Czytaj lub słuchaj artykuł online

Zeskanuj kod QR, aby otworzyć artykuł na XO.PL

Źródło artykułu:

https://xo.pl/it-na-wesolo-data-backup

DANE I ICH OCHRONA

Backup, czyli dlaczego jedna kopia to czasami żadna kopia

Centralny Magazyn Dokumentów imienia Pana Kierownika spłonął. Razem z nim dwa sejfy i cały cudowny **RAID**. Kierownik właśnie odkrywa, że odporność na awarię dysku nie jest odpornością na pożar, przypadkowe usunięcie ani ransomware. Na szczęście księgowa ma stary dysk w szufladzie. Rozpoczyna się Operacja „Ocalić Cokolwiek” — czyli opowieść o backupach, które nie muszą być piękne, ale muszą dać się odtworzyć.

Rozdział pierwszy: skarpetki ratują firmę

Kierownik stoi przed zgliszczami.

— PANOWIE! NIE MAMY MAGAZYNU!
— Wiemy, panie kierowniku.
— NIE MAMY SERWERÓW!
— Wiemy.
— NIE MAMY **RAID-U**!
— Też wiemy.
— TO CO MY W OGÓLE MAMY?!

Zza pleców odzywa się księgowa.

— Ja mam dysk.
— JAKI DYSK?!
— Z dokumentami firmy. W domu, w szufladzie pod skarpetkami.
— PANI TRZYMA DOKUMENTY FIRMY POD SKARPETKAMI?!
— Tak. A pan trzymał oba sejfy w jednym płonącym budynku.
— ...
— ...
— PROSZĘ NATYCHMIAST PRZYNIEŚĆ TE SKARPETKI!

🤣🤣🤣

Tak właśnie zaczyna się historia o **backupie**, czyli zapasowej kopii danych, z której możemy odzyskać coś utraconego. Najlepsza kopia nie musi być najdroższa. Musi być **poprawna, odpowiednio chroniona i możliwa do odtworzenia**. Przypadkowy dysk sprzed dwóch lat może ocalić ważne zdjęcia, chociaż nie zastąpi dobrze zaplanowanego, aktualnego systemu kopii.

Nasze hasło na dziś brzmi: **„Nie ma głupiego backupu. Głupi jest brak backupu!”** To zachęta, by zacząć od czegoś realnego, a nie obietnica, że każda przypadkowa kopia zapewnia wystarczającą ochronę.

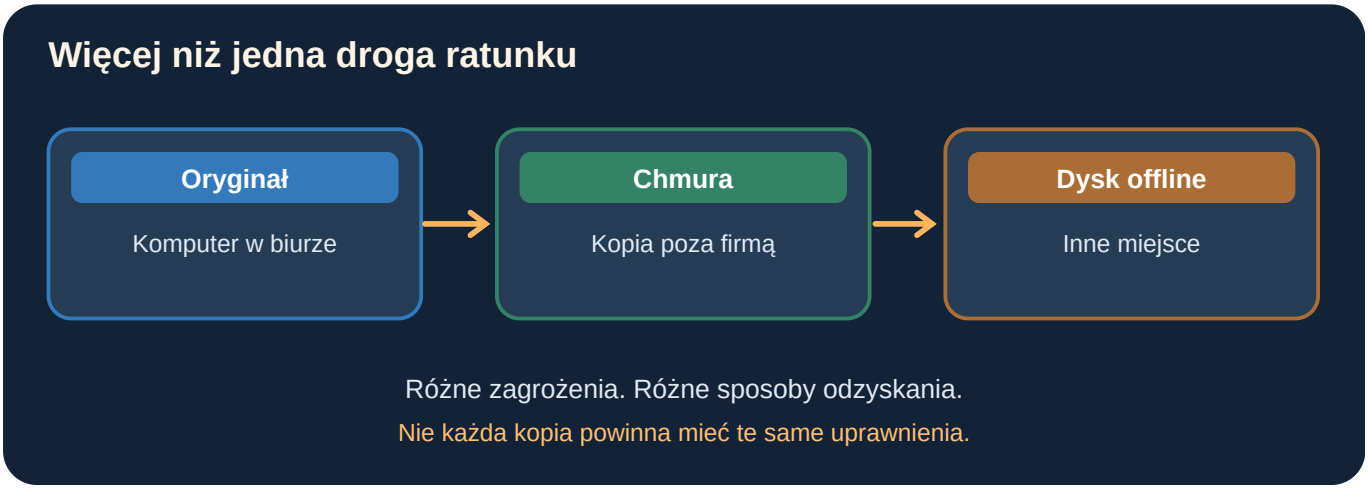
Rozdział drugi: jeden magazyn, wiele dróg ratunku

