



JAKIE KOSZTY MOŻE WYGENEROWAĆ AWARIA IT W TWOJEJ FIRMIE?

JAKIE KONSEKWENCJE NIESIE BRAK PRZYGOTOWANIA NA TAKIE SYTUACJE?

Każda godzina przestoju IT ma swoją cenę.

Profesjonalne przygotowanie na sytuacje awaryjne to dziś „must have” dla zachowania ciągłości działania biznesu.

Co ważne, nie wymaga to ogromnych nakładów finansowych, lecz przede wszystkim metodycznego zaplanowania działań.

NIE MASZ CZASU? PODSUMOWANIE W PIGUŁCE

- **Atak ransomware w biurze rachunkowym** często oznacza **wstrzymanie ciągłości biznesu i wysokie ryzyko opóźnień JPK/ZUS/US** – nie dlatego, że chmura przestaje działać, lecz dlatego, że firma **traci bezpieczny dostęp do danych, podpisów i zespołu** oraz musi **zweryfikować integralność dokumentów**.
- **Koszt incydentu (wariant referencyjny):** **~260 tys. zł, z czego ~200 tys. zł to okup;** reszta to przestój, technika i weryfikacja danych
- **Mit „zapłacimy i po sprawie”:** po odszyfrowaniu **nie ma gwarancji** kompletności i spójności danych — trzeba je **weryfikować** z dokumentami źródłowymi.
- **Co zmienia wynik:** właściwy backup **poza zasięgiem ataku** + testy co kwartał pozwalają nie płacić okupu.
- **Efekt po wdrożeniu:** **1–2 dni przerwy i ~20–30 tys. zł kosztów,** bez „ruletki” z danymi; do tego MFA, porządek uprawnień, nowoczesna ochrona stacji i krótkie szkolenia anty-phishingowe.



BIURO RACHUNKOWE

SYTUACJA WYJŚCIOWA

Działalność lokalna:

Jeden oddział; obsługa klientów lokalnie + zdalna z obszaru całego kraju.

Struktura zatrudnienia:

10 księgowych (tryb pracy hybrydowy).

Liczba obsługiwanych klientów:

Około 150 klientów.

Średni przychód z klienta:

Około 1500 zł netto miesięcznie (różne modele współpracy/rodzaje klientów, dywersyfikacja usług: księgowość, kadry płace, usługi dodatkowe).

ARCHITEKTURA INFRASTRUKTURY IT:

1. Sieć i bezpieczeństwo:

- Firewall UTM z IPS/IDS, filtrowaniem treści i VPN SSL z MFA.
- EDR/antywirus biznesowy na stacjach i serwerach.

2. Serwery i przechowywanie:

- Serwer lokalny, ERP, pliki.
- Backup hybrydowy (NAS RAID6 + chmura).
- Testy odtwarzania backupów – brak w praktyce.

3. Oprogramowanie:

- Dostęp do aplikacji księgowych odbywa się przez zdalny pulpit/terminal: programy uruchomione są na serwerze, a na stanowiskach wyświetlany jest jedynie ich ekran.
- Office 365 / Google Workspace (e-mail, archiwizacja).
- **Systemy:** ERP (Comarch/ Enova365), kadrowo-płacowe, e-deklaracje (ZUS, US).

4. Dostęp i kontrola:

- MFA do ERP i VPN.
- Szyfrowanie danych na dyskach lokalnych.

SCENARIUSZ AWARII:

- **Atak ransomware zaszyfrował systemy ERP i dane klientów w biurze rachunkowym, a niesprawna synchronizacja danych z chmurą, uniemożliwiła szybkie odtworzenie. Firma podjęła decyzję o zapłaceniu okupu.**
- **Żądanie okupu: 200 000 zł.**
- **Czas trwania awarii:** 5 dni (pełny brak systemów).
- **Zdarzenie kwalifikuje się jako naruszenie RODO** → obowiązek zgłoszenia, ryzyko kary i utraty klientów.

PODJĘTE DZIAŁANIA:

ROAD MAPA przywrócenia systemów do działania:

1. Diagnostyka i analiza incydentu.
2. Nieskuteczna próba odtworzenia danych.
3. Opłata okupu i uzyskanie kluczy deszyfrujących.
4. Odszyfrowanie danych i weryfikacja ich integralności.
5. Testy końcowe i walidacja działania.
6. Przegląd bezpieczeństwa systemów i usług IT.
7. Działania prawne i organizacyjne.
8. Działania prewencyjne i ponowny audyt bezpieczeństwa.

KOSZTY INCYDENTU:

1. Koszty pracownicze:

- 5 dni, bezproduktywne godziny pracownicze: $10 \times 325 \text{ zł (średnia stawka)} \times 5 = 16\ 250 \text{ zł}$.
- Weryfikacja odtworzonych i wprowadzanie zaległych danych: $14 \text{ dni} \times 10 \text{ osób} \times 325 \text{ zł} = 45\ 500 \text{ zł}$. **Razem: 61 750 zł.**

2. Koszty utraconego przychodu:

Rozliczanie klientów realizowane jest w trybie miesięcznym, biuro nie traci przychodu, koszty pojawiają się w czasie potrzebnym do nadrobienia zaległości powstałych podczas niedostępności systemów.

3. Koszty techniczne odzyskiwania danych:

Outsourcing specjalistów IT + odzyskiwanie danych = **15-20 tys. zł** (estymacja wg cen dostępnych na rynku, zależnie od stopnia uszkodzeń i konieczności wsparcia konsultantów zewnętrznej firmy). **Okup: 200 000 zł.**

4. Koszty dodatkowe (niematerialne, ale realne):

- Ryzyko utraty klientów i reputacji (trudne do wyceny – potencjalnie dziesiątki tys. zł w długim okresie).
- Możliwe kary administracyjne za naruszenie RODO/danych osobowych/finansowych

WNIOSKI:

1. Łączny koszt incydentu: 260 tys. zł.

Struktura: 200 tys. zł to żądanie okupu; pozostałe 60 tys. zł to technika, przestój i weryfikacja danych.

2. “Zapłacimy i po sprawie?” - niekoniecznie!

Fakt: po „odszyfrowaniu” nie ma gwarancji, że dane są kompletne i niezmienione.

Skutek: konieczna żmudna weryfikacja z dokumentami źródłowymi (czas, koszty, ryzyko błędów).

Decyzja: strategia firmy musi zakładać **niepłacenie okupu**, tylko sprawne odtworzenie danych.

3. Backup + testy = brak okupu, krótszy przestój.

Fakt: poprawnie utrzymany backup (model 3-2-1, kopia odseparowana/niemodyfikowalna, testy co kwartał) pozwala wrócić do pracy w 1–2 dni.

Skutek finansowy: 20–30 tys. zł łącznych kosztów zamiast 260 tys. zł.

Decyzja: wdrożenie i testowanie backupu to najtańsze „ubezpieczenie operacji”.

4. Minimalny pakiet zabezpieczeń, który robi różnicę

Dostępny: wieloskładnikowe logowanie (MFA) do poczty i systemów, porządek ról i uprawnień.

Stacje/serwery: nowoczesna ochrona (EDR) i aktualizacje.

Ludzie: krótkie, cykliczne szkolenia antyphishingowe zmniejszają liczbę „kliknięć” i szansę wystąpienia incydentu.

**JEŚLI CHCESZ SIĘ DOWIEDZIEĆ,
W JAKI SPOSÓB MOŻESZ
ZABEZPIECZYĆ SWOJE IT
UMÓW SIĘ NA BEZPŁATNĄ
KONSULTACJĘ.**