Cyberchaos w małej firmie

Jak odzyskać kontrolę nad bezpieczeństwem — Round Table / Warsztat

BEZPIECZEŃSTWO | MAŁE FIRMY | PRAKTYCZNE ZASADY

Dla kogo jest ten warsztat?

👤 Właściciele JDG i małych firm

Osoby zarządzające operacyjnie, które nie mają dedykowanego zespołu ds. cyberbezpieczeństwa.

🔥 Po incydencie

Gdy firma doświadczyła phishingu, podejrzanego przelewu lub wycieku danych.

📈 Przy skalowaniu

Gdy zespół rośnie i nikt nie panuje nad tym, kto ma dostęp do czego.

> „To nie będzie klasyczna prezentacja. Chcę, żebyśmy porozmawiali o tym, gdzie w małych firmach **realnie powstaje ryzyko**. Im więcej konkretnych przykładów z sali, tym większa wartość dla wszystkich."

ⓘ To nie jest wykład — spotkajmy się z praktyką!

Teza: Większość ataków nie wymaga hakera

> „Większość ataków na małe firmy nie zaczyna się od zaawansowanego hakera. Zaczyna się od prostych rzeczy: **hasła w mailu, dostępu po byłym pracowniku, braku weryfikacji przelewu.**"

Największe ryzyko

Były pracownik, który **nadal ma dostęp** do systemów firmy.

Pytanie otwierające

„Kto z Was wie dziś dokładnie, kto ma dostęp do **wszystkich kluczowych systemów**?"

Ryzyko zaczyna się od dostępu, którego nikt nie kontroluje.

AKT 1: Chaos Operacyjny (10–30 min)

Cyberbezpieczeństwo w małej firmie zaczyna się od **porządku, nie od narzędzi**.

Brak zasad dostępu

Nikt nie wie, kto ma dostęp, gdzie są dane i kto za co odpowiada. Za szerokie uprawnienia to norma.

Hasła w mailach i Excelach

Dane logowania krążą w wiadomościach, arkuszach i notatkach. Każdy może je przejąć.

Byli pracownicy z dostępem

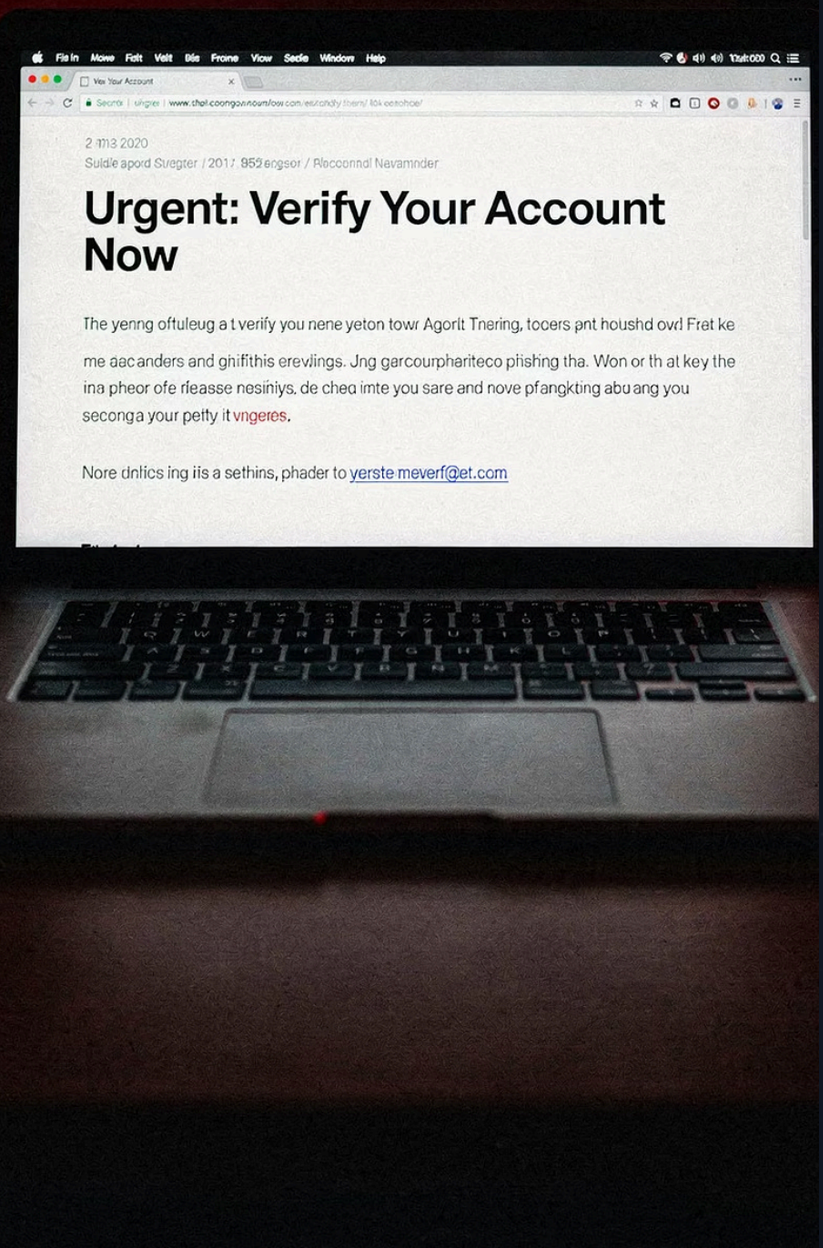
Odejście z firmy nie oznacza automatycznego odebrania dostępów do poczty, dysku i CRM.