Kierownik zwołuje naradę.

— OD DZISIAJ BACKUP MA BYĆ WSZĘDZIE!
— W biurze, w drugim budynku i w chmurze?
— TAK! I U KSIĘGOWEJ!
— A W LODÓWCE? — pyta Franek.
— JEŚLI SIĘ ZMIEŚCI, TO TEŻ!
— Panie kierowniku, lodówka nie jest zalecanym magazynem dysków.
— TO PROSZĘ KUPIĆ LODÓWKĘ INFORMATYCZNĄ!

🤣🤣

Pomysł jest prosty: **nie trzymaj wszystkich dróg ratunku w zasięgu jednej katastrofy**. Awaria dysku, błąd człowieka, kradzież sprzętu, pożar, zalanie, awaria dostawcy czy przejęcie konta to różne zagrożenia. Kopia w innym miejscu pomaga przy części z nich, ale sama lokalizacja nie zawsze chroni przed usunięciem przez sieć.



Backup na dodatkowym dysku podłączonym na stałe do tego samego komputera jest lepszy niż żaden, ale nie chroni przed wszystkim. Kopia na innym urządzeniu, w chmurze, poza budynkiem albo na odłączonym dysku może ograniczyć inne rodzaje ryzyka. Nie chodzi o kupowanie najdroższej technologii — chodzi o niezależność zagrożeń i o sprawdzenie, czy da się dane odzyskać.

Rozdział trzeci: dwa dyski jadą na zmianę

Franek przychodzi z dwoma dyskami zewnętrznymi.

— Jeden będzie robił kopię w biurze, drugi pozostanie w innej lokalizacji. Potem zamienimy je rolami.
— CZYLI DYSKI BĘDĄ JEŹDZIĆ NA WYCIECZKI?!
— Tak, ale nie oba naraz.
— A JAK JEDEN SIĘ ZGUBI?!
— Dlatego mamy drugi i sprawdzamy, czy zawiera poprawną kopię.
— TO PROSZĘ IM KUPOWAĆ BILETY W OBIE STRONY!

🤣

To może być zupełnie rozsądna strategia: **rotowane dyski zewnętrzne**. Robimy kopię na jednym, bezpiecznie go odłączamy, wynosimy do innej lokalizacji, a następnie używamy drugiego. Rotację należy organizować tak, aby nie zabrać ostatniej sprawdzonej kopii z bezpiecznego miejsca, zanim nowa rzeczywiście powstanie.



Dysk w domu, biurze, innym mieszkaniu czy zabezpieczonej szafie może być przydatny. Nie potrzeba Fort Knox. Potrzeba zdrowego rozsądku: **sucho, bez nadmiernego ciepła i wilgoci, bez wstrząsów, bez przypadkowego dostępu obcych**. W transporcie przyda się etui, a na postoju — niewystawianie nośnika na widok.

— PANIE KIEROWNIKU! BACKUP JEST JUŻ POZA BIUREM!
— GDZIE?!
— NA TYLNEJ PÓŁCE SAMOCHODU!
— A CO TO ZA KARTKA NA SZYBIE?!
— „DYSK Z BACKUPEM FIRMY. PROSZĘ NIE KRAŚĆ”.
— PANIE FRANKU! PAN WŁAŚNIE ZROBIŁ REKLAMĘ DLA ZŁODZIEI!

