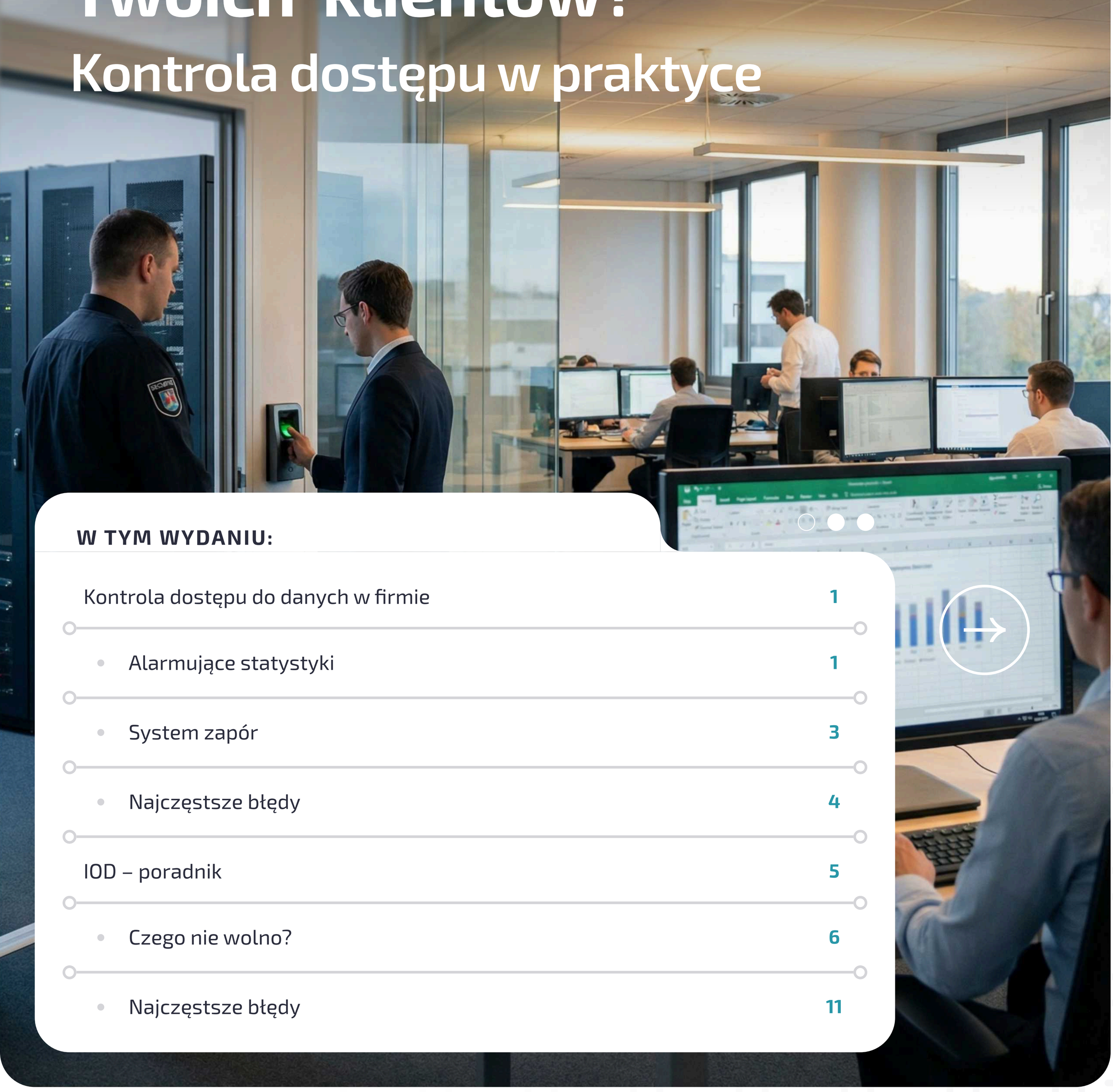
Kto widzi dane Twoich klientów?

Kontrola dostępu w praktyce



W TYM WYDANIU:

LexDigital

lexdigital.pl

Dariusz Janiak
Information Security & Data Protection Expert

Kontrola dostępu do danych w firmie

Czy wiesz, kto ma dane klientów?

Osób, którym zależy na zapewnieniu ograniczenia dostępu do zasobów jest w zasadzie garstka. Natomiast osób zainteresowanych dostępem do nich mogą być tysiące, setki tysięcy, a czasami miliony. Sprawdź nasz przewodnik i dowiedz się, jak zabezpieczyć swoją organizację!

