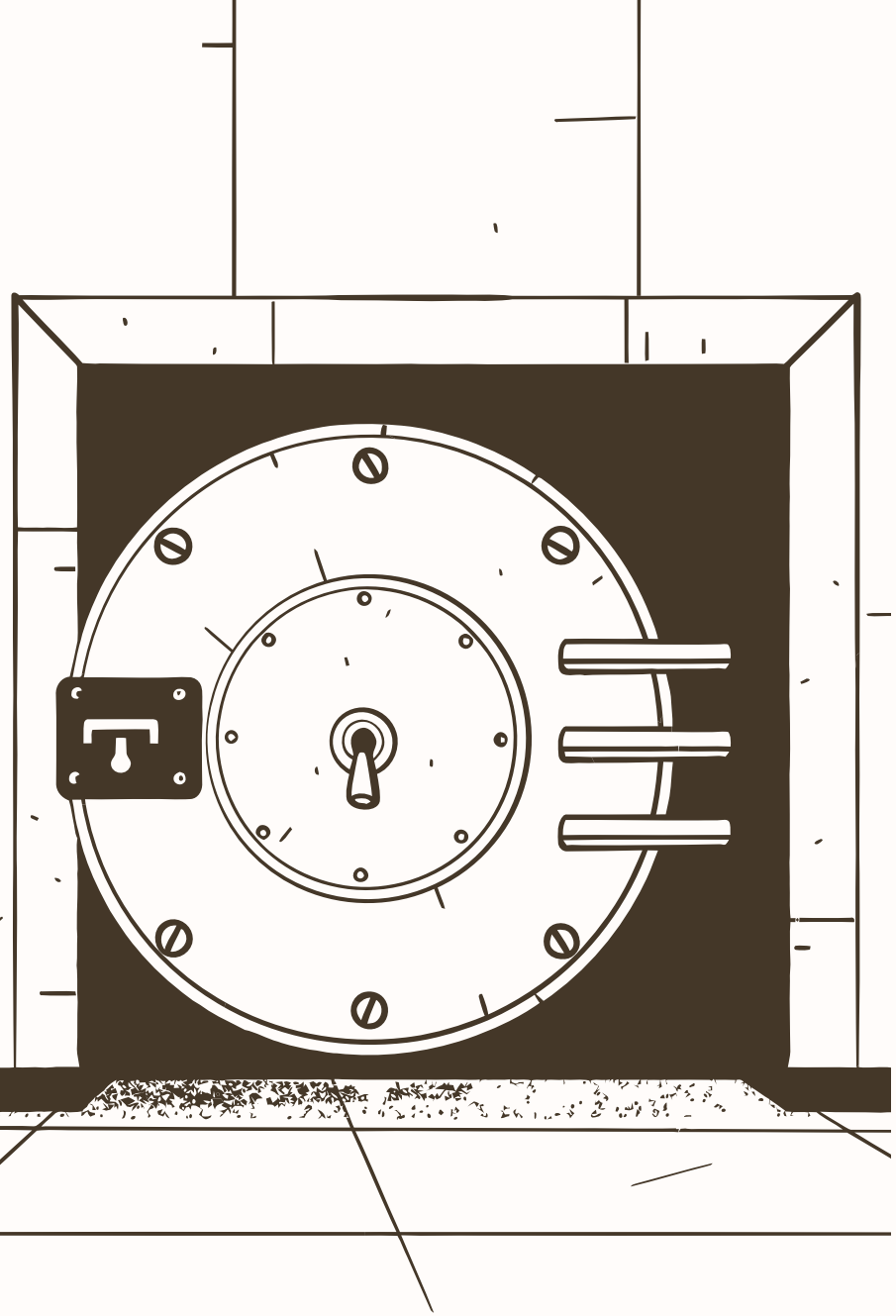


Ransomware - działanie i ochrona przed szyfrowaniem danych

Ransomware to jeden z najgroźniejszych typów cyberataków, który może dotknąć zarówno duże organizacje, jak i indywidualnych użytkowników. W tej prezentacji omówimy, czym jest ransomware, jak działa, jakie zagrożenia niesie oraz - co najważniejsze - jak się przed nim skutecznie chronić.

