RAPORT Z BADANIA

# Polskie firmy z sektora MŚP wobec cyberzagrożeń

listopad 2026



Badanie na zlecenie:

CHRONPESEL.PL

KRAJOWY REJESTR DŁUGÓW www.krd.pl

Patronat:

IPODO Instytut Prawa Ochrony Danych Osobowych

UNIWERSYTET VIZJA

# Spis treści

## Wprowadzenie

Słowo wstępne Adama Łąckiego, prezesa Zarządu KRD 3–4
Słowo wstępne Jakuba Groszkowskiego, honorowego prezesa IPODO 5–6
O badaniu i najważniejsze wnioski 7

## I Doświadczenia firm

Ponad połowa firm doświadczyła kradzieży danych lub próby ich wyłudzenia 8
Jak dochodzi do kradzieży danych? 9
Fałszywe wiadomości najczęstszą formą prób wyłudzenia 10
Czego najbardziej obawiają się przedsiębiorcy? 11
Oszustwo może zaczynać się od zwykłej wiadomości służbowej 12

## II Konsekwencje i reakcje firm

Cyberzagrożenia mogą zakłócić pracę firmy 13
Ile trwały przestoje i jak duże były straty firm? 14
Skutki cyberincydentu mogą wykraczać poza utratę danych 15
Kto pomaga wykrywać cyberzagrożenia? 16
Komu firmy zgłaszają incydenty? 17
Jak firmy reagują po wykryciu cyberzagrożenia? 18

## III Zabezpieczenia w codziennej pracy

Jak firmy zabezpieczają dane i systemy? 19–20
Prywatne urządzenia w sprawach służbowych 21
Ryzyko i obowiązki przedsiębiorców 22
Technologia i zarządzanie bezpieczeństwem 23

## IV Pracownicy i przygotowanie na incydenty

Jak firmy szkolą pracowników? 24
Czy firmy ćwiczą reagowanie na zagrożenia? 25
Co trzecia firma ma spisany plan znany pracownikom 26
Do zasad ochrony danych warto wracać w trakcie zatrudnienia 27
Jak firmy wspierają ochronę danych pracowników? 28

## V Współpraca z podmiotami zewnętrznymi

Większość firm przekazuje dane podmiotom zewnętrznym 29
Czy przedsiębiorcy obawiają się naruszeń u partnerów? 30
Ochrona danych we współpracy z dostawcami 31

**Autorzy raportu i patroni** 32



CHRONPESEL.PL
KRAJOWY REJESTR DŁUGÓW
Instytut Prawa Ochrony Danych Osobowych
UNIWERSYTET VIZJA

# Ochrona danych w codziennych decyzjach biznesowych



SŁOWO WSTĘPNE

**Adam Łącki**
prezes Zarządu
Krajowego Rejestru Długów
Biura Informacji Gospodarczej SA

Szanowni Państwo,

prowadzenie firmy wymaga codziennej oceny ryzyka. Sprawdzamy wiarygodność kontrahenta, ustalamy warunki współpracy i pilnujemy rozliczeń. Podobnej uwagi wymagają informacje, na których opierają się te działania. Dane klientów, dokumenty handlowe czy dostęp do firmowych kont są częścią prowadzonego biznesu. Ich ochrona powinna mieć stałe miejsce w decyzjach właściciela i kadry zarządzającej.

Krajowy Rejestr Długów wspólnie z serwisem ChronPESEL.pl zlecił badanie polskich MŚP, aby poznać doświadczenia przedsiębiorców oraz stosowane przez nich sposoby ochrony informacji. Kradzieży danych lub próby ich wyłudzenia doświadczyło 58 proc. badanych firm. Za tym wynikiem stoją zdarzenia, z którymi przedsiębiorcy musieli zmierzyć się podczas prowadzenia działalności.

Zapytaliśmy też przedsiębiorców o przekazywanie danych podmiotom zewnętrznym. Odpowiedzi pokazują skalę współpracy, w której warunki korzystania z informacji trzeba ustalić z firmą wykonującą zlecone zadania.