Prywatne konta służbowo

Pracownicy używają prywatnych kont do firmowej komunikacji — dane firmy trafiają poza kontrolę.

⚠ 👉 **Kluczowa zasada:** Ryzyko zaczyna się od wygody. Nie da się chronić czegoś, czego nie masz spisanego.

> 🔑 **Metafora:** Poczta to pilot do firmy. Kto ma pocztę, często może sterować resztą.



AKT 2: Moment Pęknięcia (30–40 min)

Atak często wygląda jak **zwykły dzień pracy**. Nie ma alarmu, nie ma hakera w kapturze — jest tylko mail i pośpiech.

To nie jest filmowy atak. To zwykły mail, zwykła faktura i zwykły pośpiech — a firma traci pieniądze, zanim cokolwiek zauważy.

💸 Najdroższy klik w firmie

To przycisk **„Wyślij przelew"** — kliknięty bez weryfikacji, pod presją czasu.

Pytania prowokujące

- Czy u Was zmiana numeru konta przechodzi tylko mailem?
- Czy ktoś może zatwierdzić przelew bez drugiej osoby albo drugiego kanału?

Pieniądze uciekają tam, gdzie decyzje podejmuje się w pośpiechu.

Rozwiązanie: Safe Word — darmowa bariera (40–50 min)

> „Safe Word to proste hasło ustalone wcześniej. Jeśli ktoś prosi o przelew, zmianę konta albo nietypowe działanie — **musi potwierdzić safe word**."

1

Prośba o przelew lub zmianę konta

Mail, WhatsApp, telefon — nieważne skąd przychodzi.

2

Żądanie potwierdzenia Safe Word

„OK, potwierdź safe word albo dzwonię na znany numer."

3

Weryfikacja drugim kanałem

Telefon na znany numer lub osobiste potwierdzenie.

Zatrzymuje socjotechnikę

Zatrzymuje deepfake

Zatrzymuje presję czasu

Kosztuje 0 zł

👉 Safe Word to **hamulec ręczny dla pieniędzy**. Prosta zasada, zero kosztów, natychmiastowy efekt.

AKT 3: Co NIE działa — Iluzja bezpieczeństwa (50–65 min)

„Mamy IT" nie znaczy **„mamy bezpieczeństwo"**. Firmy często mają narzędzia, ale nie mają kontroli.