Skąd wiadomo, że system kontroli dostępu funkcjonuje wadliwie? Przykładowo, jeśli w Twojej organizacji:

użytkownik biurowy w pierwszym dniu pracy dostaje szerokie, nadmierne uprawnienia administratorskie do zasobów

pracownicy logują się na konta nieobecnych w pracy pracowników

uprawnienia są nadawane bez możliwości późniejszej weryfikacji, kto wydał na nie zgodę

po odejściu z pracy pracownika jego konta do zasobów pozostają aktywne

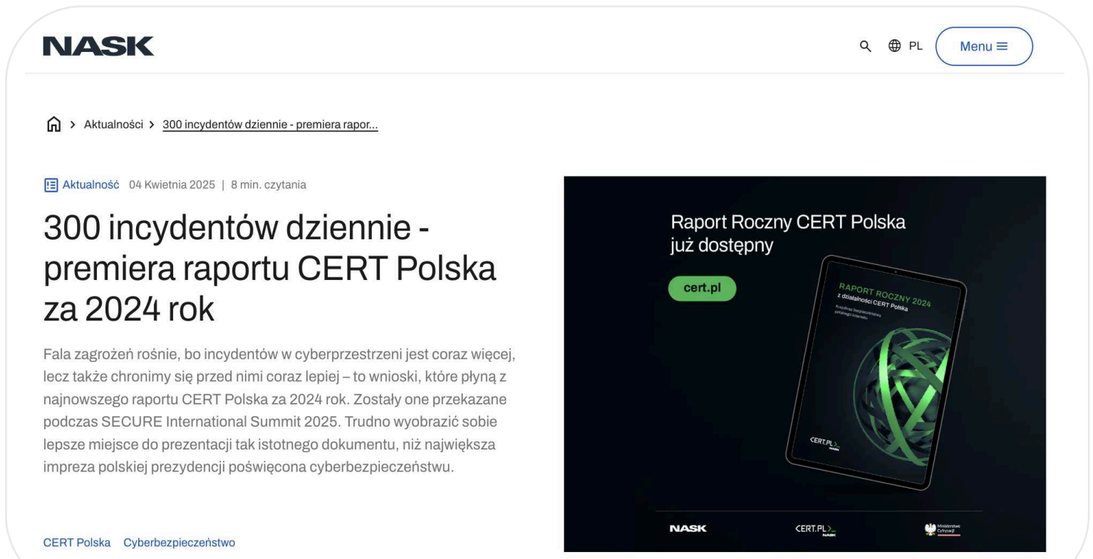
pracownicy zapisują hasła, bo nie mogą ich zapamiętać

lub mają miejsce podobne sytuacje, to system kontroli dostępu prawdopodobnie nie działa prawidłowo.

Alarmujące statystyki

Według danych ESET w pierwszej połowie 2025 roku Polska znalazła się na pierwszym miejscu na świecie pod względem liczby wykrytych ataków ransomware, wyprzedzając w tym zakresie nawet Stany Zjednoczone. Zespół reagowania na incydenty bezpieczeństwa komputerowego CERT Polska działający w strukturze NASK w 2024 roku odnotował rekordowy wzrost aktywności cyberprzestępców.

Liczba zgłoszeń wyniosła 600 000, co stanowi wzrost rok do roku średnio o około 62%. Od stycznia do sierpnia doszło do 946 incydentów bezpieczeństwa komputerowego w ochronie zdrowia. Obok takich incydentów jak wprowadzenie do systemu złośliwego oprogramowania czy wyłudzenie danych, dochodziło także właśnie do nieautoryzowanego dostępu do systemów.



Problem dotyczy także samorządów, które według NIK mają poważne problemy z cyberbezpieczeństwem w zakresie m.in identyfikacji zbiorów danych wymagających ochrony, zabezpieczenia fizycznego serwerowni czy złożoności haseł.

Skuteczna kontrola dostępu to najważniejsze narzędzie, które pozwoli zabezpieczyć się przed hakerami!

Czym jest kontrola dostępu?

W najprostszym ujęciu kontrola dostępu to zespół środków organizacyjnych i technicznych mających na celu ograniczenie kto, kiedy i w jakim zakresie może przetwarzać określone informacje i mieć do nich dostęp.

Podstawowe pojęcia z tego zakresu to przede wszystkim:

- **identyfikacja**, czyli posiadanie przez osobę, która chce mieć dostęp informacji identyfikujących (np. login)
- **uwierzytelnienie**, czyli proces potwierdzenia tożsamości
- **autoryzacja**, czyli proces weryfikacji, czy osoba logująca się może mieć dostęp do żądanego zasobu.

Jak w takim razie zbudować system kontroli dostępu? Szczegółowych instrukcji dostarcza norma ISO 27001. Według kontrolki 5.15 należy ustanowić i wdrożyć system dostępu w oparciu o zasady dostępu fizycznego i logicznego i powiązanych z tym aktywów. Wymaga to określenia, co chcemy i musimy chronić, a to oczywiście wymaga rozpoznania aktywów organizacji.