🤣🤣

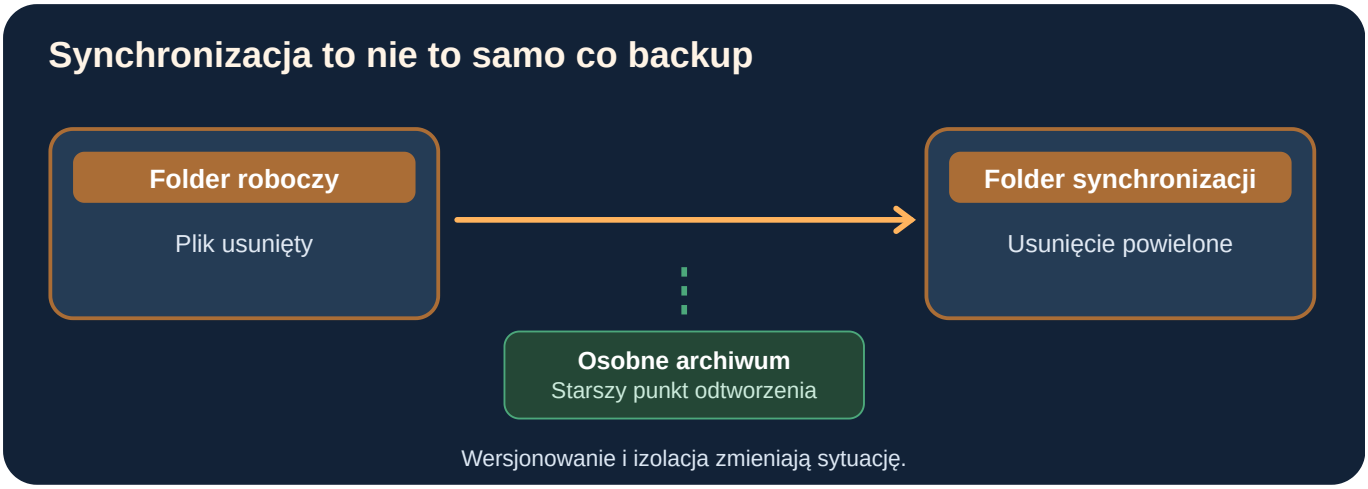
Nie zostawiamy dysków w nagrzanym samochodzie ani w miejscach, w których łatwo je ukraść. Nośnik wynoszony z firmy powinien być odpowiednio zabezpieczony; jeśli zawiera dane poufne, zwykle warto go zaszyfrować.

Rozdział czwarty: chmura nie gryzie. Ale potrafi synchronizować katastrofy

— PANIE KIEROWNIKU! WSZYSTKIE DOKUMENTY SĄ W DROPBOXIE!
— DOSKONALE! MAMY BACKUP!
— To zależy.
— JAK TO ZALEŻY?!
— Jeśli folder jest tylko synchronizowany, usunięcie pliku może dotrzeć do pozostałych urządzeń.
— TO CO TO ZA BACKUP?!
— To przede wszystkim synchronizacja.
— TO PROSZĘ GO ZSYNCHRONIZOWAĆ TAK, ŻEBY NIC NIE ZNIKAŁO!

🤣🤣

Dropbox, OneDrive, Google Drive i podobne usługi mogą być częścią sensownego systemu backupów. Warunek: trzeba rozumieć, jak działają wersjonowanie, **odzyskiwanie** usuniętych plików, retencja, uprawnienia i kopiowanie do niezależnych archiwów. Sam folder synchronizowany jeden do jednego nie gwarantuje ochrony przed przypadkowym usunięciem ani ransomware.



Można na przykład przygotowywać osobne archiwa z datą, przechowywać wiele punktów odtworzenia i chronić je przed automatycznym nadpisywaniem. Warto sprawdzić rzeczywiste ograniczenia wybranej usługi i przetestować odzyskanie plików. Nie ma obowiązku korzystania wyłącznie z „profesjonalnego" systemu backupowego, jeśli prostsza usługa została świadomie i odpowiednio skonfigurowana.

Rozdział piąty: archiwum, którego automat nie może skasować

Do magazynu wchodzi informatyk.