# Koszty i warunki zewnętrznej obsługi firmy

**Adam Łącki — ciąg dalszy wstępu**

80 proc. badanych firm przekazuje dane pracowników lub klientów podmiotom zewnętrznym, np. przy zlecaniu obsługi księgowej, kadrowo-płacowej lub informatycznej.

## Co obejmuje opłata za obsługę IT?

Porównując oferty obsługi informatycznej, warto ustalić, czy opłata za utrzymanie systemu obejmuje pomoc przy problemach z dostępem do danych i ich odtworzeniu. Trzeba też uzgodnić, kto podejmie działania po zgłoszeniu takiej sytuacji, w jakim czasie i za które prace przedsiębiorca zapłaci dodatkowo. Pozwala to ocenić koszt usługi wraz ze wsparciem, którego firma rzeczywiście potrzebuje.

## Przekazanie danych przy zmianie partnera

Przy zmianie biura rachunkowego lub firmy kadrowo-płacowej warto wcześniej uzgodnić termin i sposób przekazania danych oraz dokumentacji. Trzeba też sprawdzić, czy nowy partner będzie mógł wykorzystać otrzymane pliki i czy ich przygotowanie wymaga dodatkowej opłaty. Dostęp do historii rozliczeń lub dokumentów pracowniczych powinien być zapewniony także podczas przenoszenia obsługi. Te ustalenia pomagają zaplanować koszty zmiany i pracę własnego zespołu.

Zachęcam do wykorzystania tej publikacji jako punktu wyjścia do rozmowy o konkretnych decyzjach związanych z ochroną danych we własnej firmie. Warto zakończyć ją ustaleniem, co wymaga zmiany i kto dopilnuje jej wprowadzenia.

# Ochrona danych a ciągłość działania firm



SŁOWO WSTĘPNE

**Jakub Groszkowski**
zastępca prezesa UODO
w latach 2022–2024,
honorowy prezes Instytutu Prawa
Ochrony Danych Osobowych

Szanowni Państwo,

oddajemy w Państwa ręce raport „Polskie firmy z sektora MŚP wobec cyberzagrożeń". Jest on szczególnie ważny w kontekście ostatnich, największych wycieków w historii Polski. Kierujemy go do przedsiębiorców, kadry zarządzającej oraz wszystkich, którzy na co dzień odpowiadają za ochronę danych i bezpieczeństwo systemów. Chcemy upowszechniać wiedzę o zagrożeniach i sposobach przeciwdziałania im.

Omawiamy najważniejsze zagadnienia związane z codziennym funkcjonowaniem przedsiębiorstw. Pokazujemy, jak ochrona danych osobowych wiąże się ze zdolnością do prowadzenia działalności w razie cyberzagrożenia.

Punktem odniesienia jest przygotowanie na każdym etapie – od rozpoznawania zagrożeń i stosowania odpowiednich zabezpieczeń, przez wykrycie incydentu i ocenę jego skutków dla osób fizycznych, po przywrócenie sprawnego funkcjonowania przedsiębiorstwa. Szczególną uwagę poświęcamy sektorowi MŚP, w którym zadania związane z bezpieczeństwem informacji często wykonują osoby łączące je z innymi obowiązkami. Publikacja ma im pomóc ocenić obecną gotowość i ustalić, co warto zrobić w pierwszej kolejności.

Sektor MŚP ma kluczowe znaczenie dla polskiej gospodarki. Tworzy miejsca pracy, zapewnia dostęp do usług na lokalnych rynkach i odpowiada za blisko połowę krajowego PKB. Często mikro-, małe i średnie firmy są też dostawcami dla większych partnerów biznesowych, pełniąc rolę administratorów danych lub podmiotów przetwarzających. Jeśli utracą one dostęp do systemu zamówień lub informacji potrzebnych do wypłaty wynagrodzeń, konsekwencje odczują ich pracownicy, klienci i kontrahenci. Sprawne reagowanie na incydenty ma więc znaczenie dla ciągłości działania całych łańcuchów dostaw.

