Z F O D O

Incydenty ochrony danych osobowych 2024

Raport Związku Firm Ochrony Danych Osobowych

00 O raporcie

- Badaniem objęliśmy **325 organizacji** obsługiwanych przez firmy zrzeszone w ramach ZFODO w okresie 1/01/2024 - 31/12/2024.
- Na obsługiwane organizacje składa się zarówno sektor publiczny, jak i sektor prywatny.
- Obsługiwane organizacje współpracowały z firmami zrzeszonymi w ramach ZFODO w zakresie outsourcingu IOD lub innej stałej współpracy w zakresie ochrony danych osobowych.

01 Wstęp

Z przyjemnością przedstawiamy kolejną edycję raportu o incydentach ochrony danych osobowych, przygotowaną przez Związek Firm Ochrony Danych Osobowych. Naszym celem jest przybliżenie kluczowych zagadnień związanych z występowaniem i obsługą incydentów w Polsce.

Raport opiera się na rzeczywistych, całkowicie zanonimizowanych danych dostarczonych przez członków ZFODO. Analiza pozwala wskazać trendy i zmiany w podejściu przedsiębiorców do problemu incydentów.

Dane pokazują, że ryzyko dotyczy każdej branży. Największym wyzwaniem pozostaje prawidłowe wykonanie obowiązków wynikających z RODO, co wymaga wiedzy i doświadczenia. Ich zdobycie jest trudne – incydenty zdarzają się rzadko (średnio 1,38 razy w roku na organizację), a błędna reakcja może mieć poważne skutki.

Budowanie wewnętrznych kompetencji wiąże się z dużymi kosztami – etaty, szkolenia, czas. Dlatego coraz więcej firm sięga po outsourcing, który zapewnia szybki i opłacalny dostęp do ekspertów gotowych wesprzeć organizację już w ciągu 72 godzin od incydentu.

Najlepszym rozwiązaniem pozostaje jednak zapobieganie, czyli wcześniejsza identyfikacja ryzyk i stałe wsparcie w zakresie ochrony danych – niezależnie od tego, czy zapewnia je zespół wewnętrzny, czy zewnętrzni specjaliści.

Prezes Zarządu ZFODO
Przemysław Zegarek

02

Prawdopodobieństwo wystąpienia incydentu

449
odnotowanych incydentów

325
organizacji

1,38
średni liczba incydentów przypadających na orgnizację

- Badaniem objęliśmy 325 organizacji, obsługiwanych przez 8 firm zrzeszonych w ramach ZFODO w zakresie outsourcingu IOD lub innej stałej współpracy dotyczącej ochrony danych osobowych. Łącznie w okresie od 1 stycznia do 31 grudnia 2024 w ww. liczbie organizacji, odnotowano 449 incydentów.

Daje to średnią 1,38 incydentu rocznie na każdą organizację. Badanie opieramy na incydentach, które zostały zgłoszone firmom zrzeszonym w ZFODO przez obsługiwane przez nich organizacje. Liczba incydentów, które wystąpiły w rzeczywistości może być wyższa.

ZFODO mówi...

PRZEMYSŁAW ZEGAREK
PREZES ZARZĄDU LEX-ARTIST SP. Z O.O.

W tym roku średnia naruszeń jest najwyższa w historii naszych raportów. Skomentuję to przewrotnie - bardzo dobrze, że odnotowujemy więcej naruszeń!

W mojej opinii ta średnia jest wciąż niedoszacowana. Naruszeń w rzeczywistości jest więcej, tylko część z nich jest zamiatana pod dywan.

03 Incydenty zgłoszone Organowi Nadzoru

- Zgodnie z art. 33 ust. 1 RODO, incydentu możemy nie zgłaszać Regulatorowi, jeśli „jest mało prawdopodobne, by naruszenie to skutkowało ryzykiem naruszenia praw lub wolności osób fizycznych”

ZFODO mówi...

TOMASZ OCHOCKI
WICEPREZES ZARZĄDU ODO 24 SP. Z O.O.