— Panie kierowniku, automatyczne kopie są przydatne, ale trzeba też chronić starsze archiwa.
— PRZED CZYM?!
— Choćby przed przejęciem konta automatu.
— TO NIECH AUTOMAT BĘDZIE GRZECZNY!
— Lepiej, żeby nie miał uprawnień do kasowania historycznych kopii.
— JAK TO?! MÓJ AUTOMAT NIE MOŻE WSZYSTKIEGO?!
— Właśnie o to chodzi.

🤣🤣

Jednym z ciekawych rozwiązań jest **oddzielanie bieżącego backupu od archiwum historycznego**. Okresowo można przenosić lub kopiować sprawdzone punkty odtworzenia do obszaru, którym zarządza niezależny mechanizm, a produkcyjny automat nie ma prawa ich zmieniać ani usuwać.



Liczą się rzeczywiste ograniczenia uprawnień i niezależność dostępu, a nie nazwa folderu „TAJNE — NIE DOTYKAĆ”. Podobną rolę mogą pełnić kopie **offline** (fizycznie odłączone), **offsite** (w innej lokalizacji) i **immutable/WORM** (chronione przed zmianą w określonym czasie). To różne cechy: kopia offsite może być dostępna online, a kopia immutable niekoniecznie znajduje się poza budynkiem.

— PANIE FRANKU, DLACZEGO AUTOMAT NIE WIDZI ARCHIWUM?!
— Bo jeśli ktoś go przejmie, też nie powinien móc go usunąć.
— TO JA PŁACĘ ZA AUTOMAT, KTÓRY NIE WIE, GDZIE SĄ NASZE DANE?!
— Właśnie dlatego nadal możemy je mieć.

Przy wielu warstwach kopii trzeba uważać, żeby uszkodzenie lub niepożądane zmiany nie zostały bezrefleksyjnie przeniesione do wszystkich kolejnych miejsc. Dlatego zachowujemy historyczne wersje, kontrolujemy retencję i co jakiś czas sprawdzamy integralność oraz odtwarzanie.

Rozdział szósty: pełny, przyrostowy, różnicowy i migawka

Kierownik domaga się definicji.

— CHCĘ PEŁNY BACKUP!
— To kopiujemy cały wybrany zestaw danych.
— A JAK ZMIENI SIĘ JEDNA FAKTURA?!
— Możemy użyć kopii przyrostowej, zapisującej zmiany od poprzedniego backupu w danym łańcuchu.
— A RÓŻNICOWA?!
— Zwykle zapisuje zmiany od ostatniej kopii pełnej.
— A MIGAWKA?!
— Utrwala widok danych z określonego momentu, zależnie od systemu.
— PANOWIE, JA CHCIAŁEM KOPIĘ FAKTURY, A DOSTAŁEM CZTERY WYRAZY!

🤣

Pełny backup obejmuje cały zaplanowany zestaw. **Przyrostowy** zazwyczaj zapisuje to, co zmieniło się od poprzedniej kopii w jego łańcuchu; oszczędza miejsce, ale przy odzyskiwaniu może wymagać kilku ogniw. **Różnicowy** zwykle obejmuje zmiany od ostatniej kopii pełnej, dlatego może rosnąć z czasem. **Snapshot** jest migawką stanu, która często wykorzystuje mechanizmy systemu plików lub magazynu blokowego. Migawka w tym samym urządzeniu nie zastępuje automatycznie niezależnej kopii poza nim.

Retencja to reguły określające, jak długo zachowujemy kolejne wersje i punkty odtworzenia. Mogą zależeć od czasu, znaczenia danych i dostępnej pojemności. „Trzymamy jak najdłużej, dopóki wystarczy miejsca” bywa użytecznym podejściem, ale wymaga świadomego zwalniania przestrzeni, żeby nie stracić ostatniej dobrej kopii.

Rozdział siódmy: ransomware odwiedza magazyn

Drzwi otwierają się z hukiem.