Poznasz krok po kroku mechanizm działania tego złośliwego oprogramowania oraz praktyczne wskazówki, które pomogą zabezpieczyć Twoje cenne dane przed cyberszantażystami.

Czym jest ransomware?

Definicja

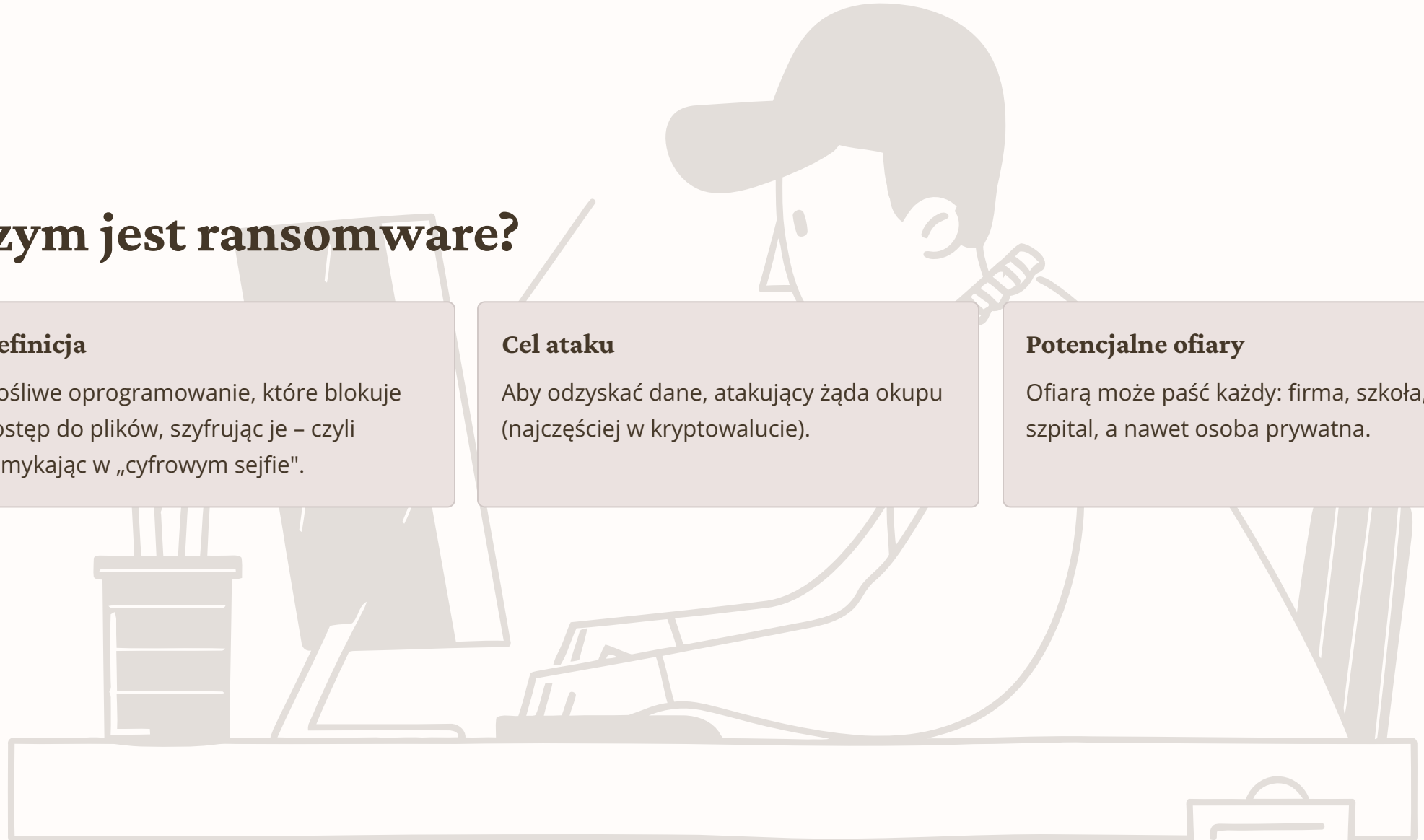
Złośliwe oprogramowanie, które blokuje dostęp do plików, szyfrując je – czyli zamykając w „cyfrowym sejfie".

Cel ataku

Aby odzyskać dane, atakujący żąda okupu (najczęściej w kryptowalucie).