Oznacza to określenie:

- z jakiego powodu chcemy chronić dane informacje
- jak zabezpieczenia mają funkcjonować w odniesieniu do konkretnych aktywów
- jak chcemy chronić te aktywa.

System zapór

Kontrola dostępu to nic innego jak system równorzędnych zapór, występujących na różnych poziomach i w różnych sferach organizacji:

Zasada minimalnych uprawnień

według której dostęp przyznaje się tylko w sytuacji, kiedy dane uprawnienia są faktycznie niezbędne

Rozdział krytycznych funkcji

Przykładowo: osoba, która zarządza kontami użytkowników nie powinna zatwierdzać dostępu ani używać kont do operacji produkcyjnych

Szkolenia pracowników

zwłaszcza w zakresie ochrony przed socjotechniką

Automatyzacja onboardingu

czyli powiązanie zdarzeń kadrowych ze zdarzeniami operacyjnymi (przyznanie lub odcięcie dostępu od zasobu w odpowiednim momencie)

Jeden centralny system tożsamości

czyli autorytatywne źródło informacji o użytkowniku, które ogranicza błędy ludzkie i rozproszenie kont

Uwierzytelnianie wieloskładnikowe

dla wszystkich zasobów wrażliwych

Zarządzanie dostępem uprzywilejowanym

System z dostępem „just in time" ograniczonym do czasu realizacji zadania i rejestracją sesji administratorów

Wymuszona polityka kluczy kryptograficznych

chociażby poprzez szyfrowanie, a następnie zastosowanie kontroli dostępu do kluczy deszyfrujących

Należy łączyć elementy obowiązkowej kontroli dostępu (zautomatyzowanej) z kontrolą uznaniową, w zależności od tego, z jakimi zasobami mamy do czynienia. Można stosować takie macierze kontroli dostępu jak RBAC (Role-Based Access Control) czy ABAC (Attribute-Based Access Control), czyli organizować kontrolę dostępu wokół ról przypisanych do zasobów, a nie decyzji indywidualnych administratora. Wcześniej określone role zapobiegają nieuprawnionej eskalacji uprawnień.

Ważna jest też tak zwana **głęboka ochrona fizyczna**, czyli zestawienie wielu wzajemnie uzupełniających się barier w ten sposób, żeby zasoby krytyczne były lokowane w najgłębszej warstwie.