# Zabezpieczenia i reagowanie na incydenty

**Jakub Groszkowski — ciąg dalszy wstępu**

## Zabezpieczenia w codziennej pracy

W małej firmie warto zacząć od uwierzytelniania dwuskładnikowego w poczcie elektronicznej i na kontach administracyjnych, aktualizowania oprogramowania oraz nadawania pracownikom tylko tych uprawnień, których potrzebują do pracy. Co najmniej jedną kopię zapasową należy oddzielić od głównych systemów i regularnie sprawdzać, czy da się z niej odtworzyć dane. Krótkie szkolenia oparte na przykładach pomagają rozpoznawać próby wyłudzenia. Każdy powinien wiedzieć, komu zgłosić podejrzaną wiadomość lub pomyłkę przy przesyłaniu informacji.

## Plan działania i obowiązki po naruszeniu

Plan reagowania na incydenty warto przygotować i wdrożyć z wyprzedzeniem. Dokument powinien określać, kto ogranicza skutki zdarzenia, ocenia ryzyko dla osób fizycznych i odpowiada za zgłoszenie. Każde naruszenie ochrony danych osobowych wymaga analizy i udokumentowania. Jeśli może zagrażać prawom lub wolnościom osób, administrator informuje właściwy organ nadzorczy – w Polsce Prezesa UODO. Należy to zrobić bez zbędnej zwłoki, w miarę możliwości w ciągu 72 godzin od stwierdzenia naruszenia. Przy wysokim ryzyku co do zasady trzeba również niezwłocznie zawiadomić osoby, których dane dotyczą.

Jestem przekonany, że niniejsza publikacja stanowi cenne źródło informacji o świadomości polskich firm z sektora MŚP dotyczącej ochrony danych osobowych i cyberzagrożeń. Zawiera również praktyczne wskazówki dla wszystkich zainteresowanych tymi zagadnieniami.

# O badaniu

Badanie „Polskie firmy z sektora MŚP wobec cyberzagrożeń” zostało przeprowadzone w październiku 2026 roku przez IMAS International na zlecenie serwisu ChronPESEL.pl i Krajowego Rejestru Długów na reprezentatywnej próbie 508 mikro-, małych i średnich przedsiębiorstw. Patronami badania są Instytut Prawa Ochrony Danych Osobowych oraz Uniwersytet VIZJA.

## Najważniejsze wnioski

**58 proc.**

**firm doświadczyło kradzieży danych lub próby ich wyłudzenia**

Wśród firm, które doświadczyły takich zdarzeń, 20 proc. wskazało przestój, 17 proc. straty finansowe, a 16 proc. utratę klienta lub kontraktu. Skutki mogą więc dotyczyć zarówno ciągłości pracy, jak i relacji handlowych.

**39 proc.**

**wykrycie dzięki zgłoszeniu pracownika**

W firmach, które doświadczyły kradzieży danych lub próby ich wyłudzenia, zgłoszenia pracowników pomagały wykrywać zdarzenia niemal równie często jak działania informatyków. Podkreśla to znaczenie szkoleń, które częściej deklarowano przy zatrudnieniu niż wielokrotnie w jego trakcie.

**34 proc.**

**firm ma spisany plan znany pracownikom**

Testy lub ćwiczenia co najmniej raz w roku deklaruje 65 proc. przedsiębiorstw. Rzadziej wskazywano spisane zasady postępowania znane pracownikom. Obecnie 32 proc. badanych firm nie ma żadnego planu, wliczając przedsiębiorstwa dopiero zamierzające go opracować.

**80 proc.**

**firm przekazuje dane podmiotom zewnętrznym**

Wśród firm przekazujących partnerom zewnętrznym dane pracowników lub klientów 52 proc. obawia się ich naruszenia. Zasady dostępu do informacji i postępowania po incydencie mają więc znaczenie również w relacjach z podmiotami obsługującymi firmę.

