Kopie zapasowe

Cele Lekcji

01

Poznaj backup

Zrozumieć, czym jest backup i dlaczego jest niezbędny w codziennym życiu cyfrowym

02

Odkryj zasadę 3-2-1

Nauczyć się zasady ochrony danych, która chroni przed utratą informacji

03

Przeanalizuj ryzyka

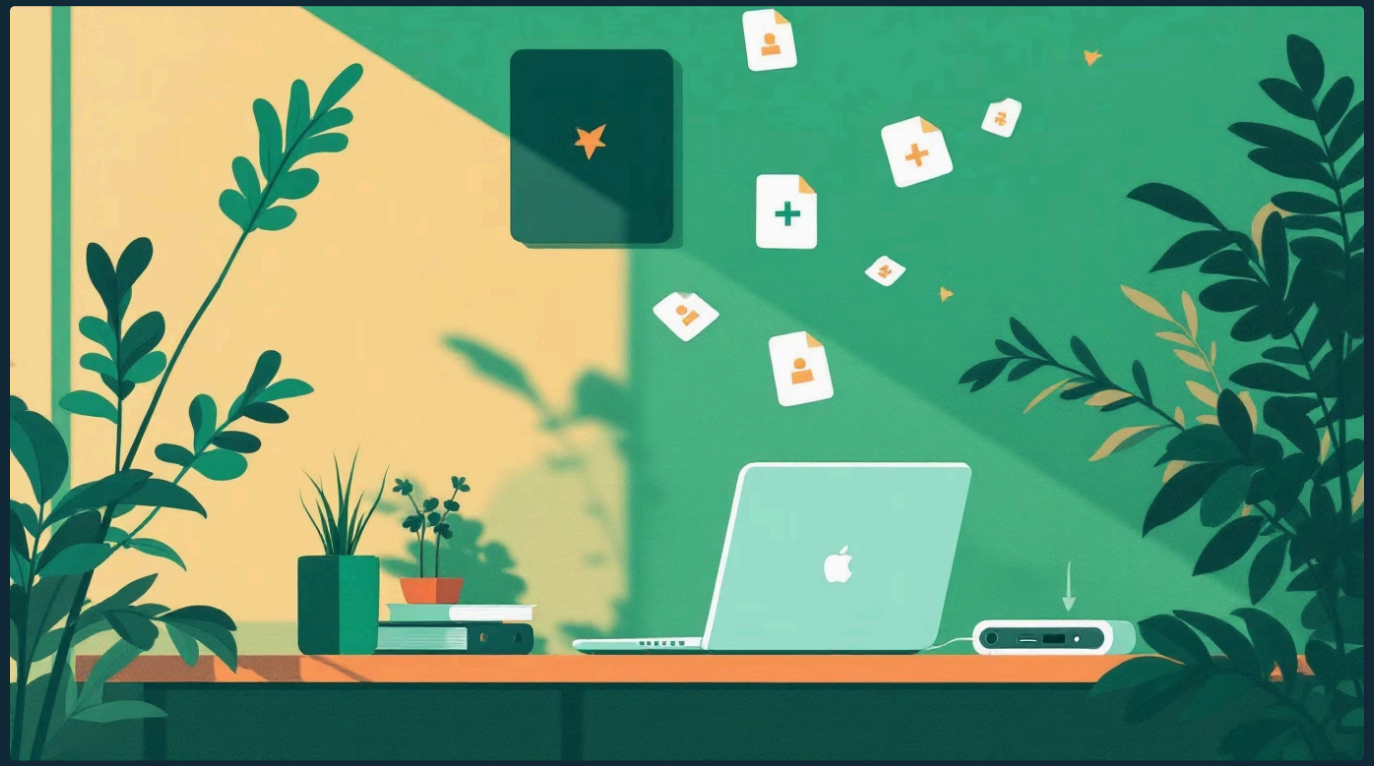
Rozpoznać konsekwencje utraty danych w kontekście biznesowym i osobistym

04

Wybierz nośniki

Poznać różne sposoby przechowywania kopii zapasowych i ich zastosowania

Czym Jest Backup?