Najczęstsze błędy

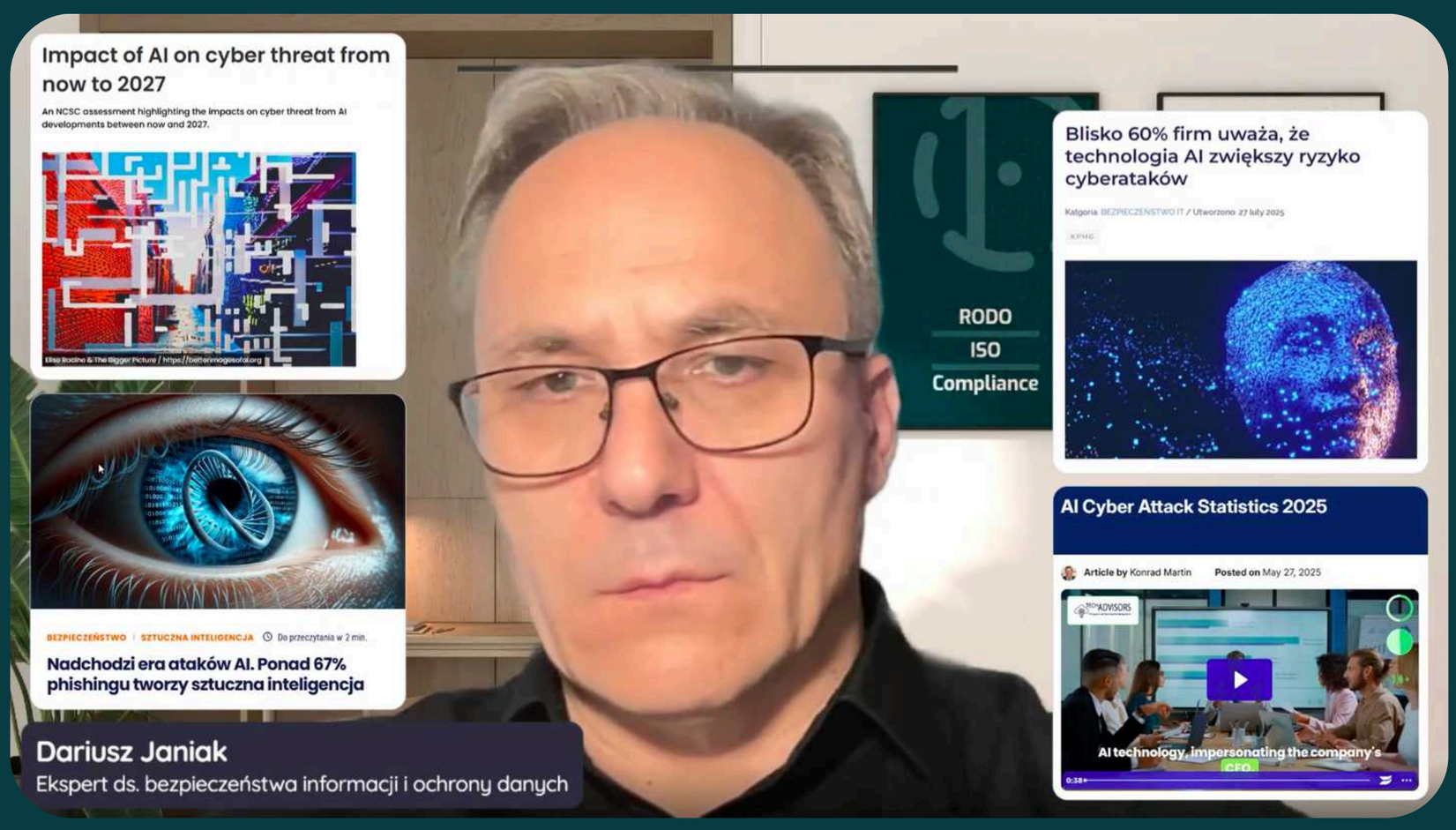
- **Reaktywne podejście**, czyli implementacja rozwiązań bezpieczeństwa dopiero po wystąpieniu incydentu. Z oczywistych względów lepiej jest stosować systemowe podejście jak najwcześniej i zapobiegać sytuacjom kryzysowym, bo każda z nich może nieść ogromne ryzyko dla organizacji.
- **Brak oparcia o klasyfikację informacji**, czyli traktowanie wszystkich zasobów jako wrażliwych czy krytycznych
- **Ochrona obwodowa** – założenie, że wszystko, co wewnątrz sieci jest zaufane
- **Oparcie wyłącznie na technologii** bez uwzględnienia czynnika ludzkiego. Zmuszanie do używania zbyt wielu haseł i skomplikowanych tokenów może spowodować, że zniecierpliwieni ludzie będą omijać zabezpieczenia, aby ułatwić sobie życie.
- **Brak interakcji z działem HR** tworzy ryzyko, że zasoby, które powinny być już zablokowane, są dalej są aktywne dla danego użytkownika.
- **Brak automatyzacji** - opieranie całego systemu o działania ręczne sprawia, że czasami przeglądy uprawnień odbywają się tylko na papierze.
- **Brak płynnego zarządzania tożsamością** i zautomatyzowanych procesów zarządzania kontami użytkowników.
- **Brak logowania zdarzeń**, na przykład brak wymogu logowania wszystkich prób dostępu, przez co nie ma możliwości odtworzenia zdarzeń.

Planując zapewnienie kontroli dostępu należy pamiętać, że jest to proces złożony, który powinien być realizowany w ujęciu kompleksowym. Prawidłowe wdrożenie modelu zarządzania kontrolą dostępu musi łączyć ze sobą aspekty systemowe, organizacyjne, zarządzania personelem, technologiczne, prawne i biznesowe. Dobrze zaprojektowana i wdrożona kontrola dostępu stanowi najważniejszą barierę ochronną zasobów organizacji.

Sprawdź cykl

„Akademia LexDigital"

na YouTube i LinkedIn, omawiający praktyczne aspekty SZBI wg ISO 27001 i korzyści z wdrożenia.



Natalia Dzieciuchowicz
Data Protection Expert

Inspektor Ochrony Danych - poradnik

Kim jest, czym się zajmuje i jak wspiera biznes?

W gąszczu przepisów o ochronie danych łatwo się zgubić, a błędy mogą kosztować firmę utratę reputacji i wysokie kary. Dlatego coraz więcej przedsiębiorców powołuje Inspektora Ochrony Danych (IOD) – specjalistę, dbającego o zgodność działań z RODO i bezpieczeństwo informacji. Sprawdź, kim jest IOD, jakie ma obowiązki, czego nie powinien robić i jak jego wsparcie może pomóc Twojej firmie działać zgodnie z prawem i minimalizować ryzyka.

Kim jest IOD?

Zgodnie z motywem 97 RODO, **Inspektor Ochrony Danych to osoba dysponująca wiedzą fachową na temat prawa i praktyk w zakresie ochrony danych osobowych.** Jego wiedza powinna być dopasowana do rodzaju i skali operacji przetwarzania prowadzonych przez organizację.