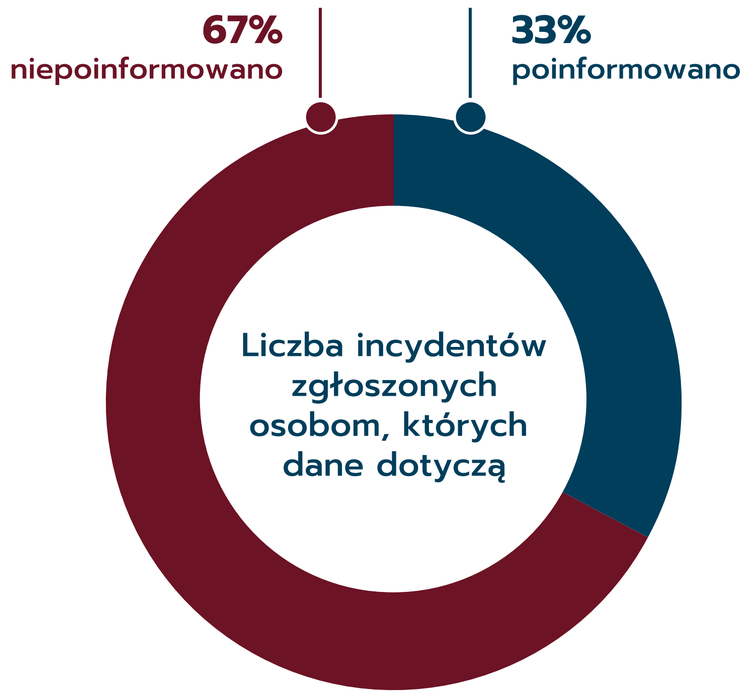
Od początku prowadzenia badań w 2020 roku proporcja zgłoszonych naruszeń ochrony danych osobowych utrzymywała się na względnie stałym poziomie. Wyjątkiem był rok 2022, kiedy to administratorzy danych zgłosili jedynie 23,14% zidentyfikowanych naruszeń. W bieżącym roku odsetek ten wzrósł do 37%, co oznacza wyraźny wzrost względem średniej z całego okresu badań (32,23%).

Moim zdaniem wzrost ten wynika zarówno z czynników obiektywnych – takich jak rosnąca aktywność cyberprzestępcza – jak i subiektywnych, np. rosnącej świadomości administratorów w zakresie obowiązku raportowania naruszeń. Na wzrost zgłoszeń wpływa również polityka nakładania kar przez UODO, z których około 20% dotyczy właśnie nieprawidłowości związanych z naruszeniami.

Przewiduję, że w kolejnym badaniu trend ten ulegnie dalszemu przyspieszeniu, m.in. w efekcie opublikowanego niedawno przez UODO poradnika dotyczącego naruszeń. Nawet jeśli nie była to intencja Urzędu, zawarte tam tezy mogą przyczynić się do trwałego zakotwiczenia poziomu, od którego dokonuje się zgłoszenia na bardzo niskim pułapie.

04

Incydenty zgłoszone osobom, których dane dotyczą



- Niezależnie od zgłoszenia incydentu do Regulatora, zgodnie z art. 34 RODO, *„Jeżeli naruszenie ochrony danych osobowych może powodować wysokie ryzyko naruszenia praw lub wolności osób fizycznych”* to powinniśmy o nim poinformować także same osoby objęte naruszeniem.

Podobnie jak w przypadku raportowania incydentów do Regulatora, ocena wysokiego ryzyka naruszenia praw lub wolności, budzi trudności interpretacyjne. W poprzednim badaniu o incydencie nie poinformowano w 81,51% przypadków.

ZFODO mówi...

