To jubileuszowe wydanie materiału przygotowanego przez zespół LexDigital z okazji **20-lecia Europejskiego Dnia Ochrony Danych Osobowych**, obchodzonego corocznie 28 stycznia.

Rok 2026 przynosi kolejne wyzwania w obszarze ochrony danych, prywatności i cyberbezpieczeństwa. Sztuczna inteligencja, praca zdalna, chmura oraz rosnąca liczba ataków opartych na socjotechnice sprawiają, że bezpieczeństwo informacji w coraz większym stopniu zależy od codziennych decyzji pracowników.

Poniżej przedstawiamy najważniejsze trendy i zagrożenia na 2026 rok, wraz z praktycznymi wskazówkami, jak chronić dane – swoje i organizacji.

Nowe oblicza zagrożeń. AI na usługach cyberprzestępców

Wraz z rozwojem technologii AI zmienił się również obszar cyberprzestępczości **(deepfake, a także podszywanie się pod ludzi)**. Ataki phishingowe stały się trudniejsze do rozpoznania. Dzięki wykorzystaniu sztucznej inteligencji wiadomości, rozmowy telefoniczne (vishing – voice phishing) czy spotkania online mogą wyglądać i brzmieć bardzo wiarygodnie, w rzeczywistości będąc pułapkami przygotowanymi przez przestępców.

Na co zwrócić uwagę:

Pamiętaj, jaki kanał komunikacji obowiązuje w Twojej organizacji. Coraz częściej spotyka się podszywanie pod przełożonych lub współpracowników (również podczas rozmów wideo)

Nietypowe lub pilne polecenia (np. przelew, udostępnienie danych) powinny być zawsze potwierdzone innym kanałem komunikacji

Pośpiech i presja czasu to najczęstsze narzędzia atakujących

Pamiętaj:
ograniczone zaufanie i chwila weryfikacji mogą zapobiec poważnemu incydentowi.

Shadow AI – niekontrolowane użycie narzędzi AI

Narzędzia oparte na sztucznej inteligencji są coraz powszechniej wykorzystywane w codziennej pracy – do pisania maili, tłumaczeń czy streszczeń dokumentów. Problem pojawia się wtedy, gdy są używane **bez wiedzy organizacji**.

Dlaczego to ryzykowne?

Dane wprowadzane do publicznych narzędzi AI mogą zostać zapisane lub wykorzystane dalej

Nawet pozornie „neutralne" informacje mogą ujawniać dane poufne

Brak kontroli oznacza brak odpowiedzialności za dane

Pamiętaj:
korzystaj wyłącznie z narzędzi AI dopuszczonych do użytku służbowego.

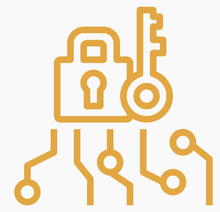
Tożsamość cyfrowa – nowe „klucze" do organizacji

Cyberataki coraz rzadziej polegają na łamaniu systemów, a coraz częściej na przejmowaniu kont użytkowników.

Co to oznacza dla pracownika:

Login i hasło to dziś dostęp do wielu systemów jednocześnie

Przejęcie jednego konta może umożliwić dostęp do danych całej organizacji



Uwierzytelnianie wieloskładnikowe (MFA) znacząco ogranicza ryzyko

Pamiętaj:
Twoje konto służbowe to realna wartość – chroń je jak klucz do biura!

Incydent to nie wstyd – znaczenie szybkiego zgłaszania

Żadna organizacja nie jest całkowicie odporna na incydenty.
O skutkach decyduje czas reakcji, a nie sam fakt zdarzenia.

Dobre praktyki:

Zgłaszaj każdą podejrzaną sytuację

Nie obawiaj się konsekwencji – zgłoszenie to element odpowiedzialności

Szybka informacja pozwala ograniczyć skutki incydentu

Pamiętaj:
brak reakcji może być większym zagrożeniem niż sam błąd.

Jak możesz chronić firmę i siebie?

korzystaj z MFA i silnych haseł

zachowuj ostrożność przy mailach, linkach i załącznikach

nie udostępniaj danych w niezatwierdzonych narzędziach AI

sprawdzaj uprawnienia do dokumentów w chmurze

reaguj i zgłaszaj wątpliwości

Pamiętaj:
bezpieczeństwo danych to nie jednorazowe działanie, lecz codzienne decyzje.
Każdy pracownik ma realny wpływ na ochronę informacji – swoich, klientów i całej organizacji.