# Ponad połowa firm doświadczyła kradzieży danych lub próby ich wyłudzenia

**58 proc.**

BADANYCH FIRM

zetknęło się z kradzieżą danych osobowych lub próbą ich wyłudzenia

RODZAJE ZDARZEŃ

**48 proc.**

próba wyłudzenia danych osobowych

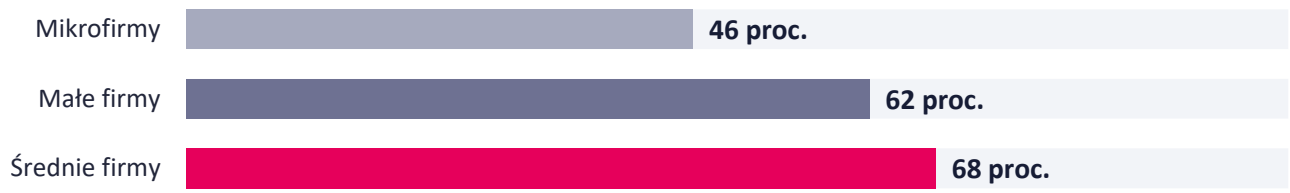
**24 proc.**

kradzież danych osobowych

**14 proc.** firm wskazało oba rodzaje zdarzeń

## Różnice ze względu na wielkość firmy

Odsetek wszystkich firm danej wielkości





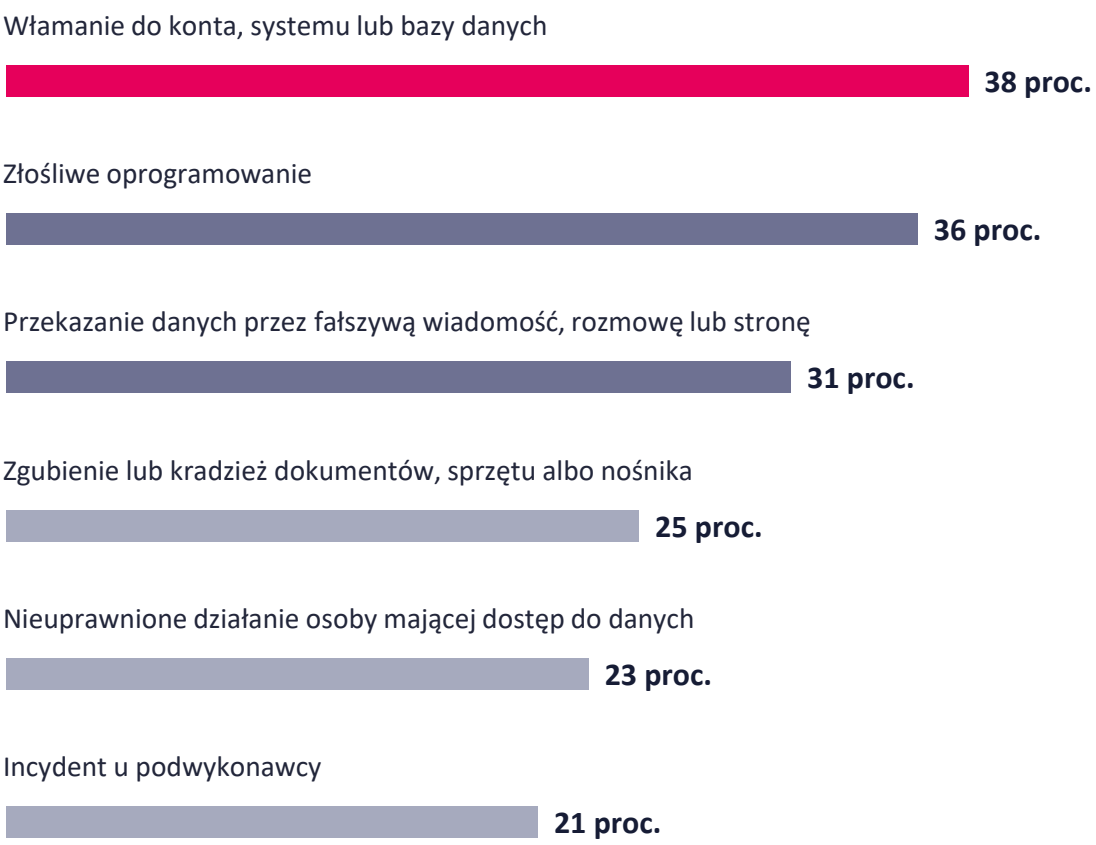

CHRONPESEL.PL
KRAJOWY REJESTR DŁUGÓW
Instytut Prawa Ochrony Danych Osobowych
UNIWERSYTET VIZJA