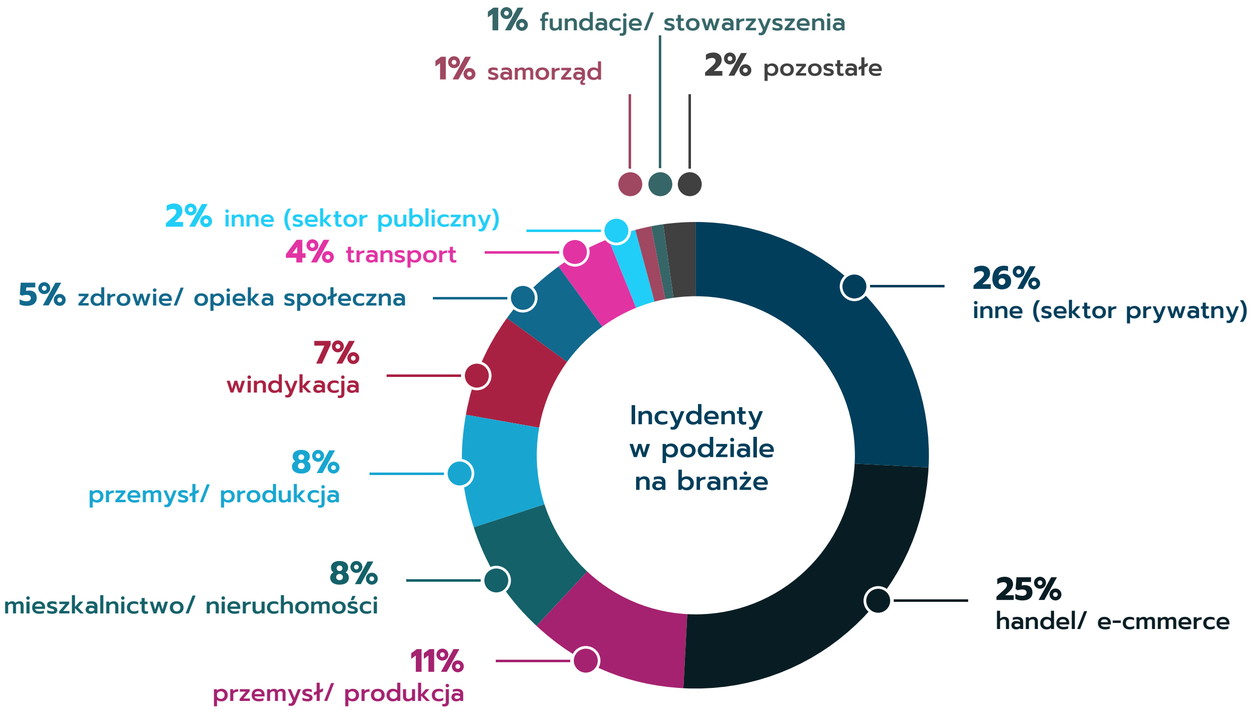
MICHAŁ SZTĄBEREK

EKSPERT DS. OCHRONY DANYCH OSOBOWYCH, CEO W ISECURE SP. Z O.O.

W 2024 roku jedynie 33% przypadków naruszeń ochrony danych osobowych skutkowało poinformowaniem osób objętych incydentem, podczas gdy w aż 67% przypadkach administrator danych nie zdecydował się na tego typu działania. Taka dysproporcja może budzić pytania o sposób oceny ryzyka naruszeń i praktyki stosowane przez administratorów. Z drugiej strony należy jednak zauważyć, że w 2025 roku sytuacja może ulec zmianie. Wydany nie tak dawno temu przez UODO zaktualizowany poradnik dotyczący zgłaszania naruszeń ochrony danych osobowych zawiera wytyczne i przykłady, które mogą przełożyć się na bardziej rygorystyczne działania administratorów w omawianym obszarze. Można więc przewidywać, że w nadchodzących miesiącach odsetek przypadków, w których osoby zostaną poinformowane o naruszeniu ich danych, wzrośnie – przede wszystkim ze względu na wyżej wskazane wytyczne UODO, jak i chęć zminimalizowania ryzyka po stronie administratorów (lepiej na wszelki wypadek poinformować zainteresowanego, bo jest takie pole we wzorze zgłoszenia naruszenia niż tego nie robić). Można na to spojrzeć też bardziej pozytywnie - to sygnał dla organizacji, że proaktywna komunikacja z osobami, których dane są przetwarzane, staje się coraz ważniejszym elementem odpowiedzialnego zarządzania incydentami naruszenia ochrony danych.

05

Branże najbardziej narażone na ryzyko naruszeń ochrony danych osobowych



- Sektor prywatny wygenerował większość incydentów odnotowanych przez ZFODO. Nie można jednak wyciągnąć z tego zbyt daleko idących wniosków. Firmy zrzeszone w ZFODO obsługują w większości sektor prywatny.

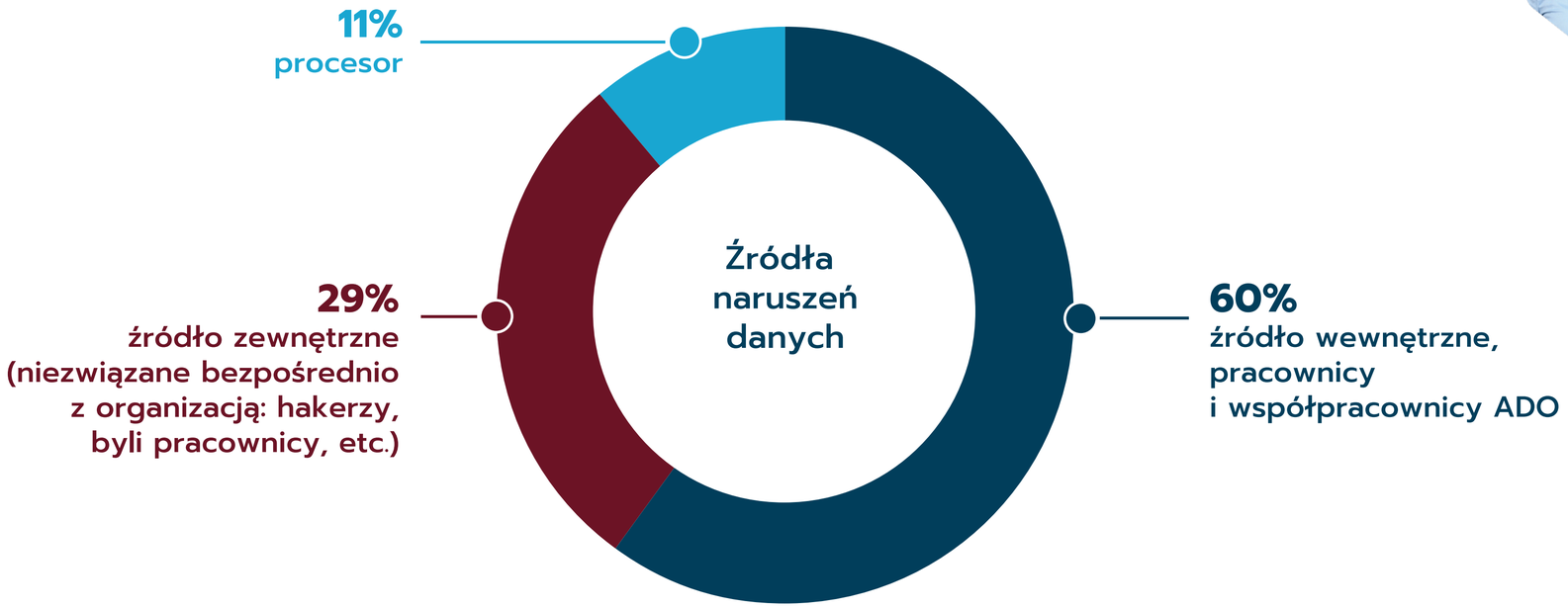
ZFODO mówi...

