SZKOLENIE SECURITY AWARENESS. PRÓBKA RAPORTU PO SZKOLENIU

Szkolenie security awareness. Raport po szkoleniu

Agenda, frekwencja, wyniki testu, wnioski i zapisy SZBI z jednego szkolenia dla całej firmy

Próbka produktu. Dokument pokazuje, co klient otrzymuje po szkoleniu security awareness PushSec: nie tylko slajdy, ale komplet zapisów, których wymaga ISO/IEC 27001 (pkt 7.2, 7.3, A.6.3), audytor klienta i kwestionariusz bezpieczeństwa. Spółka, uczestnicy i wyniki są fikcyjne. Podmiot jest ten sam, co w pozostałych próbkach PushSec.

Metryka szkolenia

Dokument	Raport po szkoleniu. Security awareness dla całego zespołu
Klient	Demo SaaS Sp. z o.o. (podmiot fikcyjny, dalej: Spółka)
Termin i forma	05.09.2026, online na żywo, 2 godziny z przerwą; nagranie dostępne 30 dni dla nieobecnych
Prowadzący	Rafał Dobrosielski, PushSec. Auditor wiodący ISO/IEC 27001 (BSI, IRCA)
Zakres	Moduł bazowy dla wszystkich ról plus blok dla działu deweloperskiego i blok dla kadry zarządzającej
Powiązanie z SZBI	ISO/IEC 27001:2022 pkt 7.2, 7.3, kontrola A.6.3; ustalenie HC-2026-07 z health-checku (program szkoleń bez weryfikacji efektu)
Data wydania	08.09.2026
Klasyfikacja	Materiał demonstracyjny, do publikacji (wersja kliencka: Poufne)

1. Wynik w liczbach

43 z 45	8,4 / 10	41	2
uczestników (96%)	średni wynik testu	zaświadczeń wydanych (próg 7/10)	osoby do powtórki testu

Dwie osoby nieobecne (urlop) obejrzą nagranie i wykonają test do 19.09.2026. Dwie osoby poniżej progu powtórzą test po materiale uzupełniającym. Po domknięciu 45 z 45 pracowników będzie miało aktualny zapis szkolenia za 2026 r.

2. Agenda zrealizowana

Czas	Moduł	Dla kogo	Kluczowy przekaz
10 min	Dlaczego to dotyczy Ciebie	Wszyscy	Bezpieczeństwo w SaaS to warunek sprzedaży do enterprise, nie koszt IT. Trzech klientów Spółki podlega DORA.
25 min	Phishing i inżynieria społeczna	Wszyscy	Cztery cechy podejrzanej wiadomości, zasada jednego kliknięcia, jak zgłosić w 30 sekund. Trzy przykłady na materiale zbudowanym pod Spółkę.
15 min	Hasła, MFA i urządzenia	Wszyscy	Menedżer haseł, MFA na wszystkich narzędziach firmowych, praca hybrydowa, ekran i biurko.

Czas	Moduł	Dla kogo	Kluczowy przekaz
15 min	Dane klientów i klasyfikacja informacji	Wszyscy	Cztery klasy informacji z polityki Spółki, co wolno wysłać mailem, co wymaga narzędzia firmowego. Narzędzia AI a dane klientów.
10 min	Incydent: co robić w pierwszych 15 minutach	Wszyscy	Zgłoś, nie kasuj, nie napraw samodzielnie. Kanał zgłoszeń, kto odbiera, co się dzieje dalej.
20 min	Blok dla deweloperów	Zespół deweloperski (18 os.)	Sekrety w repozytorium, zależności, przegląd kodu pod bezpieczeństwo, środowiska i dane produkcyjne w testach.
15 min	Blok dla kadry zarządzającej	Zarząd i kierownicy (6 os.)	Akceptacja ryzyka, odpowiedzialność za decyzje, co audytor i klient enterprise będą chcieli zobaczyć.
10 min	Test i zamknięcie	Wszyscy	10 pytań, próg 7 poprawnych, wynik natychmiast.

3. Wyniki testu per obszar

Obszar	Poprawne odpowiedzi	Wniosek
Phishing i inżynieria społeczna	91%	Dobrze. Najczęstszy błąd: pilna wiadomość od przełożonego z prośbą o przelew (pytanie 3).
Hasła i MFA	96%	Bardzo dobrze.
Klasyfikacja informacji i narzędzia AI	68%	Najsłabszy obszar. 14 osób uznało, że dane klienta można wkleić do publicznego narzędzia AI, jeśli usunie się nazwę firmy. Rekomendacja w sekcji 5.
Zgłaszanie incydentów	88%	Dobrze. Pięć osób nie znało kanału zgłoszeń; kanał został pokazany na szkoleniu.
Blok dla deweloperów (18 os.)	83%	Dobrze. Do wzmocnienia: sekrety w plikach konfiguracyjnych.

4. Przykładowe pytania testowe

Trzy z dziesięciu pytań. Pytania są budowane na kontekście Spółki, nie z ogólnej bazy, dlatego wyniki mierzą realne zachowania, a nie znajomość definicji.

Pytanie 3. Otrzymujesz wiadomość od Prezesa z prośbą o pilny przelew na nowy rachunek dostawcy. Prezes jest na spotkaniu. Co robisz?

