To jeden z powodów, dla których plan odtwarzania warto opracować **zanim** cokolwiek zniknie.

## Rozdział jedenasty: chmura też ma pamięć — ale nie wieczną

— PANIE FRANKU! W CHMURZE MÓJ PLIK TEŻ ZNIKNĄŁ!
— Synchronizacja mogła przenieść usunięcie.
— CZYLI CHMURA MNIE ZDRADZIŁA?!
— Sprawdźmy historię wersji, kosz usługi i archiwalne punkty odtworzenia.
— A JAK TAM NIE MA?!
— Wtedy wracamy do innych kopii.
— ...
— PROSZĘ ZADZWONIĆ DO KSIĘGOWEJ. NIECH JESZCZE NIE WYRZUCA SKARPETEK!

🤣🤣

Usługi chmurowe mogą oferować **historię wersji, kosze, okresy retencji i mechanizmy przywracania**. Ich zakres bywa różny i zależy od planu, konfiguracji oraz wieku zdarzenia. Synchronizacja nie jest tym samym co niezależny **backup**. Nawet jeśli usługa pozwala odzyskać skasowany plik, warto mieć kopię, której automatyczne usuwanie albo przejęte poświadczenia nie dosięgną.

Gdy problem wynika z kradzieży konta lub ransomware, najpierw należy zadbać o **bezpieczeństwo** dostępu i powstrzymanie dalszych zmian. Odtworzenie plików bez opanowania incydentu może oznaczać, że za chwilę znikną ponownie.

## Rozdział dwunasty: kiedy laboratorium, a kiedy samodzielna próba?

— PANIE KIEROWNIKU, ILE SĄ WARTE TE DANE?
— BEZCENNE!
— A ile mamy niezależnych kopii?
— ZERO!

— Czy dysk działa prawidłowo?
— STUKA JAK STARY TRAKTOR!
— W takim razie nie eksperymentujmy.
— ALE NA FORUM NAPISALI, ŻEBY GO WŁOŻYĆ DO ZAMRAŻARKI!
— A na drugim forum napisali, żeby go nie słuchać.
— TO KTÓRE FORUM MA RACJĘ?!
— W tym przypadku: żadne zamiast diagnozy.

🤣🤣

Samodzielna próba może mieć sens przy **mało istotnych danych, stabilnym nośniku i jasnym, logicznym problemie**, najlepiej po wykonaniu bezpiecznego obrazu i z pełną świadomością ryzyka. Przy fizycznych objawach awarii, nośnikach po zalaniu lub pożarze, poważnych uszkodzeniach elektroniki albo danych o wyjątkowej wartości lepiej zasięgnąć pomocy profesjonalnego laboratorium.

Żadne uczciwe laboratorium nie powinno obiecywać absolutnej skuteczności. Warto zapytać o diagnostykę, sposób pracy z nośnikiem, politykę kosztów, poufność danych oraz sposób przekazania odzyskanych plików. Jeśli dane są objęte szczególnymi wymaganiami bezpieczeństwa, ich powierzenie osobie trzeciej również wymaga rozwagi.

## Rozdział trzynasty: kierownik robi listę rzeczy, których nie wolno robić

Na ścianie nowego magazynu wisi tablica. Kierownik pisze wielkimi literami:

— „NIE NADPISYWAĆ!”
— Dobrze, panie kierowniku.
— „NIE FORMATOWAĆ W PANICE!”
— Bardzo dobrze.
— „NIE URUCHAMIAĆ NAPRAW W CIEMNO!”
— Doskonale.
— „SPRAWDZIĆ KOSZ, WERSJE I **BACKUP**!”
— Świetnie.
— „NIE WKŁADAĆ DYSKÓW DO ZAMRAŻARKI!”
— Obowiązkowo.
— „ZADZWONIĆ DO FRANKA, ZANIM ZROBIĘ COKOLWIEK!”
— To najlepszy punkt — mówi Franek.
— „I NIE DOTYKAĆ SKARPETEK KSIĘGOWEJ!”
— To już chyba osobna polityka bezpieczeństwa.

🤣🤣🤣

**Najważniejsze zasady:** zatrzymaj działania mogące zmienić utracone dane; zacznij od kosza, historii wersji i sprawdzonego **backupu**; rozpoznaj, czy nośnik jest sprawny; nie eksperymentuj na jedynym oryginale; przy poważnej awarii powierz decyzję fachowcom; a po odzyskaniu sprawdź, czy dane rzeczywiście działają.

Odzyskiwanie nie jest magią. Czasem można uratować wszystko, czasem część, a czasem nic. **Najlepszy moment na przygotowanie planu odzyskiwania jest przed utratą danych.**

## Finał: archeolog, który nie musiał kopać

— PANIE FRANKU! ZNALAZŁ PAN MÓJ DOKUMENT?!
— Tak. W automatycznie zapisanej historii edycji.
— BEZ ROZKRĘCANIA DYSKU?!
— Bez.
— BEZ LABORATORIUM?!
— Bez.
— BEZ ZAMRAŻARKI?!
— Tym bardziej bez.
— TO PO CO JA PRZECZYTAŁEM TE WSZYSTKIE PORADNIKI?!
— Żeby następnym razem najpierw sprawdzić historię wersji.

Do gabinetu zagląda księgowa.

— A **backup** wczoraj też się zrobił.
— DOSKONALE! TO MOŻEMY ZNOWU PRZESTAĆ SIĘ MARTWIĆ!
— Możemy przestać panikować. Nie możemy przestać sprawdzać kopii.
— PANOWIE! CZY WY MOŻECIE CHOCIAŻ JEDEN DZIEŃ NIE MÓWIĆ MI O **BACKUPACH**?!

🤣🤣🤣🤣

**Zapamiętaj:** po utracie danych pierwszym zadaniem nie jest „coś natychmiast naprawić”, tylko **nie odebrać sobie ostatniej szansy na odzyskanie**. A jeżeli masz sprawdzony **backup**, cała ta archeologia bardzo często okazuje się niepotrzebna.

*Centralny Magazyn Dokumentów ogłasza sukces. Kierownik odzyskał dokument. Franek odzyskał spokój. Księgowa odzyskała skarpetki — i to bez użycia specjalistycznego oprogramowania.*