IOD to niezależny doradca i strażnik zgodności z RODO. Odpowiada za monitorowanie, doradztwo i komunikację z organem nadzorczym. Może być pracownikiem firmy lub ekspertem zewnętrznym powołanym na podstawie umowy.

Podstawowe obowiązki inspektora wynikają z **art. 39 RODO** i obejmują m.in.:

- Informowanie administratora i/lub podmiotu przetwarzającego o obowiązkach wynikających z RODO oraz innych przepisów Unii lub państw członkowskich o ochronie danych.
- Monitorowanie przestrzegania RODO, innych właściwych przepisów Unii lub państw członkowskich o ochronie danych osobowych.
- Monitorowanie przestrzegania polityk ochrony danych osobowych.
- Prowadzenie działań zwiększających świadomość personelu w zakresie obowiązków wynikających z RODO i przyjętych polityk administratora (działania zwiększające świadomość personelu administratora/podmiotu przetwarzającego są niezwykle istotnym elementem całego systemu ochrony danych osobowych. Wg statystyk pracownik stanowi najpoważniejsze źródło naruszeń ochrony danych osobowych. Szkolenia personelu

uczestniczącego w procesach związanych z operacjami przetwarzania danych są zatem kluczowe). O obowiązkach spoczywających na pracownikach w związku z przetwarzaniem danych nie wystarczy poinformować raz – to proces ciągły i tylko taki zapewni właściwy poziom świadomości.

udzielanie zaleceń co do oceny skutków dla ochrony danych – monitorowanie wykonania i ocena prawidłowości przeprowadzonej oceny skutków dla ochrony danych (Inspektor, na podstawie oceny ryzyka związanego z przetwarzaniem danych w określonym procesie doradza, czy należy przeprowadzić ocenę skutków dla ochrony danych).

IOD jest też zaangażowany w bieżące procesy firmy – opiniuje umowy powierzenia przetwarzania danych, reaguje na naruszenia i wspiera administratora w komunikacji z UODO.

Pozostałe obowiązki IOD

współpraca z organem nadzorczym oraz pełnienie funkcji punktu kontaktowego dla Prezesa UODO w kwestiach związanych z przetwarzaniem danych (np. w postępowaniach administracyjnych prowadzonych przez Urząd). Zgodnie z artykułem 39 (1)(d) i (e) RODO, "IOD powinien „współpracować z organem nadzorczym” i „pełnić funkcję punktu kontaktowego dla organu nadzorczego w kwestiach związanych z przetwarzaniem, w tym z uprzednimi konsultacjami, o których mowa w art. 36, oraz w stosownych przypadkach prowadzić konsultacje we wszelkich innych sprawach.”

Pełnienie funkcji punktu kontaktowego dla podmiotów danych (osoby, których dane dotyczą, mogą kontaktować się z Inspektorem Ochrony Danych we wszystkich sprawach związanych z przetwarzaniem ich danych osobowych oraz wykonywaniem praw przysługujących im na mocy RODO – art. 38 ust. 4 RODO),

Uczestniczenie w konsultacjach we wszelkich sprawach w zakresie ochrony danych osobowych (w zakresie wykonywania swoich zadań Inspektor ochrony danych bierze również udział w procesie realizacji praw osób, reaguje na skargi osób, których dane dotyczą).

Czego Inspektor Ochrony Danych nie powinien robić

RODO (art. 38) jasno wskazuje, że IOD musi działać niezależnie. Dlatego istnieje szereg czynności, które nie mogą być mu narzucane lub mogą prowadzić do konfliktu interesów.

Inspektor nie powinien:

1. wykonywać zadań, które mogą wpływać na jego bezstronność,
2. reprezentować firmy przed sądem w sprawach dotyczących ochrony danych,
3. podejmować decyzji w imieniu administratora (IOD doradza, ale nie decyduje),
4. być odwoływany w dowolnym momencie bez uzasadnienia,
5. wykonywać obowiązków bez zapewnienia mu odpowiednich zasobów (czasu, budżetu, narzędzi, dostępu do informacji).

IOD nie może być traktowany jako „parasol ochronny” dla administratora – jego zadaniem jest wskazywać ryzyka i rekomendować rozwiązania, nie ponosi jednak odpowiedzialności za decyzje zarządu.

Urząd podkreśla, że IOD powinni być włączani we wszystkie sprawy dotyczące ochrony danych osobowych, w tym w sprawy dotyczące naruszeń ochrony danych osobowych. O zaistnieniu naruszenia IOD powinien być niezwłocznie informowany, aby umożliwić mu monitorowanie procesu jego obsługi od najwcześniejszego etapu.