— DZIEŃ DOBRY! PRZYSZEDŁEM ZASZYFROWAĆ PAŃSTWU DOKUMENTY!
— OCHRONAAAA! — wrzeszczy kierownik.
— Serwer już zaszyfrowany.
— TO MAMY NAS-A!
— Był dostępny z tego samego konta.
— TO MAMY DRUGI SERWER!
— To samo hasło administratora.
— ...
— Jego też.
— A dysk, który od dwóch tygodni leży odłączony w innym miejscu? — pyta księgowa.
— JAKI DYSK?! — pyta napastnik.
— Ten pod skarpetkami.
— PANI KSIĘGOWO... CZY MOGĘ PANIĄ UŚCISKAĆ?!

🤣🤣🤣

Przejęcie serwera lub konta może zagrozić każdej kopii, do której napastnik uzyska dostęp. Dlatego niezależne konta, minimalne uprawnienia, izolacja, wersjonowanie, kopie offline lub niezmienialne archiwa są tak cenne. **Nieprzewidywalna nazwa folderu nie zastąpi faktycznej izolacji.** Nietypowość może pomagać, ale tylko razem z rzeczywistymi barierami.

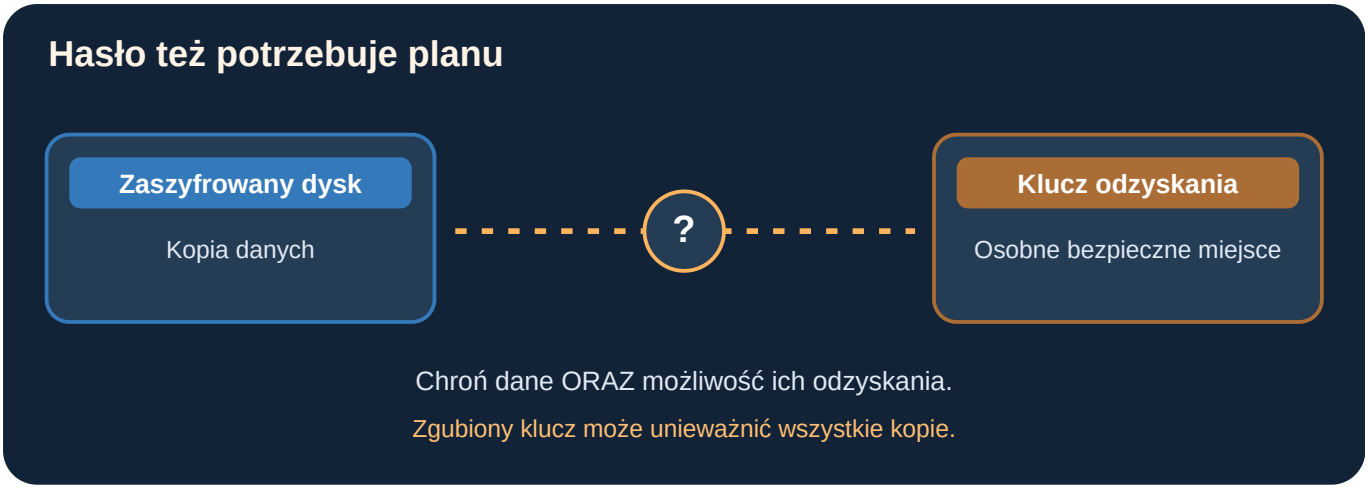
Rozdział ósmy: zaszyfrowany dysk i karteczka z hasłem

— PANIE KIEROWNIKU! ZASZYFROWAŁEM BACKUP!
— DOSKONALE! A HASŁO?!
— Na karteczce.
— GDZIE?!
— Przyklejona do dysku.
— TO PO JAKĄ CHOLERĘ SZYFROWALIŚMY TEN DYSK?!

🤣🤣

Szyfrowanie chroni poufność danych, zwłaszcza gdy nośnik zostanie zgubiony lub skradziony. Przy dokumentach firmowych, danych osobowych i innych wrażliwych zbiorach zwykle jest bardzo ważne. Przy nieistotnych, niewrażliwych plikach także niezaszyfrowana kopia może być lepsza niż żadna — jeśli nie narusza to wymagań poufności czy obowiązujących zasad.