Potencjalne ofiary

Ofiarą może paść każdy: firma, szkoła, szpital, a nawet osoba prywatna.



Jak działa ransomware – krok po kroku

Infekcja

Ransomware dostaje się do komputera np. przez fałszywy załącznik w e-mailu, pobranie zainfekowanego pliku lub złośliwe oprogramowanie z nieznanego źródła.

Szyfrowanie danych

Program blokuje dostęp do dokumentów, zdjęć, arkuszy, baz danych, również plików sieciowych lub dysków zewnętrznych.

Żądanie okupu

Pojawia się komunikat z żądaniem zapłaty w zamian za odszyfrowanie danych.

Szantaż

Czasami atakujący grozi, że dane zostaną opublikowane, sprzedane lub całkowicie usunięte.

Co może się stać po ataku ransomware?

Utrata dostępu

Firma traci dostęp do systemów i dokumentów, co paraliżuje jej działanie.

Zatrzymanie pracy

Praca staje – nie można wystawić faktur, sprawdzić maili, obsłużyć klientów.

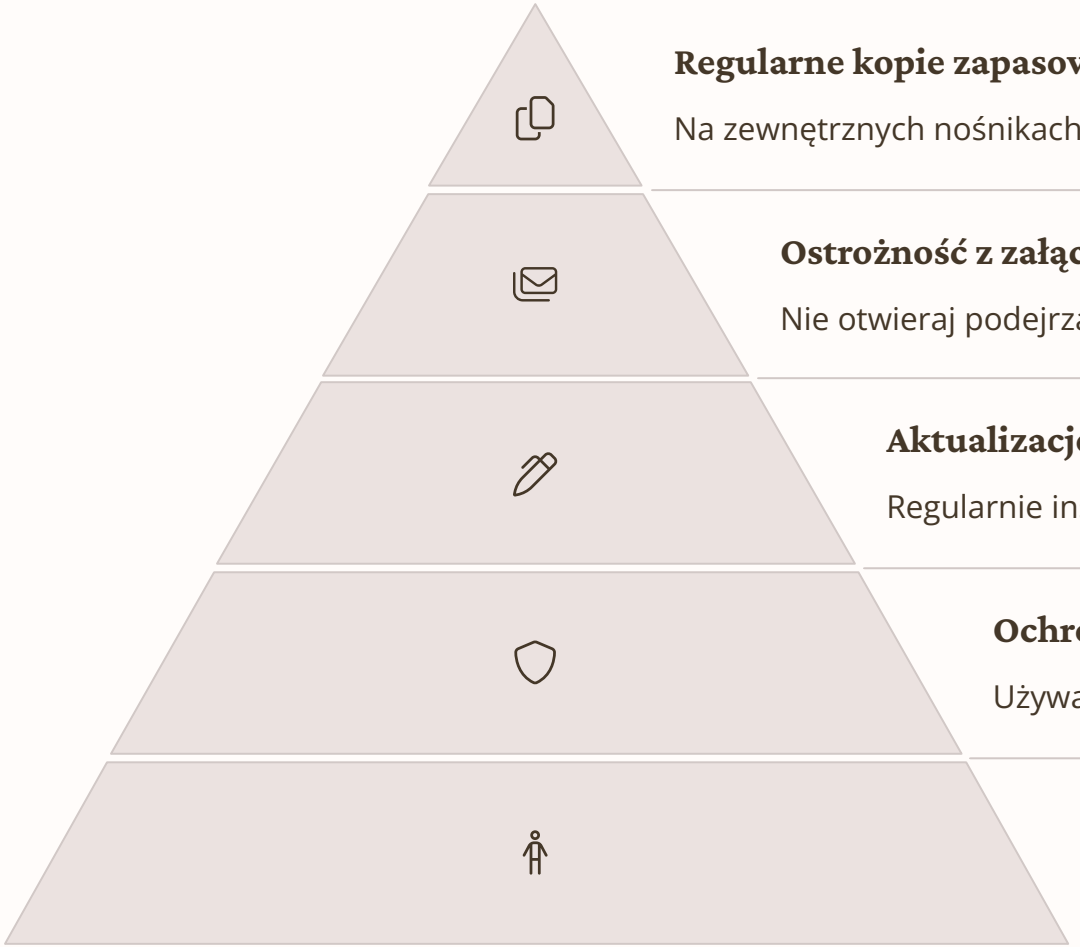
Konsekwencje prawne

Ujawnienie lub utrata danych (również osobowych) może narazić organizację na kary i odpowiedzialność.