Przykłady działania IOD w sprawie naruszeń:

- pomoc w zapobieganiu naruszeniom, np. poprzez promowanie w organizacji wiedzy o ochronie danych osobowych, organizowanie szkoleń oraz formułowanie zaleceń dotyczących bezpieczeństwa przetwarzania danych;
- udzielanie wskazówek dotyczących odpowiedniego reagowania na naruszenia ochrony danych osobowych, w tym zaradzania im , zgłaszania ich Prezesowi UODO oraz zawiadamiania osób, których dane dotyczą;
- doradztwo w zakresie dokumentowania naruszeń i zarządzania dokumentacją;
- przekazywanie dodatkowych informacji o naruszeniach organowi nadzorczemu i osobom, których dane dotyczą.

IOD nie mogą jednak wykonywać zadań, za które odpowiadają wyłącznie administratorzy lub podmioty przetwarzające.

IOD nie powinni:

zgłaszać naruszeń ochrony danych osobowych Prezesowi UODO w imieniu administratorów ani podpisywać i wysyłać takich zgłoszeń

zawiadamiać w imieniu administratorów osób, których dane dotyczą, o naruszeniach ochrony danych osobowych

dokumentować naruszeń ochrony danych osobowych w imieniu administratorów (w szczególności, jeśli wiązałoby się to z ustalaniem celów i sposobów przetwarzania danych osobowych albo określaniem działań zaradczych)

podejmować zobowiązań dotyczących bezpieczeństwa przetwarzania w imieniu administratorów lub podmiotów przetwarzających

działać na podstawie pełnomocnictwa w sprawach dotyczących ochrony danych osobowych.

Niewłaściwy podział ról może powodować problemy, dlatego warto pamiętać, że gdy IOD wykonują obowiązki spoczywające na administratorach lub podmiotach przetwarzających mogą tracić obiektywizm i popadać w konflikt interesów. Z kolei pełnomocnictwo wymaga ścisłego wykonywania poleceń, co może naruszać niezależność IOD.

Rola Inspektora ochrony danych została doprecyzowana w wydanym przez UODO w lutym 2025 roku Poradniku dotyczącym naruszeń ochrony danych osobowych.

Sprawdź nasze obszerne omówienie dotyczące niezależności IOD.

Naruszenie zasad dotyczących statusu IOD może skutkować sankcjami administracyjnymi ze strony Prezesa UODO, w tym karami pieniężnymi.

Kwalifikacje i kompetencje IOD

Skuteczny Inspektor Ochrony Danych powinien posiadać:

- znajomość krajowych i unijnych przepisów dotyczących ochrony danych osobowych,
- praktyczne doświadczenie w zakresie wdrażania RODO,
- wiedzę o procesach biznesowych i systemach IT wykorzystywanych w firmie,
- znajomość zasad bezpieczeństwa informacji,
- umiejętność komunikacji i prowadzenia szkoleń dla pracowników.

Europejska Rada Ochrony Danych Osobowych wskazuje, że IOD powinien aktywnie wspierać organizację w budowie „kultury ochrony danych” – poprzez doradztwo, audyty i nadzór nad wdrożeniem zasad takich jak privacy by design, czy reagowanie na incydenty.

"Wytyczne Europejskiej Rady Ochrony Danych (EROD) dotyczące inspektorów ochrony danych (IOD)" to podstawowy dokument (pierwotnie opublikowany przez Grupę Roboczą Art. 29, a następnie zatwierdzony przez EROD) szczegółowo interpretujący przepisy RODO (Art. 37-39). Jest on podstawowym źródłem wiedzy o tym, jak organy nadzorcze postrzegają rolę, zadania i pozycję IOD.

Kiedy powołanie IOD jest obowiązkowe?

Zgodnie z art. 37 RODO, powołanie Inspektora Ochrony Danych jest obowiązkowe, gdy:

przetwarzania dokonuje organ lub podmiot publiczny,

główna działalność polega na regularnym i systematycznym monitorowaniu osób na dużą skalę,

główna działalność obejmuje przetwarzanie na dużą skalę danych wrażliwych (np. o zdrowiu, poglądach, karalności).

EROD doprecyzowuje trzy przypadki wymienione w art. 37 RODO:

1 Ustanowienie kontekstu:

- każdy "organ lub podmiot publiczny" musi wyznaczyć IOD
- wyjątkiem są sądy w zakresie sprawowania wymiaru sprawiedliwości
- wytyczne wskazują, że jeden IOD może być wyznaczony dla kilku mniejszych organów publicznych

2 Regularne i systematyczne monitorowanie na "dużą skalę":

- "regularne" oznacza m.in. stałe, ciągłe lub okresowo powtarzające się
- "systematyczne" oznacza m.in. planowe, zorganizowane, prowadzone w ramach strategii
- "duża skala" - EROD zaleca brać pod uwagę:
  - liczbę osób, których dane dotyczą
  - ilość danych przetwarzanych i ich zakres
  - czas trwania i zasięg geograficzny przetwarzania.