# Jak dochodzi do kradzieży danych?

Wśród firm, które doświadczyły kradzieży danych osobowych, najczęściej wskazywanym sposobem było włamanie do konta, systemu lub bazy danych. Zbliżony odsetek przedsiębiorstw wymieniał złośliwe oprogramowanie.

## Najczęściej wskazywane sposoby kradzieży

Odsetek firm, które doświadczyły kradzieży danych osobowych



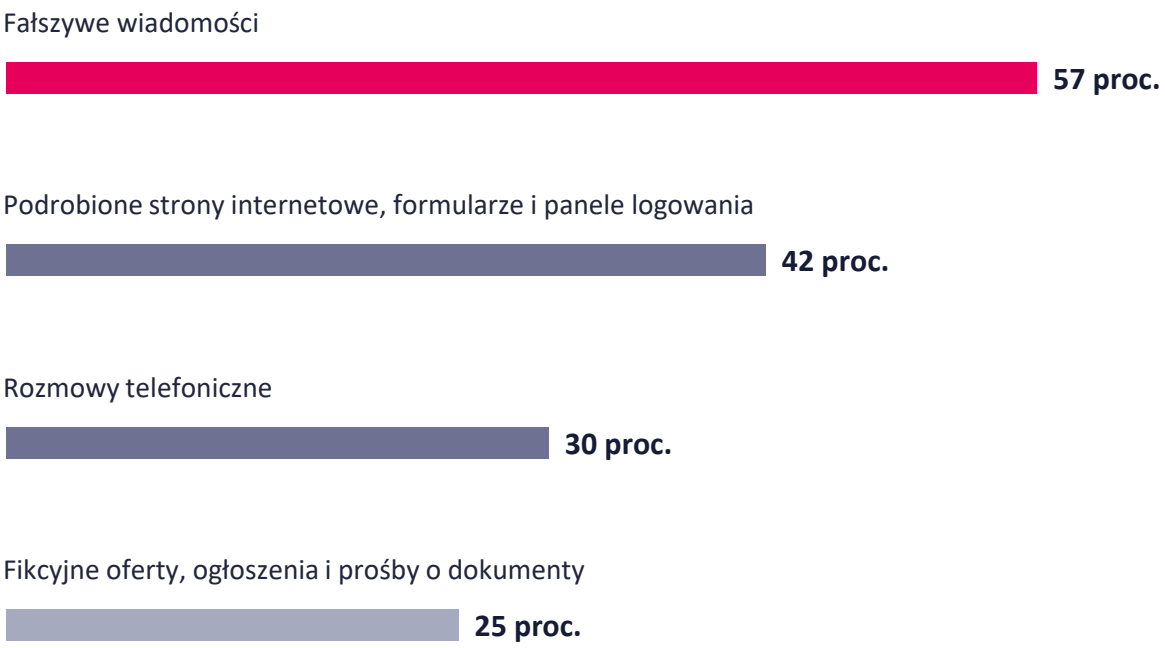

Pozostałe odpowiedzi pokazują, że do utraty poufnych informacji dochodziło także po ich przekazaniu w wyniku oszustwa, zagubieniu dokumentów lub sprzętu oraz nieuprawnionym działaniu osoby z dostępem do danych. Część przedsiębiorców wskazała incydent u podwykonawcy.

# Fałszywe wiadomości najczęstszą formą prób wyłudzenia

Fałszywe wiadomości mogą trafiać do pracowników e-mailem, SMS-em, przez komunikator lub portal społecznościowy. Nadawca może podszywać się pod bank, urząd, kontrahenta albo inną osobę z firmy. Wyniki dotyczą przedsiębiorstw, które zetknęły się z próbą wyłudzenia danych.