MAŁGORZATA SITKIEWICZ
RADCA PRAWNY, JDS CONSULTING SP. Z O.O. SP.K

Raport rzuca ciekawe światło na obszar zgłaszania naruszeń ochrony danych w podziale na branże. Szczególną uwagę zwraca bardzo wysoki odsetek incydentów w sektorze handlu i e-commerce (25%). To nie tylko dowód na dużą i wciąż rosnącą skalę przetwarzania danych w tym sektorze, ale także sygnał, że sektor e-commerce coraz lepiej rozumie i potrafi rozpoznawać sytuacje, w których doszło do naruszenia ochrony danych. Na wysoką liczbę zgłoszeń incydentów może wpływać także wysoka cyfrowa świadomość konsumentów, wspierana przez dostępność informacji o przysługujących im środkach ochrony. To może świadczyć o pozytywnym trendzie: użytkownicy sieci są coraz bardziej wyczuleni na bezpieczeństwo danych.
Równocześnie warto zauważyć znaczący udział branży finansowej, w tym ubezpieczeniowej, mieszkaniowej i windykacyjnej (łącznie 23%) w strukturze zgłoszeń. Sektory te operują danymi finansowymi, w tym danymi o zadłużeniu, a ryzyko poważnych skutków naruszeń dla podmiotów danych jest tam wysokie. Duży udział w łącznej liczbie zgłoszeń może wynikać z wysokiej kultury organizacyjnej i lepszego zrozumienia obowiązków wynikających z przepisów o ochronie danych.

06

Źródło naruszeń danych osobowych



Źródła naruszeń zdecydowaliśmy się podzielić na 3 kategorie:

- Zewnętrzne – niezwiązane bezpośrednio z organizacją, hakerzy, byli pracownicy, etc.
- Wewnętrzne – pracownicy i współpracownicy organizacji.
- Procesor – podmioty przetwarzające dane osobowe na zlecenie administratora.

Zdecydowana większość incydentów została spowodowanych działaniami pracowników lub współpracowników organizacji.

ZFODO mówi...

MAGDALENA CIEŚLAK
RADCA PRAWNY, DISCRETIA SP. Z O.O.

Dane za 2024 r. potwierdzają, że przeważająca liczba naruszeń ochrony danych osobowych nadal ma źródło wewnętrzne (60%). Istotną zmianą wymagającą uwagi jest jednak znaczący wzrost incydentów o charakterze zewnętrznym z 13% w 2023 r. do 29%. Taka dynamika wskazuje na intensyfikację zagrożeń wynikających z ataków phishingowych, cyberataków czy wykorzystania podatności technicznych, które coraz skuteczniej omijają dotychczas stosowane środki zabezpieczające.

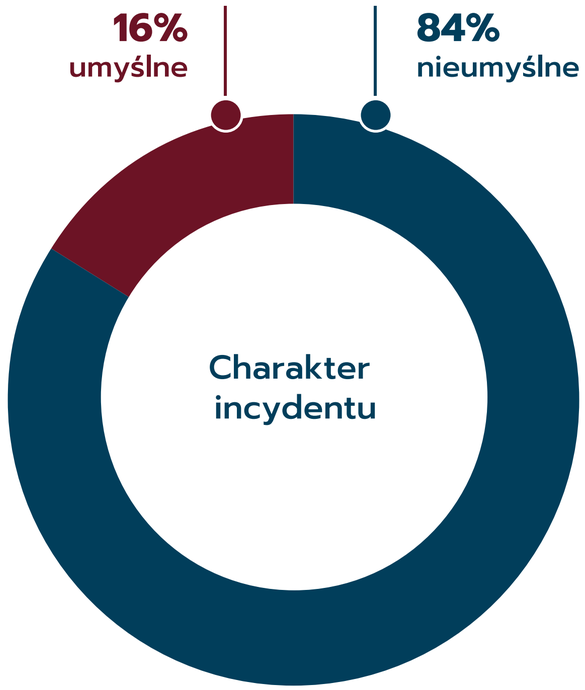
W świetle powyższego nie sposób ograniczać się do formalnego wypełniania obowiązków wynikających z RODO. Konieczne staje się wdrożenie skutecznych mechanizmów monitorowania zagrożeń, sprawnych procedur reagowania na incydenty oraz systemowego podejścia do budowania odporności organizacji.