Przykłady podane przez EROD: profilowanie klientów w banku, przetwarzanie danych pacjentów przez szpital, monitorowanie lokalizacji przez aplikację, śledzenie zachowań w internecie (targetowanie behawioralne).

3 Przetwarzanie na "dużą skalę" danych wrażliwych (Art. 9) lub o wyrokach (Art. 10):

- dotyczy to sytuacji, gdy główną działalnością firmy jest przetwarzanie tych danych.
- EROD podkreśla, że przetwarzanie danych pracowników (nawet szczególnych kategorii, np. zwolnień lekarskich) nie jest uznawane za "główną działalność" w tym kontekście.

Przykład: Przetwarzanie danych genetycznych przez laboratorium, danych o zdrowiu przez firmę ubezpieczeniową lub danych o poglądach politycznych przez partię.

W pozostałych przypadkach wyznaczenie inspektora nie jest obowiązkowe, ale często stanowi **dobrą praktykę i realne zabezpieczenie interesów** – zwłaszcza w branżach, gdzie przetwarzane są dane klientów, pracowników czy partnerów biznesowych.

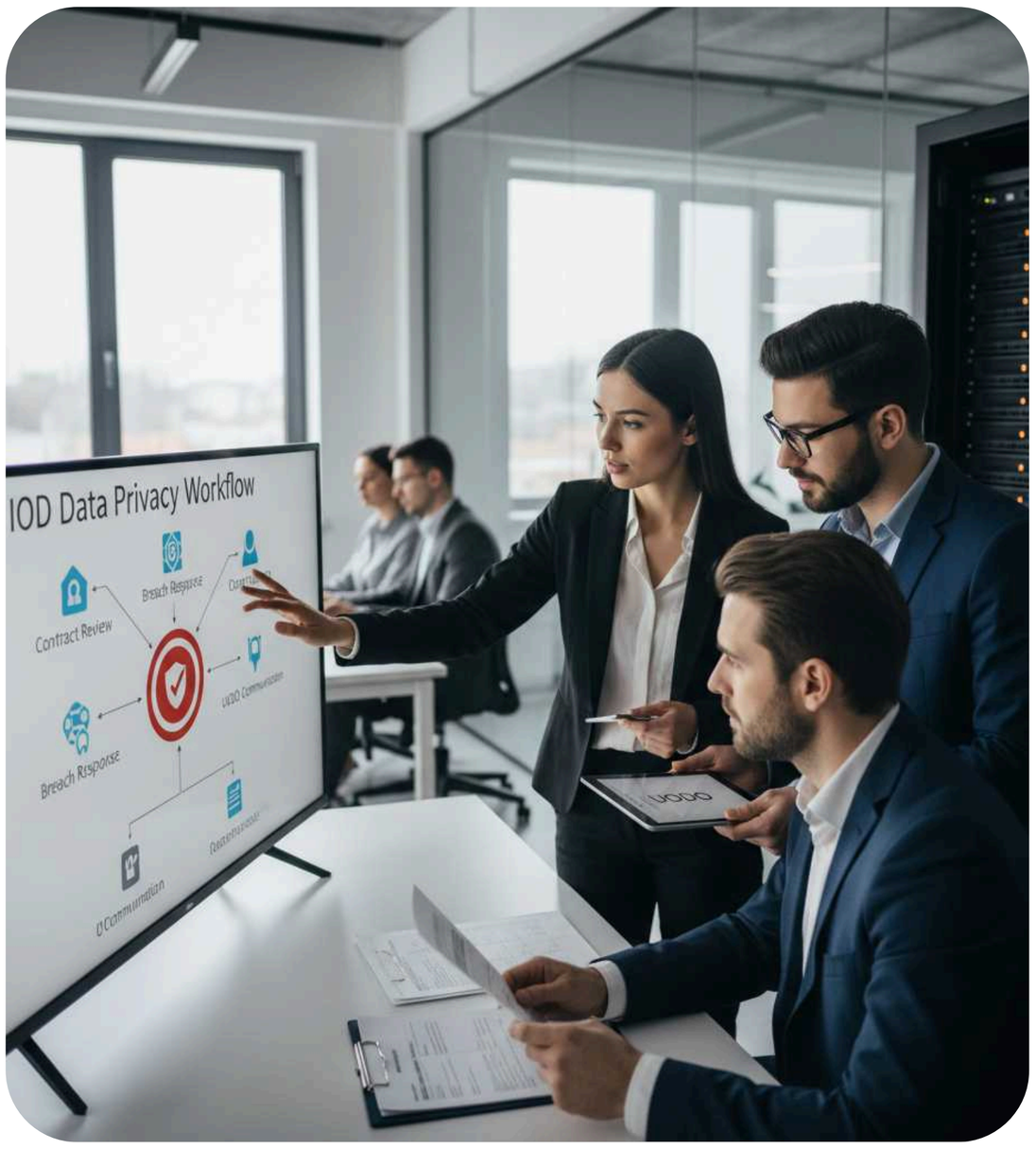
Administrator danych, który zdecyduje się na powołanie IOD ma obowiązek zgłosić jego dane do Urzędu Ochrony Danych Osobowych (art. 10 ustawy z 10 maja 2018 r.).

