

Skuteczne szkolenia z ochrony danych osobowych

Posted on 2026-10-01

Kontrole UODO i analiza naruszeń pokazują, że wiele szkoleń nie buduje świadomości adekwatnej do ryzyka -zwłaszcza błędów pracowników, takich jak niewłaściwe udostępnienie danych czy podatność na phishing.

Często trudno nie odnieść wrażenia, że stosowane jest podejście „*przeszkoliłem pracownika i mam spokój*”. W praktyce edukacja ogranicza się do krótkiego, często powierzchownego szkolenia po zatrudnieniu, zakończonego podpisaniem oświadczenia o zapoznaniu się z procedurami. Przez kolejne lata pracownik ten nie bierze już udziału w żadnych działaniach podnoszących świadomość.

Nie wystarczy przeszkolić pracownika przy

zatrudnianiu

Z perspektywy międzynarodowych standardów to podejście błędne i nie daje realnej ochrony. Systemy bezpieczeństwa informacji oraz ochrony danych osobowych to mechanizmy żywe i stale ewoluujące. Zmieniają się przepisy prawa, technologia, procedury wewnętrzne, a przede wszystkim metody działania samych cyberprzestępców. Jednorazowe szkolenie nie wykształci, a tym bardziej nie utrzyma pożądanych nawyków. Świadomości nie da się budować incydentalnie – standardy wymagają ciągłego, cyklicznego szkolenia.

Rzetelne szkolenie wstępne to oczywiście obowiązkowy punkt wdrażania każdego nowego pracownika lub osoby zmieniającej stanowisko, uświadamiający podstawowe zasady. Na tym jednak nie koniec, ponieważ wszyscy pracownicy muszą regularnie otrzymywać aktualizacje polityk i procedur w zaplanowanych odstępach czasu. Organizacja musi też reagować na bieżąco: uruchamiać dodatkowe szkolenia po zmianach prawa, wdrożeniach nowych technologii oraz po incydentach.

Materiał na szkoleniu musi być dostosowany do obowiązków i roli w organizacji

Kolejnym błędem organizacyjnym jest oferowanie identycznych treści szkoleniowych wszystkim pracownikom; niezależnie od ich roli. Kierowanie jednakowego materiału do

całego personelu – niezależnie od tego, czy szkolimy administratora IT, księgową, czy pracownika recepcji – mija się z celem. Każda z tych osób wykonuje inne zadania, co przekłada się na różne poziomy i rodzaje ryzyka. Zgodnie z międzynarodowymi standardami, program uświadamiania musi być dostosowany do konkretnych ról, zakresu odpowiedzialności i umiejętności uczestników, w szczególności:

- Personel techniczny i IT: wymaga dedykowanych planów szkoleniowych obejmujących specjalistyczne umiejętności, takie jak bezpieczna konfiguracja systemów, bezpieczne zarządzanie sieciami czy zasady bezpiecznego kodowania
- Pracownicy biurowi i administracja (np. księgowość, kadry): w ich przypadku szkolenia powinny skupiać się na bezpiecznym obchodzeniu się z dokumentacją zawierającą dane osobowe, a także na poprawnym stosowaniu kontroli dostępu i bezpiecznym korzystaniu z poczty elektronicznej oraz aplikacji biznesowych
- Sekretariat i pierwsza linia kontaktu: to osoby, które wymagają szczególnego wyczulenia na rygorystyczną weryfikację tożsamości interesantów.

Skuteczny program szkoleniowy nie może być też czysto teoretyczną recytacją zapisów prawnych i firmowych regulaminów. Musi uwzględniać te zagrożenia, które najczęściej materializują się w codziennej pracy na danym stanowisku. Praktyka pokazuje, że plagą są ataki socjotechniczne (w tym phishing) polegające na manipulowaniu ludźmi w celu zmuszenia ich do określonych działań lub wyjawienia poufnych informacji.

Szkolenia muszą uczyć, jak rozpoznawać podejrzaną wiadomość e-mail, zainfekowane pliki czy fałszywe strony internetowe. Pracownicy muszą wiedzieć, jak właściwie reagować na takie sytuacje i do kogo zgłaszać incydenty. Ważne jest nie tylko pokazanie „*jak*” postępować, ale też wyjaśnienie „*dlaczego*” zachowanie bezpieczeństwa jest kluczowe. Szkolenia powinny uwzględniać wnioski z rzeczywiście zaistniałych incydentów, które pokazują realne scenariusze zagrożeń.

Trzeba sprawdzać, czego pracownicy nauczyli się na szkoleniu

Na koniec pozostaje kwestia weryfikacji. Szkolenie to w systemie zarządzania środkami organizacyjny mający zapewnić bezpieczeństwo. Podobnie jak każde inne zabezpieczenie, musi ono podlegać regularnej ocenie skuteczności. Samo przeprowadzenie wykładu i zebranie podpisów na liście obecności to żaden dowód na to, że pracownicy przyswoili niezbędne kompetencje. Międzynarodowe standardy określają jasne mechanizmy weryfikacji:

- Ewaluacja wiedzy: bezpośrednio po zakończeniu sesji, a także wyrywkowo w okresach między szkoleniami, należy weryfikować poziom wiedzy i zrozumienia treści – np. na przykład za pomocą testów
- Kontrolowane symulacje ataków: niezwykle skuteczną metodą oceny postaw w praktyce są kontrolowane akcje phishingowe oraz ćwiczenia reagowania na incydenty. Pozwalają one w bezpiecznych warunkach sprawdzić, czy pracownicy faktycznie potrafią wykryć próbę ataku i czy stosują procedury zgłaszania
- Pętla zwrotna: wyniki testów oraz symulacji nie mogą trafiać do szuflady. Powinny służyć do identyfikacji luk w wiedzy zespołu i stawać się podstawą do celowanej aktualizacji kolejnych edycji programu szkoleniowego

Podnoszenie świadomości z zakresu ochrony danych osobowych to długofalowy proces budowania kultury bezpieczeństwa, a nie jednorazowy obowiązek do odznaczenia w kadrach. Tylko szkolenia cykliczne, elastycznie dopasowane do ról i ukierunkowane na realne zagrożenia, które poddaje się regularnym testom skuteczności mogą zapewnić

Skuteczne szkolenia z ochrony danych osobowych

organizacji skuteczną ochronę.