Nie trzeba jednak chować każdej kopii w bunkrze. Warto stosować sprawdzone mechanizmy **szyfrowania**, silne hasła lub klucze i proporcjonalne zabezpieczenia. **Szyfrowanie nie chroni samo w sobie przed usunięciem danych** i nie pomoże w odzyskaniu zawartości, gdy zgubimy jedyny klucz.



— OD DZISIAJ ŻADNYCH KARTECZEK! — zarządza kierownik.
— To gdzie zapisujemy hasła?
— W GŁOWIE!
— Czyjej?
— MOJEJ!

Trzy lata później.

— Panie kierowniku, potrzebujemy hasła do archiwum.
— ...
— Panie kierowniku?
— CZY NIE MOŻNA PRZYWRÓCIĆ MOJEJ PAMIĘCI Z BACKUPU?!

🤣🤣🤣

Papierowa kopia hasła albo klucza odzyskiwania **nie jest z definicji zła**. Może mieć sens, jeśli jest zabezpieczona i przechowywana oddzielnie od nośnika. Dobrym rozwiązaniem bywa też odpowiednio chroniony menedżer haseł i niezależna procedura odzyskania dostępu. Najgorszy pomysł to świetnie zaszyfrować jedyną kopię i trwale zgubić możliwość jej odczytania.

Rozdział dziewiąty: czy szyfrowanie jest wieczne?

— PANOWIE! BACKUP JEST ZASZYFROWANY! CZYLI NIKT GO NIGDY NIE ODCZYTA?!
— Takiej gwarancji nie ma.
— JAK TO?!
— Mogą pojawić się błędy, słabe hasła i nowe możliwości ataków. Rozwija się też informatyka kwantowa.
— TO KOMPUTER KWANTOWY PRZYJDZIE MI CZYTAĆ FAKTURY?!
— Nie wszystkie algorytmy są tak samo zagrożone.
— TO MOŻE SCHOWAM DYSK POD SKARPETKAMI?!
— Najlepiej zaszyfrowany i z osobno przechowywanym kluczem.

🤣

Żadnemu praktycznemu wdrożeniu szyfrowania nie można obiecać stuprocentowego bezpieczeństwa na zawsze. Szczególnie zagrożone przez dostatecznie zaawansowane komputery kwantowe są popularne dziś mechanizmy kryptografii klucza publicznego, takie jak RSA i ECC. **AES-256**, używany do szyfrowania

danych, nie jest przez znane ataki kwantowe łamany w taki sam sposób i pozostaje mocnym wyborem przy poprawnej implementacji, dobrych kluczach i hasłach.

Nie ma jednak powodu rezygnować z **szyfrowania**. Trzeba je rozsądnie stosować, aktualizować systemy i pamiętać, że często słabszym ogniwem jest hasło na karteczce przyklejonej do dysku, a nie sam algorytm.

Rozdział dziesiąty: reguła 3-2-1 i kierownik bez ograniczeń

— PANIE KIEROWNIKU, ZALECA SIĘ ZASADĘ 3-2-1.
— CO TO JEST?!
— Trzy kopie danych łącznie, dwa rodzaje nośników, jedna kopia poza lokalizacją — to popularna wersja tej reguły.
— A MOGĘ MIEĆ SIEDEM?!
— Oczywiście.
— W CZTERECH MIEJSCACH?!
— Jak najbardziej.
— TO PROSZĘ NIE OGRANICZAĆ MOJEJ KREATYWNOŚCI!

🤣🤣

3-2-1 to przydatna zasada orientacyjna, a nie magiczny wzór gwarantujący bezpieczeństwo. Spotyka się też rozszerzenie **3-2-1-1-0**: dodatkowa kopia offline lub immutable oraz zero błędów potwierdzonych weryfikacją. Najważniejsze nie są jednak same liczby, lecz niezależność kopii, ryzyko wspólnego usunięcia oraz możliwość ich odtworzenia.