Równocześnie należy odnotować spadek udziału incydentów po stronie podmiotów przetwarzających z 21% w 2023 r. do 11%. Może to świadczyć o poprawie w zakresie kontroli kontraktowej oraz lepszym egzekwowaniu postanowień umów powierzenia przetwarzania danych osobowych. Moim zdaniem nie powinno to jednak prowadzić do nadmiernego poczucia bezpieczeństwa, wzrost incydentów zewnętrznych potwierdza, że realna ochrona danych wymaga uwzględnienia całego łańcucha przetwarzania, w tym dostawców, partnerów biznesowych oraz infrastruktury chmurowej.

Podsumowując, zgodność z RODO powinna być traktowana nie jako stan formalny, lecz jako wynik świadomego i ciągłego zarządzania ryzykiem, inwestycji w bezpieczeństwo informacji oraz operacyjnej gotowości na wypadek incydentów.

07

Umyślność bądź nieumyślność incydentu



- **Aż 84% incydentów stanowiły działania nieumyślne (w poprzednim badaniu statystyka wyglądała podobnie: 85%). W tej kategorii między innymi:**
  - błędnie zaadresowane maile,
  - brak stosowania kopii ukrytej,
  - wysyłka korespondencji tradycyjnej z błędną zawartością (dane osobowe innej osoby).

Wśród działań umyślnych odnotowaliśmy między innymi:

- kradzieże laptopów (lub innych nośników danych),
- różnego rodzaju wyłudzenia informacji,
- udostępnianie danych osobowych osobom nieuprawnionym.

ZFODO mówi...

MICHAŁ GEILKE
ORLECCY - BEZPIECZEŃSTWO I EDUKACJA

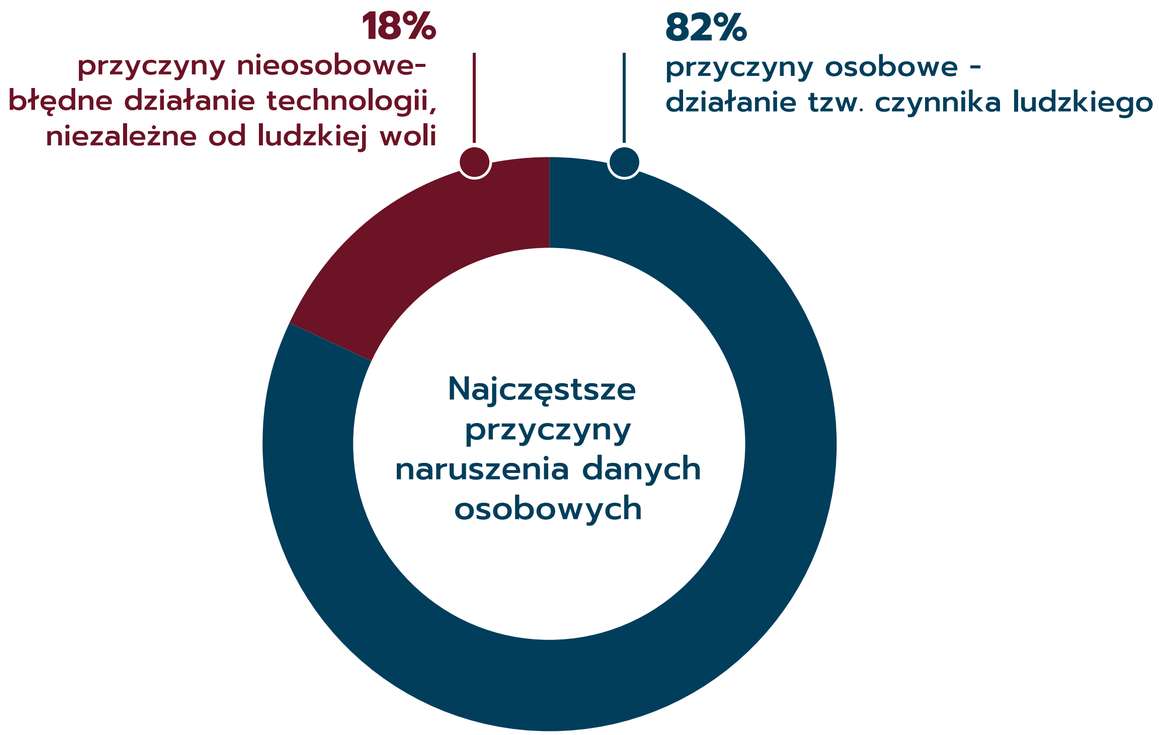
Jakiś czas temu Pan Kevin Mitnick powiedział: „Firmy wydają miliony dolarów na zapory sieciowe, szyfrowanie i urządzenia zabezpieczające dostęp i są to pieniądze wyrzucone w błoto – żadna z tych metod nie rozwiązuje najważniejszego problemu w łańcuchu bezpieczeństwa: ludzi, którzy używają, zarządzają i obsługują systemy informatyczne."
Nasza coroczna analiza incydentów wskazuje, że aż 84% wycieków danych osobowych miało charakter nieumyślny, co potwierdza globalny trend, według którego największym zagrożeniem dla bezpieczeństwa informacji pozostaje niestety czynnik ludzki.