Najczęstsze błędy

- „Mamy IT, więc jesteśmy bezpieczni"
- Narzędzia zamiast zasad
- Outsourcing bez nadzoru i kontroli
- Backup mylony z synchronizacją

Mit: Chmura = Backup

Usunięcie danych → synchronizacja usuwa wszędzie.

Ransomware → szyfruje wszystko w chmurze.

Brak historii wersji → brak możliwości odtworzenia.

⊗ 👉 **Synchronizacja = kopiowanie błędu.** Chmura nie zwalnia z odpowiedzialności za backup.

Rozwiązanie: Cloud-to-Cloud Backup

1

Backup poczty

Niezależna kopia całej skrzynki mailowej poza głównym dostawcą.

2

Backup dysku i chmury

Osobna usługa cloud-to-cloud dla Google Workspace lub Microsoft 365.

3

Historia wersji

Możliwość cofnięcia się do wcześniejszej wersji pliku lub folderu.

4

Test odzyskania

Regularny test, czy backup faktycznie działa i można z niego skorzystać.

> „Gdyby dziś zniknęła poczta albo folder z fakturami, ile czasu zajęłoby Wam odzyskanie pracy?"

⚠ 👉 **Backup, którego nie testowałeś, nie istnieje.**

Nowe ryzyko: Shadow AI (65–75 min)

> „Shadow AI to sytuacja, w której pracownicy używają narzędzi AI **bez zasad, bez kontroli** i często bez świadomości, jakie dane tam trafiają."

Co trafia do AI bez kontroli?

- Faktury i dane finansowe
- Dane osobowe klientów
- Umowy i dokumenty prawne
- Wewnętrzne procedury firmy

Skutki braku zasad AI

- Wyciek danych poza firmę
- Brak kontroli nad informacjami
- Brak świadomości pracowników
- Naruszenie RODO i umów

1

Największy wyciek 2026

Może nie wyjść przez hakera — tylko przez skrót w codziennej pracy z AI.

0 zł

Koszt zasad AI

Lista zakazanych danych i dozwolonych narzędzi kosztuje zero złotych.

⊗ 👉 **Największy wyciek = człowiek + AI bez zasad.** AI zwiększa produktywność i ryzyko jednocześnie.

Fundamenty 2026: Co DZIAŁA (75–85 min)

Bezpieczeństwo to **sposób pracy, nie projekt IT**. Oto cztery filary, które realnie chronią małą firmę.

1

Kontrola dostępu

- Lista: kto / do czego / po co
- Regularny przegląd uprawnień
- Natychmiastowe usuwanie zbędnych dostępów

2

MFA i Passkeys

- MFA na poczcie, banku, chmurze, social mediach
- Passkeys tam, gdzie dostępne
- Konto właściciela = konto administracyjne firmy

3

Clean Desk

- Brak haseł na kartkach
- Blokada ekranu po odejściu od biurka
- Niszczarka dla wrażliwych dokumentów

4

Zasady korzystania z AI

- Lista dozwolonych narzędzi AI
- Lista danych, których NIE wolno wrzucać
- Świadomość całego zespołu

ⓘ 👉 **Biurko też jest powierzchnią ataku.** Konto właściciela to konto administracyjne całej firmy.

3 Rzeczy na Poniedziałek (80–85 min)

Nie trzeba wielkiego projektu. Trzeba zacząć od **trzech decyzji**.

Zadanie 1: Lista dostępów

Spisz: kto ma dostęp, do czego, po co i czy nadal powinien mieć. Poczta, dysk, CRM, bank, social media.

Zadanie 2: MFA i Passkeys

Włącz na: poczcie, banku, chmurze, social mediach i wszystkich systemach firmowych.

Zadanie 3: Safe Word

Wdróż dla: przelewów, zmian kont bankowych, pilnych próśb i nietypowych decyzji.

> „Którą z tych trzech rzeczy realnie jesteście w stanie zrobić **w poniedziałek**?"

Bezpieczeństwo zaczyna się od **decyzji, nie od budżetu**.