Pozycja IOD w organizacji

Art. 38 RODO to kluczowy element wytycznych, mający zapewnić IOD niezależność. Według niego:

- IOD musi być "właściwie i niezwłocznie włączany" we wszystkie sprawy dotyczące ochrony danych. Nie może być informowany post-factum.
- IOD podlega bezpośrednio "najwyższemu kierownictwu" (np. zarządowi, prezesowi). Nie może podlegać np. kierownikowi IT czy szefowi działu prawnego.
- Administrator musi zapewnić IOD zasoby (czas, finanse, szkolenia, personel) niezbędne do wypełniania zadań.
- IOD jest niezależny. Nie można mu wydawać instrukcji, jak ma wykonywać swoje obowiązki.
- IOD nie może być odwołany ani ukarany za wypełnianie swoich zadań (np. za zgłoszenie problemu kierownictwu lub organowi nadzorczemu).

Wytyczne podkreślają, że IOD pełni funkcję doradczo-monitorującą, a nie wykonawczą (Zadania IOD Art. 39 RODO).



URZĄD OCHRONY DANYCH OSOBOWYCH

Konflikt interesów

EROD bardzo surowo podchodzi do kwestii konfliktu interesów. Z tego powodu inspektor ochrony danych osobowych nie może zajmować w organizacji stanowiska, na którym określa "cele i sposoby" przetwarzania danych.

EROD bardzo surowo podchodzi do kwestii konfliktu interesów. Z tego powodu inspektor ochrony danych osobowych nie może zajmować w organizacji stanowiska, na którym określa "cele i sposoby" przetwarzania danych.

Wg EROD IOD nie powinien piastować funkcji takich jak:

- prezes, dyrektor generalny, członek zarządu,
- dyrektor finansowy (CFO),
- dyrektor operacyjny (COO),
- dyrektor ds. marketingu,
- kierownik działu HR,
- kierownik działu IT.

Zasada konfliktu interesów dotyczy również firm zewnętrznych. Np. firma, która świadczy usługi IT (i decyduje o sposobach zabezpieczeń), nie powinna być jednocześnie IOD.

Najczęstsze błędy wykazywane przez UODO

UODO w ramach kontroli działalności IOD zwraca uwagę na powtarzające się błędy, takie jak:

- brak publikacji danych kontaktowych inspektora
- nieaktualne informacje o IOD na www firmy
- pomijanie inspektora przy decyzjach dotyczących danych,
- konflikty interesów (np. IOD jest jednocześnie szefem IT)
- brak odpowiednich zasobów i czasu na wykonywanie obowiązków
- nieinformowanie UODO o zmianie inspektora

Takie uchybienia mogą zostać uznane za naruszenie RODO i skutkować sankcjami administracyjnymi.

Outsourcing IOD

RODO (art. 37 ust. 6) dopuszcza powierzenie funkcji Inspektora Ochrony Danych podmiotowi zewnętrznemu. To rozwiązanie szczególnie korzystne dla małych i średnich przedsiębiorstw – pozwala zapewnić wysoki poziom kompetencji bez kosztów utrzymania etatu.

Zewnętrzny IOD zapewnia też obiektywność, bieżącą aktualizację wiedzy i pełne wsparcie w kontaktach z UODO.

Dlaczego warto powołać IOD, nawet jeśli nie musisz?

- **zmniejszasz ryzyko kar finansowych,**
- **chronisz reputację i zaufanie klientów,**
- **masz wsparcie w razie incydentu,**
- **możesz skoncentrować się na rozwoju biznesu, a nie na formalnościach.**

Inspektor Ochrony Danych to nie tylko wymóg prawny, ale strategiczny partner w zapewnianiu bezpieczeństwa informacji w firmie. Jego wiedza i niezależność pomagają budować zaufanie, unikać błędów i działać zgodnie z zasadą „privacy first”. Dla firm – zwłaszcza tych, które rozwijają działalność online, przetwarzają dane klientów czy pracowników – powołanie IOD to inwestycja w spokój, bezpieczeństwo i wiarygodność.

Newsletter RODO

Listopad 2025 nr 11/2025

Dziękujemy za przeczytanie naszego newslettera!

Masz pytania?

SKONTAKTUJ SIĘ Z NAMI

LexDigital

lexdigital.pl LinkedIn