Ignorowanie zagrożenia ze strony czynnika ludzkiego może skutkować poważnymi naruszeniami, nawet bez udziału podmiotów czy osób trzecich, którym by zależało na wystąpieniu incydentu w danej instytucji.

Ze wskazanej statystyki wynika, że incydenty występują najczęściej podczas codziennych sytuacji/czynności, takich jak np. wysłanie wiadomości e-mail, co dodatkowo zwiększa ich ilość.
W kontekście powyższych danych, wyraźnie widać, że inwestycje w typowo „techniczne" cyberbezpieczeństwo muszą iść w parze z regularnym szkoleniem pracowników czy innych działań uświadamiających, wdrażaniem odpowiednich polityk bezpieczeństwa informacji oraz procesów reagowania na incydenty.

08

Przyczyny osobowe vs przyczyny nieosobowe



- Do przyczyn osobowy zaliczyliśmy działania tzw. czynnika ludzkiego. A więc zarówno działania umyślne zewnętrznych osób (np. hakerów), jak i niezawinionych pomyłek pracowników organizacji.

Przyczyny nieosobowe to sytuacje, kiedy naruszenie spowodowane było błędnym działaniem technologii, sytuacjami niezależnymi od ludzkiej woli.
W poprzednim badaniu rozkład przedstawiał się następująco 86% - przyczyny osobowe, 14% - przyczyny nieosobowe.

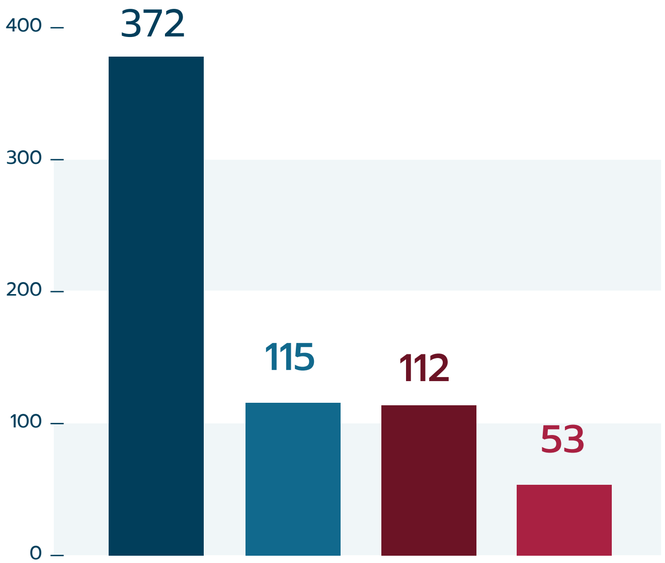
ZFODO mówi...

MAGDALENA CHMIELEWSKA
PREZES ZARZĄDU, ODO MANAGEMENT GROUP SP. Z O.O.