Twoja definicja

Przedstaw swoje zrozumienie pojęcia backupu na podstawie własnych doświadczeń z ochroną danych.

Pytania do refleksji

- Kiedy ostatnio utworzyłeś kopię swoich danych?
- Jakie pliki są dla Ciebie najważniejsze?
- Co by się stało, gdybyś je utracił?

Zasada 3-2-1 w Ochronie Danych

3 Kopie

Oryginalne dane plus dwie kopie zapasowe

2 Nośniki

Różne typy urządzeń przechowujących

1 Poza Lokalizacją

Kopia w innym miejscu geograficznym

Ta zasada chroni przed najpopularniejszymi przyczynami utraty danych: awariami sprzętu, atakami malware, kradzieżą i katastrofami naturalnymi.

Nośniki Danych - Przykłady

Dysk zewnętrzny

Fizyczne urządzenie przenośne, idealne do lokalnych kopii zapasowych

Chmura

Przechowywanie online, dostęp z dowolnego miejsca, automatyczne kopie

NAS

Serwer w sieci lokalnej, łączący zalety dysku i chmury

Przykład Zastosowania Zasady 3-2-1

1

Komputer

Oryginalne dane

2

Dysk zewnętrzny

Pierwsza kopia lokalna

3

Chmura

Kopia zdalna

Przykład praktyczny: Fotograf przechowuje zdjęcia na laptopie (oryginał), kopiuje na dysk zewnętrzny w domu (pierwsza kopia) i uploaduje do usługi chmurowej (druga kopia poza lokalizacją).

Przykładowe realne sytuacje

Pożar serwerowni OVH w Strasbourgu. Wiele danych “nie do odzyskania”

Pożar serwerowni OVH sparaliżował internet. Podliczyli szkody

Ofiarą pożaru padł niemal co piąty adres IP w chmurze OVH. Dotknął tym samym agencje rządowe z Wybrzeża Kości Słoniowej i Francji, kryptowalutowe serwisy oraz serwisy bankowości internetowej - wynika z raportu firmy Netcraft.

Sytuacja Problemowa

Firma logistyczna

Firma „EcoTransport” obsługuje dostawy paczek dla lokalnych sklepów. Wszystkie dane o zamówieniach (adresy, listy paczek, trasy kierowców) są zapisywane na jednym komputerze w biurze. Raz na jakiś czas pracownik robi kopię zapasową na pendrive, który trzyma w szufladzie.

Pewnego dnia dochodzi do awarii – dysk w komputerze przestaje działać i nie można odzyskać danych. Firma próbuje użyć kopii zapasowej z pendrive’a, ale okazuje się, że:

- kopia była wykonana ponad 2 tygodnie temu,
- pendrive był podłączony do tego samego komputera i również uległ uszkodzeniu.

W efekcie:

- firma traci wszystkie aktualne dane o zamówieniach,
- nie wie, jakie paczki mają być dostarczone,
- musi prosić klientów o ponowne przesłanie informacji,
- ponosi straty finansowe i traci zaufanie klientów.

Konsekwencje Utraty Danych

Utrata przychodów

Niezdolność do dostarczenia produktów klientom prowadzi do zwrotów pieniędzy i utraty wpłat z zamówień

Koszty naprawy

Wydatki na profesjonalną odzyskiwanie danych, nowy sprzęt i odbudowę systemu

Utrata klientów

Niezaufanie i negatywne recenzje spowodowane brakiem dostępu do unikalnych, niepowtarzalnych zdjęć

Czas odbudowy

Strata miesięcy pracy, konieczność ponownego nawiązania kontaktu z klientami i rekonstrukcji projektów

Jak Uniknąć Utraty Danych?