Brak gwarancji

Odzyskanie danych nie zawsze jest możliwe – nawet po zapłaceniu okupu.

Jak się chronić przed ransomware?



Regularne kopie zapasowe

Na zewnętrznych nośnikach lub w zaufanej chmurze

Ostrożność z załącznikami

Nie otwieraj podejrzanych plików

Aktualizacje systemów

Regularnie instaluj poprawki bezpieczeństwa

Ochrona antywirusowa

Używaj dobrego programu i zapory sieciowej

Świadomość użytkowników

Szkol pracowników z zasad bezpieczeństwa

Pamiętaj, że najsłabszym ogniwem w systemie bezpieczeństwa często jest człowiek. Dlatego edukacja i świadomość zagrożeń są równie ważne jak techniczne zabezpieczenia.

Co robić, jeśli dojdzie do ataku?

Nie płać okupu

Nie ma gwarancji, że dane zostaną przywrócone, a płacenie zachęca przestępców do kolejnych ataków.

Odłącz zainfekowany sprzęt

Natychmiast odłącz urządzenie od sieci, aby ograniczyć rozprzestrzenianie się wirusa na inne komputery.

Skontaktuj się ze specjalistami

Powiadom dział IT lub zewnętrznych ekspertów ds. bezpieczeństwa, którzy pomogą ocenić sytuację.

Zgłoś incydent

Poinformuj odpowiednie służby (np. CSIRT, policję, UODO – jeśli dotyczy danych osobowych).

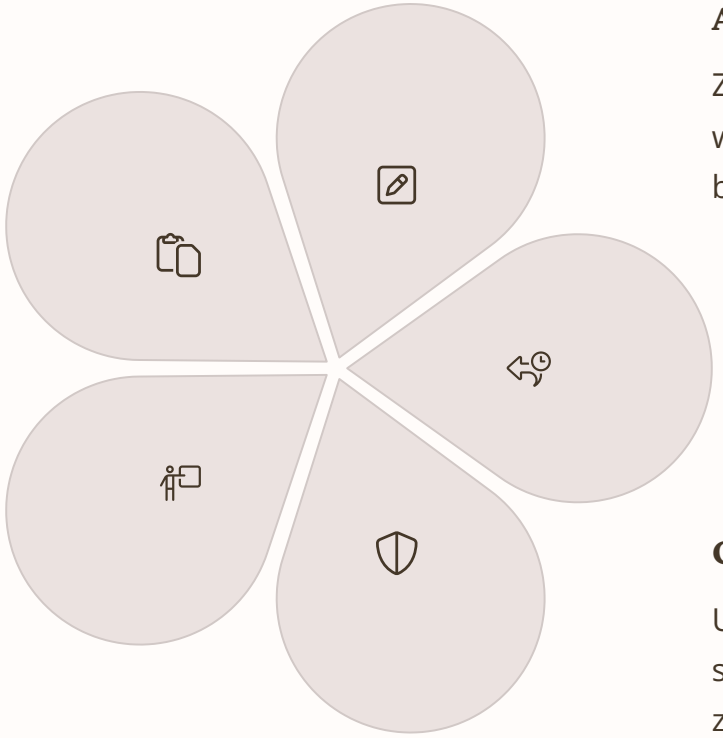
Podsumowanie – zasady ochrony przed ransomware

Kopie zapasowe

Rób regularne kopie zapasowe danych i przechowuj je oddzielnie od głównego systemu.

Edukacja

Edukuj siebie i innych – ostrożność i świadomość zagrożeń to najlepsza tarcza.



Aktualizacje

Zawsze aktualizuj system operacyjny i wszystkie programy, aby zamknąć luki bezpieczeństwa.

Ostrożność

Nie otwieraj nieznanych załączników i linków, nawet jeśli wydają się pochodzić od znajomych.

Ochrona

Używaj ochrony antywirusowej i zapory sieciowej, które mogą wykryć i zablokować zagrożenia.