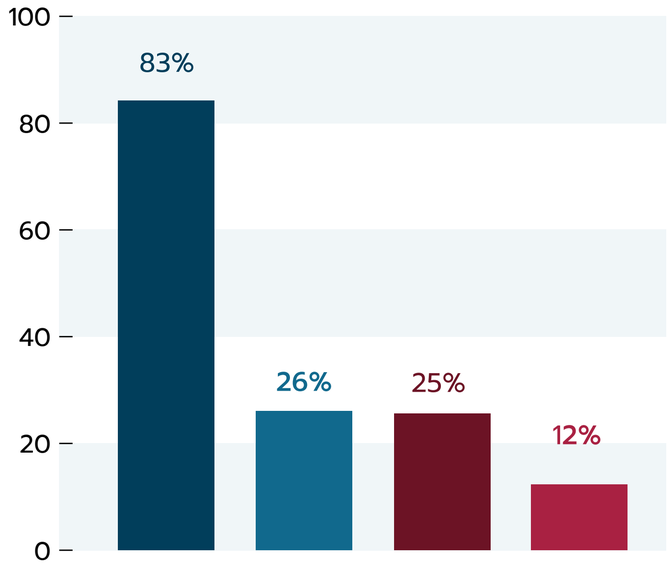
Praktyka ubiegłego roku pokazuje znaczny udział przyczyn „osobowych" (82 %) wobec „nieosobowych" (18 %) w kontekście badanych naruszeń danych. Mimo tak dużej dysproporcji nie ma to przełożenia na skalę naruszeń.
Przyczyny nieosobowe (18 %), takie jak awarie systemów, błędy oprogramowania czy ataki zewnętrzne, stanowią mniejszość, ale są powodem naruszeń o znacznie większej skali. Mają potencjał generowania masowych naruszeń co stanowi ogromne zagrożenie w systemie ochrony danych osobowych. Jeżeli mówimy o przyczynach osobowych to należy rozumieć je jako: pomyłki przy wpisie czy przesłaniu danych, nieuprawnione ujawnienie informacji czy niewłaściwe zarządzanie dostępem oraz poza systemowe, niezależne od rozwiązań technicznych i fizycznych błędny przy codziennej pracy, które obejmują mniejszy zakres danych oraz mniej rekordów naruszonych danych.
Porównując bieżące dane z raportem za rok 2023 widać tendencję spadkową jeśli chodzi o ilość naruszeń osobowych (z 86% na 83%) i tendencję wzrostową jeśli chodzi o ilość naruszeń nieosobowych (z 14% do 18%) w roku 2024.
O ile w przyszłości nie pozbędziemy się naruszeń, których źródłem są błędy ludzkie to należy spodziewać się, że będą one generowały dużo niższy poziom zagrożeń w porównaniu z naruszeniami nieosobowymi, a wdrożenie odpowiednich rozwiązań i wzmocnienie kultury bezpieczeństwa – cykliczne, praktyczne szkolenia oraz testy gotowości pracowników, a także egzekwowanie przez administratorów zapisów procedur będą przynosiły zamierzony efekt. Należy pamiętać, że skuteczna strategia zarządzania ryzykiem powinna uwzględniać zarówno ograniczanie błędów ludzkich, jak i techniczne środki zabezpieczające. Automatyzacja i wsparcie technologiczne mogą ograniczyć pole do błędu, ale nie zastąpią świadomego, odpowiedzialnego działania człowieka.

09 Najczęściej naruszane kategorie danych

Ile incydentów dotyczyło jednej z 4 kategorii danych?



W jakim procencie incydentów, znalazły się dane osobowe poniższych kategorii:



dane podstawowe dane finansowe PESEL dane szczególnej kategorii

* Dane sumują się do więcej niż 100%, ponieważ każdy z 449 incydentów mógł zawierać dane jednej lub większej ilości kategorii.

ZFODO mówi...

MAGDALENA CHMIELEWSKA
PREZES ZARZĄDU, ODO MANAGEMENT GROUP SP. Z O.O.

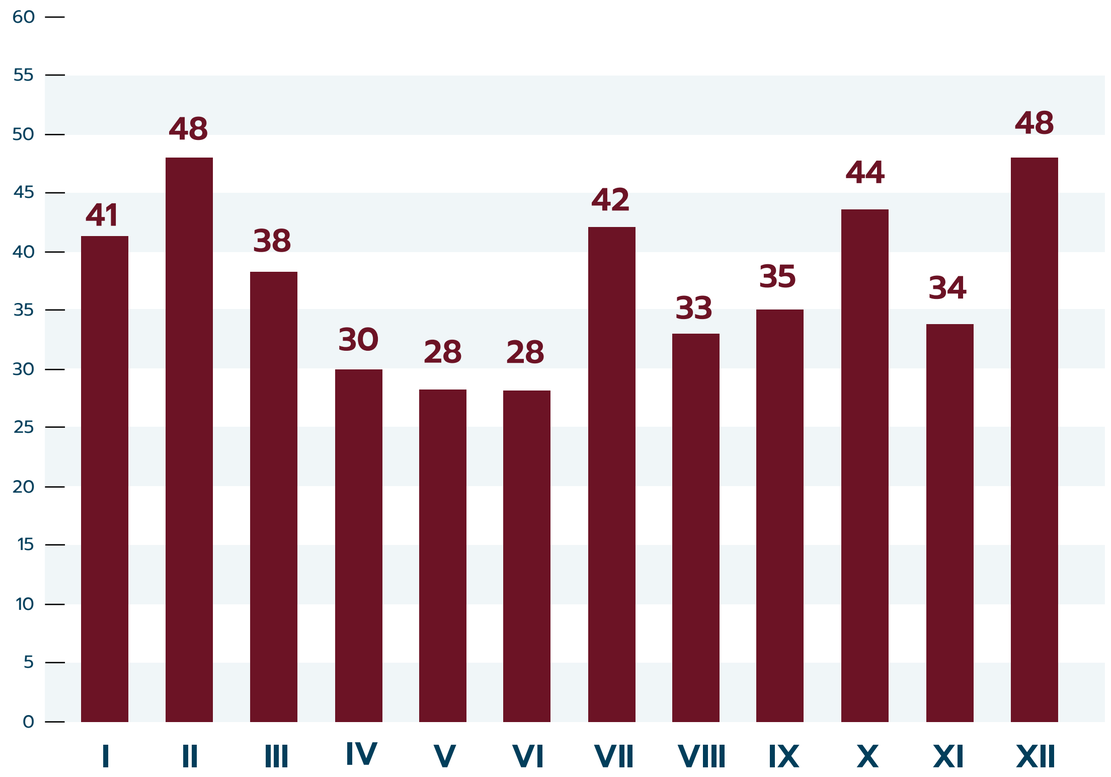
W roku 2024 podobnie jak w latach poprzednich najczęściej naruszane były dane podstawowe – aż w 83% przypadków. Kolejne miejsca zajmują dane finansowe (26%), numer PESEL (25%) oraz dane szczególnej kategorii (12%).