## Jak próbowano wyłudzić dane?

Odsetek firm, które doświadczyły próby wyłudzenia danych



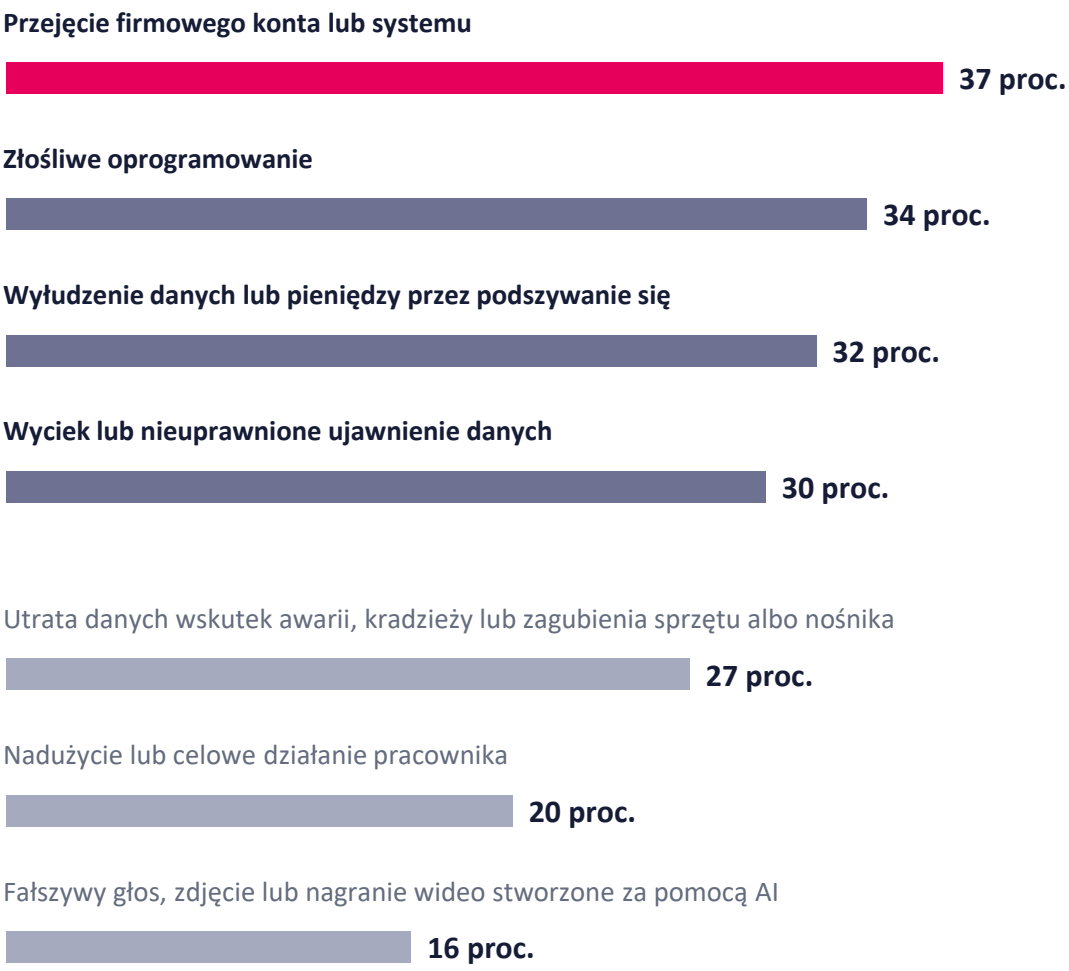

Podrobione strony i panele logowania miały przypominać prawdziwe serwisy, a oszuści dzwoniący do firm podszywali się pod inne osoby. Wskazywano też fikcyjne oferty, ogłoszenia lub prośby o dokumenty. Takie próby mogą pojawiać się przy obsłudze zamówień, rozliczeniach i kontaktach z partnerami biznesowymi.