Pięć archiwów pod jednym przejętym kontem może być mniej odporne niż kilka rzeczywiście odseparowanych kopii. Dobrze zaprojektowany backup nie powinien też być tak uciążliwy, żeby człowiek przestał go wykonywać.

Rozdział jedenasty: backup zakończony sukcesem. A odtworzenie?

— PANIE KIEROWNIKU! BACKUP ZAKOŃCZONY SUKCESEM!
— WSPANIALE!
— Codziennie od dwóch lat!
— CUDOWNIE!
— A próbowaliśmy odtworzyć pliki?
— ...
— Sprawdzaliśmy kompletność archiwów?
— ...
— Testowaliśmy odzyskanie całego systemu?
— PANIE! NIE PO TO ROBIMY BACKUPY, ŻEBY JE POTEM ODCZYTYWAĆ!

🤣🤣🤣

Komunikat „backup completed successfully” nie jest dowodem, że przywrócimy potrzebne dane. Warto regularnie **testować odtwarzanie**, sprawdzać kompletność, pamiętać o kluczach **szyfrowania**, konfiguracji aplikacji, **bazach danych** i zależnościach. Odzyskanie jednego pliku to nie zawsze to samo co uruchomienie całej firmy po awarii.

RPO mówi, jak dużo najnowszych danych możemy zaakceptować jako utracone (np. jeden dzień pracy). **RTO** określa, jak długo możemy czekać na przywrócenie działania. Dwa proste pytania pomagają dobrać częstotliwość i sposób wykonywania kopii.

— ILE MOŻEMY STRACIĆ?!
— Zależy od danych.
— I JAK DŁUGO MOŻEMY CZEKAĆ?!
— Zależy od działalności.
— CZYLI ZNOWU NIE MA JEDNEJ IDEALNEJ ODPOWIEDZI?!
— Dokładnie.

Rozdział dwunasty: backup ma działać również w zwykłym domu

Nie tylko serwer firmowy potrzebuje kopii. Zdjęcia rodzinne, dokumenty, pliki z telefonu, własne projekty czy archiwum ważnych wiadomości mogą być trudniejsze do odtworzenia niż zakup nowego komputera.

Stary dysk, pendrive, drugi komputer, kopia w chmurze — nawet prosty początek jest cenny, jeśli da się z niego odzyskać dane. Z czasem można dodać automatyzację, kolejną lokalizację, wersjonowanie i ochronę przed usunięciem. **Backup, którego nie robisz, bo jest zbyt skomplikowany, jest gorszy od prostego backupu, który rzeczywiście wykonujesz.**

Finał: czy w tej informatyce można mieć święty spokój?

Minęły trzy miesiące od pożaru. Firma ma nowy budynek, nowe serwery, kilka niezależnych sposobów odzyskania danych i procedurę testowania kopii.

— PANOWIE! MAMY BACKUPY W KILKU MIEJSCACH!
— Tak.
— CZĘŚĆ JEST OFFLINE!
— Tak.
— CZĘŚĆ MA HISTORIĘ WERSJI!
— Zgadza się.
— I PRÓBOWALIŚMY JE ODTWORZYĆ?!
— Wczoraj. Udało się.
— WSPANIALE! TO TERAZ MOŻEMY PRZESTAĆ ROBIĆ BACKUPY!
— Nie, panie kierowniku.
— ...
— Kopie trzeba wykonywać nadal.
— CZY W TEJ CHOLERNEJ INFORMATYCE COKOLWIEK MOŻNA ZROBIĆ RAZ I MIEĆ SPOKÓJ?!

Zza drzwi odzywa się księgowa.

— Można raz stracić wszystkie dane.

🤣🤣🤣🤣

Zapamiętaj trzy rzeczy: nie ma głupiego backupu — głupi jest brak backupu; prosty, regularnie wykonywany backup bywa lepszy od idealnego planu, którego nikt nie realizuje; najważniejszy jest ten backup, **z którego naprawdę można odzyskać dane**.

Dyrekcja Centralnego Magazynu Dokumentów informuje, że dysk księgowej otrzymał medal za zasługi dla firmy. Skarpetki pozostały anonimowe ze względów bezpieczeństwa.