Dane podstawowe, mimo że powszechnie przetwarzane, są najczęściej narażone na wycieki w wyniku błędów ludzkich i niedostatecznych zabezpieczeń. Ujawnienie danych finansowych i numeru PESEL niesie wysokie ryzyko kradzieży tożsamości oraz nadużyć finansowych, dla osób których dane naruszono. Mimo mniejszego udziału procentowego, danych szczególnej kategorii w sumie wszystkich naruszeń objętych raportem, to każdy incydent z ich udziałem ma potencjalnie najpoważniejsze konsekwencje prawne i społeczne.

Wyniki te wskazują na potrzebę wzmocnienia środków ochrony danych – nie tylko w zakresie danych wrażliwych, ale także danych zwykłych, przetwarzanych w codziennej pracy Administratorów. Kluczowe jest zwiększenie świadomości pracowników i poprawa ich kompetencji oraz wdrażanie skutecznych procedur i systemów bezpieczeństwa informacji, które identyfikują i ograniczają zarówno przyczyny osobowe, jak i nieosobowe naruszeń z uwzględnieniem ryzyk środowiskowych (awarii, luk, braków w infrastrukturze) w całym procesie przetwarzania danych.

10

Trend naruszeń



- Wykres obrazuje ilość naruszeń z podziałem na miesiące w których zostały one odnotowane.

ZFODO mówi...

PIOTR KAWCZYŃSKI

PIOTR KAWCZYŃSKI – WICEPREZES ZARZĄDU FORSAFE SP. Z O.O. / WICEPREZES ZARZĄDU ZFODO

Analizując dostępne raporty dotyczące bezpieczeństwa cyberprzestrzeni w Polsce, można wskazać wyraźne trendy sezonowe w liczbie zgłaszanych incydentów.
Najwięcej incydentów odnotowuje się w II kwartale roku, czyli w miesiącach:

- *kwiecień*
- *maj*
- *czerwiec*

Dodatkowo, analiza typów ataków wskazuje na wzmożoną aktywność cyberprzestępców w okresie wakacyjnym, szczególnie jeśli chodzi o kampanie ransomware.

11

Zgłoszenie naruszenia organom ścigania

ZFODO mówi...

TOMASZ OSIEJ

RADCA PRAWNY, PREZES ZARZĄDU OMNI MODO SP. Z O.O.

Patrząc na statystyki odnoszące się do zawiadomienia organów ścigania o naruszeniu ochrony danych osobowych (zawiadomienie o podejrzeniu popełnienia przestępstwa), można zastanawiać się, czy 25% zgłoszonych naruszeń to dużo czy mało? Moim zdaniem jest to znacząca liczba, tym bardziej że zawiadomienie nie może dotyczyć każdego naruszenia ochrony danych a jedynie tego, które wiąże się z podejrzeniem popełnienia przestępstwa, a więc czynu, który podlega penalizacji. Pamiętajmy także, że wiara w skuteczność organów ścigania nie jest wysoka, tym bardziej więc zgłoszenie co czwartego naruszenia do organów ścigania to bardzo wysoki wynik. Z pewnością ta rubryka powinna być szczególnie śledzona przez zarządy i osoby odpowiedzialne, bowiem tutaj odpowiedzialność zawsze ma konkretny osobowy wymiar. Odpowiedzialnym nie jest administrator (np. spółka) ale osoba fizyczna która odpowiada za to, że doszło do naruszenia!

Jeżeli:

- **zatrudniasz min. 3 osoby,**
- **specjalizujesz się w RODO min. 5 lat,**
- **Twoja firma prezentuje wysoki poziom merytoryczny i wysokie standardy etyczne,**
- **chcesz współtworzyć podobne raporty,**
- **szukasz kontaktu z praktykami z branży.**

Zapraszamy Cię do naszej organizacji:

www.zfodo.org.pl

Polecamy również zapoznanie się ze stanowiskami i opiniami ZFODO:

www.zfodo.org.pl/opinie/

Odpowiadamy w nich na praktyczne problemy stawiane przez naszych klientów.

ZFODO

Związek Firm Ochrony Danych Osobowych

Ul. Hoża 86/410

00-682 Warszawa

e-mail: kontakt@zfodo.org.pl

www.zfodo.org.pl