# Czego najbardziej obawiają się przedsiębiorcy?

Na czele listy obaw związanych z działalnością cyberprzestępców znalazły się przejęcie firmowego konta lub systemu oraz złośliwe oprogramowanie. Włamania i infekcje urządzeń były też najczęściej wskazywanymi sposobami kradzieży danych wśród przedsiębiorstw, które jej doświadczyły.

## Ranking zagrożeń

Odsetek wszystkich badanych firm wskazujących dane zagrożenie




Podszywanie się pod bank, urząd czy kontrahenta pojawia się zarówno wśród obaw, jak i w opisach prób wyłudzenia, z którymi w praktyce zetknęli się przedsiębiorcy. Wyniki obu pytań odnoszą się jednak do różnych kwestii: postrzeganych zagrożeń oraz rzeczywistych doświadczeń firm.

# Oszustwo może zaczynać się od zwykłej wiadomości służbowej



KOMENTARZ EKSPERTA

**Bartłomiej Drozd,**
ekspert serwisu ChronPESEL.pl

Cyberprzestępcy często wykorzystują zwykłe obowiązki pracowników i ich relacje z partnerami biznesowymi. Fałszywe powiadomienie o zamówieniu, fakturze lub prośba o dokumenty mogą wyglądać jak element codziennej pracy. Znajomy podpis czy logo nadawcy nie potwierdzają jednak autentyczności wiadomości.

Oszuści mogą np. wysłać fałszywy e-mail, w którym pod pretekstem aktualizacji umowy proszą o dane osób upoważnionych do składania zamówień. Powołują się przy tym na dotychczasową współpracę i nalegają na szybką odpowiedź. Pracownik może uznać to za rutynową formalność i udostępnić informacje nieuprawnionej osobie.

Fałszywe powiadomienie o zamówieniu może też prowadzić do podrobionego panelu logowania. Strona podobna do znanego serwisu służy wtedy do przejęcia loginu i hasła. Zapisana zakładka w przeglądarce pozwala otworzyć właściwy panel bez korzystania z linku podanego w wiadomości.

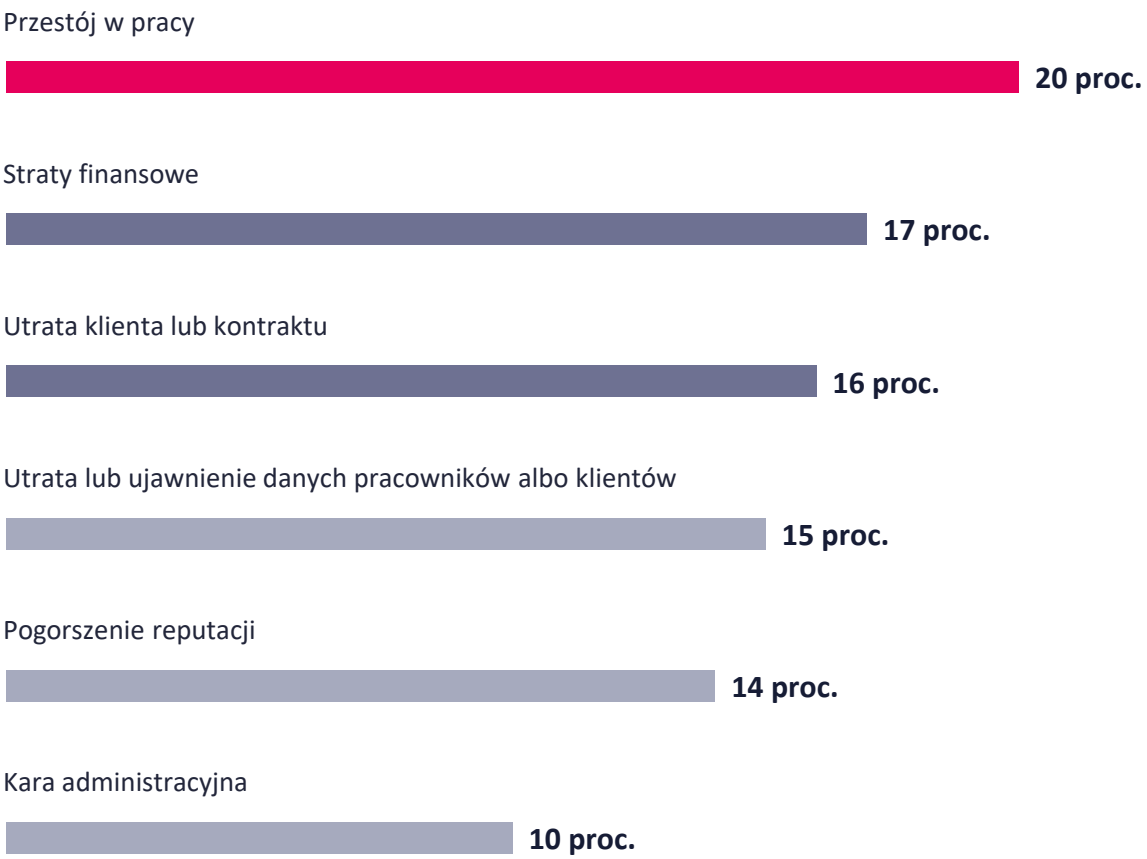
Nietypową prośbę o dokumenty należy potwierdzić przed ich przesłaniem. Najlepiej zadzwonić do znanej osoby u kontrahenta, korzystając z wcześniej zapisanego numeru. W rozmowie można ustalić, czy prośba rzeczywiście od niej pochodzi i jakie informacje są potrzebne. Odpowiedź na otrzymany e-mail lub połączenie z numerem podanym w jego treści może trafić do oszusta.