Planuj regularne kopie

Ustal harmonogram tworzenia kopii zapasowych - dziennie, tygodniowo lub miesięcznie w zależności od ważności danych

Testuj kopie

Regularnie sprawdzaj, czy kopie są poprawne i można z nich przywrócić dane

Automatyzuj proces

Używaj oprogramowania do automatycznego tworzenia kopii, aby uniknąć zapomnienia

Ochroniaj przed zagrożeniami

Instaluj aktualizacje, używaj antywirusów i zachowaj ostrożność przed podejrzanymi plikami

Co to jest RPO i RTO?

Definicja RPO (Recovery Point Objective)

RPO (ang. Recovery Point Objective) to parametr, opisujący częstotliwość oraz moment wykonywania kopii zapasowych w odniesieniu do prawdopodobieństwa wystąpienia awarii i jej wpływu na funkcjonowanie organizacji. Innymi słowy RPO mówi, kiedy wykonać backup, by wystąpienie awarii nie wpłynęło w znaczący sposób na ciągłość pracy operacyjnej przedsiębiorstwa.

Definicja RTO (Recovery Time Objective)

Kolejny termin to RTO (ang. Recovery Time Objective). Określa on ile w praktyce będzie trwało odtworzenie z kopii zapasowej wszystkich utraconych danych. Mamy tu na myśli odtworzenie ich i przywrócenie pracy wszystkich powiązanych systemów oraz usług do stanu z momentu tworzenia danej wersji backupu.

Podsumowanie

Kluczowe wnioski

- Backup to fundament bezpieczeństwa cyfrowego
- Zasada 3-2-1 zapewnia kompletnej ochrony
- Utrata danych ma poważne konsekwencje finansowe i emocjonalne
- Prewencja jest zawsze lepsza niż kuracja

Zadanie 1

Na podstawie przydzielonej firmy uzupełnij tabelę projektu backupu. Określ, jakie dane należy zabezpieczyć, jak często wykonywać kopie zapasowe, na jakich nośnikach je przechowywać oraz czy rozwiązanie spełnia zasadę 3-2-1. Uwzględnij także koszty i odpowiedzialność pracowników.

	A	B	C	D	E	F	G	H	I	J
1	**ETAP 1 – PROJEKT BACKUPU**									
2										
3	**Firma**	**Dane do backupu**	**Częstotliwość**	**Nośnik 1**	**Nośnik 2**	**Kopia off-site**	**Spełnia 3-2-1**	**Koszt miesięczny**	**Odpowiedzialny pracownik**	**Komentarz/uwagi**

Firma
Sklep internetowy
Biuro rachunkowe
Szkoła
Gabinet lekarski
YouTuber
Biuro projektowe
Serwis IT
Biblioteka
Studio fotograficzne

Zadanie 2 – ANALIZA AWARII

Na podstawie opisanego przypadku przeanalizuj skutki awarii w firmie. Uzupełnij tabelę, określając, czy firma przetrwa, ile danych może utracić, jaki będzie czas odtworzenia systemu (RTO) oraz ile danych zostanie utraconych (RPO). Na końcu zapisz wnioski i zaproponuj, co należy poprawić, aby uniknąć podobnych problemów w przyszłości.

A	B	C	D	E	F	G	H	I
Rodzaj awarii	**Firma**	**Czy firma przetrwa? (TAK/NIE)**	**Ile danych stracimy?**	**Czas odtworzenia**	**Wnioski**	**RPO (ile danych tracimy)**	**RTO (czas odtworzenia)**	**Co można poprawić?**

Firma	Rodzaj awarii
Sklep internetowy	ransomware
Biuro rachunkowe	awaria dysku
Szkoła	pożar serwerowni
Gabinet lekarski	kradzież laptopa
YouTuber	zalanie biura
Biuro projektowe	ransomware
Serwis IT	awaria NAS
Biblioteka	pożar serwerowni
Studio fotograficzne	awaria dysku

RPO - **Recovery Point Objective / RTO** - Recovery Time Objective

Ciekawostka na koniec