Najważniejsze wnioski i zasady

- [ ] **Bezpieczeństwo zaczyna się od kontroli dostępu**

  Nie od narzędzi, nie od budżetu — od wiedzy, kto ma dostęp do czego.

- [ ] **Największe straty powstają przez decyzje, nie systemy**

  Przelew bez weryfikacji, zmiana konta tylko mailem — to kosztuje firmę pieniądze.

- [ ] **Narzędzia nie naprawią chaosu**

  Chmura nie jest backupem. Synchronizacja to kopiowanie błędu.

- [ ] **Pracownik jest największym ryzykiem i największą ochroną**

  AI bez zasad przyspiesza wycieki. Świadomy pracownik zatrzymuje ataki.

- [ ] **Proste zasady działają lepiej niż skomplikowane systemy**

  Safe Word, MFA, lista dostępów — zero złotych, maksymalny efekt.

Checklisty do wdrożenia

Gotowe działania — zacznij od poniedziałku.

🔐 Dostęp

- [ ] Lista wszystkich systemów
- [ ] Lista użytkowników z dostępami
- [ ] Przypisanie odpowiedzialności
- [ ] Usunięcie zbędnych dostępów

💰 Przelewy

- [ ] Wdrożenie Safe Word
- [ ] Weryfikacja drugim kanałem
- [ ] Zasada: brak zmian kont tylko mailem

☁️ Backup

- [ ] Backup chmury (cloud-to-cloud)
- [ ] Historia wersji włączona
- [ ] Test odzyskania danych

🔑 Logowanie

- [ ] MFA na kluczowych systemach
- [ ] Passkeys tam, gdzie możliwe
- [ ] Brak współdzielenia haseł

🤖 AI

- [ ] Lista dozwolonych narzędzi AI
- [ ] Lista zakazanych danych
- [ ] Świadomość pracowników

📃 Biuro

- [ ] Brak dokumentów na biurkach
- [ ] Blokada ekranów po odejściu
- [ ] Kontrola drukarki i niszczarka

Błędy — czego NIE robić

❌ Poleganie tylko na IT

IT dba o działanie systemów, nie zawsze o ryzyko biznesowe. Outsourcing bez nadzoru to iluzja bezpieczeństwa.

❌ Brak kontroli dostępu

Nikt nie wie, kto ma dostęp. Byli pracownicy nadal logują się do systemów firmy.

❌ Wysyłanie haseł mailem

Hasła w mailach, Excelach i notatkach to otwarte drzwi dla każdego, kto przejmie skrzynkę.

❌ Brak weryfikacji przelewów

Zmiana numeru konta tylko mailem, bez drugiego kanału weryfikacji — klasyczny scenariusz straty.

❌ Traktowanie chmury jako backupu

Synchronizacja kopiuje błędy i szyfrowanie ransomware. Brak niezależnego backupu = brak backupu.

❌ Brak zasad AI i testów backupu

AI bez zasad to szybki wyciek danych. Backup bez testu to tylko nadzieja.

Podsumowanie i Następny Krok

Nie chodzi o to, żeby być nie do złamania.

👉 **Chodzi o to, żeby nie być najłatwiejszym celem.**

> „Cyberminimum to nie dokument do szuflady. To zestaw prostych zasad, które mają chronić **pieniądze, dane i spokój właściciela**."

✅ Przejdź checklistę samodzielnie

Dostępy, poczta, backup, przelewy, AI, procedury — zacznij od audytu własnej firmy.

🔍 Zrób audyt krok po kroku

Checklisty i materiały dostępne na **AudytBiura.pl** — skorzystaj po spotkaniu.

👥 Wdróż zasady w zespole

Safe Word, MFA, lista dostępów — trzy decyzje, które możesz podjąć już w poniedziałek.

„Z czym wychodzicie po tej rozmowie? **Jedna rzecz, którą zmienicie po powrocie.**"

Firmy nie padają przez ataki. Padają przez brak kontroli.