A. Wykonuję przelew, bo prośba jest pilna. B. Odpisuję z prośbą o potwierdzenie. **C. Dzwonię do Prezesa na znany numer lub potwierdzam osobiście, zgłaszam wiadomość jako podejrzaną.** D. Przekazuję do księgowości, niech zdecydują.

Pytanie 6. Chcesz użyć publicznego narzędzia AI do streszczenia umowy z klientem. Usuwasz nazwę klienta. Czy możesz wkleić treść?

A. Tak, po usunięciu nazwy dane są anonimowe. **B. Nie. Treść umowy to informacja klasy Poufne; dozwolone jest tylko narzędzie firmowe wskazane w polityce.** C. Tak, jeśli to wersja płatna narzędzia. D. Tak, jeśli klient nie jest z sektora finansowego.

Pytanie 9. Kliknąłeś link i wpisałeś hasło na stronie, która okazała się fałszywa. Minęło 5 minut. Co robisz najpierw?

A. Zmieniam hasło i nikomu nie mówię, bo już zmienione. **B. Zgłaszam natychmiast kanałem zgłoszeń, potem zmieniam hasło zgodnie z instrukcją zespołu IT.** C. Czekam, czy coś się stanie. D. Wylogowuję się ze wszystkich urządzeń i uznaję sprawę za zamkniętą.

5. Wnioski i rekomendacje

Nr	Rekomendacja	Właściciel	Termin
1	Wydać krótką instrukcję o narzędziach AI (jedna strona: co wolno, czego nie wolno, które narzędzie jest firmowe) i rozesłać z odsyłaczem do polityki klasyfikacji	Pełnomocnik ds. SZBI	14 dni
2	Włączyć pytanie o narzędzia AI do szkolenia wstępnego dla nowych osób	Dział HR	30 dni
3	Przypiąć kanał zgłaszania incydentów w narzędziu komunikacji zespołu i na stronie startowej intranetu	Kierownik IT	7 dni
4	Zaplanować symulację phishingu za 3 miesiące jako weryfikację efektu szkolenia (opcja rozszerzona)	Pełnomocnik ds. SZBI	12.2026
5	Ustalić roczny plan szkoleń: szkolenie wstępne przy zatrudnieniu, roczne dla wszystkich we wrześniu, blok dla deweloperów co pół roku	Pełnomocnik ds. SZBI	30 dni

6. Zapisy SZBI przekazane klientowi

Zapis	Zawartość	Gdzie w SZBI
Lista obecności z podpisami elektronicznymi	45 osób, status: obecny / nieobecny / nagranie	Rejestr szkoleń, A.6.3
Wyniki testu per osoba	Wynik, data, status zaświadczenia	Rejestr szkoleń, dowód kompetencji pkt 7.2
Zaświadczenia imienne (PDF)	41 sztuk, wzór poniżej	Akta pracownicze, do okazania audytorowi i klientowi
Materiały szkoleniowe	Prezentacja, nagranie, instrukcja AI	Repozytorium SZBI, katalog Szkolenia
Niniejszy raport	Wnioski, rekomendacje, plan roczny	Dane wejściowe do przeglądu zarządzania pkt 9.3

ZAŚWIADCZENIE

Jan Przykładowy

ukończył szkolenie **Security awareness dla zespołu Demo SaaS Sp. z o.o.** w dniu 05.09.2026 (2 godziny) i zaliczył test sprawdzający z wynikiem 9/10.
Zakres: rozpoznawanie phishingu i inżynierii społecznej, hasła i MFA, klasyfikacja informacji i narzędzia AI, zgłaszanie incydentów.
Prowadzący: Rafał Dobrosielski, auditor wiodący ISO/IEC 27001 (BSI, IRCA), PushSec. Nr zaświadczenia: PS-SA-2026-0912.

7. Zastrzeżenia

- Wyniki testu mierzą wiedzę i deklarowane zachowania w dniu szkolenia. Weryfikację zachowań realnych daje dopiero symulacja phishingu.
- Szkolenie nie zastępuje szkoleń stanowiskowych ani szkoleń wymaganych odrębnymi przepisami (np. RODO dla osób upoważnionych, jeśli klient prowadzi je osobno).
- Dane uczestników są przetwarzane wyłącznie na potrzeby wydania zaświadczeń i przekazywane klientowi; PushSec nie przechowuje ich po zamknięciu zlecenia poza kopią zaświadczeń.

Szkolenie security awareness. 2 900 zł netto za całą firmę, stała cena

Jedna cena niezależnie od liczby uczestników: 2 godziny na żywo, materiał zbudowany pod firmę, test, zaświadczenia, raport po szkoleniu z zapisami SZBI, nagranie na 30 dni. Warianty: AI awareness (AI Act) 2 900 zł, warsztat analizy ryzyka ISO 27005/31000 3 900 zł.

Zamówienie: pushsec.pl/sklep · info@pushsec.pl · (+48) 780 519 553

Dokument demonstracyjny PushSec. Dane spółki, ustalenia i dowody są fikcyjne. Układ, klasyfikacja i poziom szczegółowości odpowiadają dokumentowi dostarczanemu klientom. Wersja dostarczana klientowi ma klasyfikację Poufne.