# Cyberzagrożenia mogą zakłócić pracę firmy

Wyniki dotyczą firm, które doświadczyły kradzieży danych lub próby ich wyłudzenia. W tej grupie najczęściej wskazywanym zauważalnym skutkiem był przestój w pracy. Przedsiębiorcy wymieniali też straty finansowe i utratę klienta lub kontraktu.

## Konsekwencje wskazane przez firmy

Firmy, które doświadczyły kradzieży danych lub próby ich wyłudzenia




Odpowiedzi pokazują, że skutki dotyczyły bieżącej działalności oraz finansów firmy, a także relacji z klientami. Obejmowały też utratę lub ujawnienie danych osobowych, pogorszenie reputacji czy nałożenie kar administracyjnych.

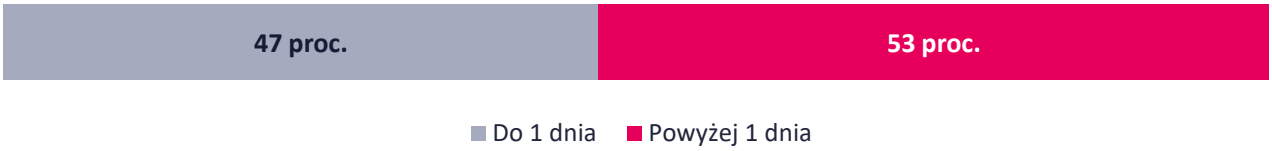
# Ile trwały przestoje i jak duże były straty firm?

Wśród firm, które odnotowały przestój, częściej wskazywano przerwę przekraczającą jeden dzień niż krótsze zakłócenie. W grupie deklarującej straty finansowe najczęściej wybierano przedział od 10 do 100 tys. zł.

## Jak długo trwał przestój?

Wśród firm, które odnotowały przerwę w pracy

**53 proc.** wskazało przerwę w pracy dłuższą niż jeden dzień




## Jak duże były straty finansowe?

Wśród firm, które zadeklarowały straty finansowe

**61 proc.** wskazało straty od 10 do 100 tys. zł




Oba zestawienia dotyczą firm, które zgłosiły konkretną konsekwencję kradzieży danych lub próby ich wyłudzenia. Przedstawione odsetki odnoszą się wyłącznie do tych grup.



CHRONPESEL.PL
KRAJOWY REJESTR DŁUGÓW
Instytut Prawa Ochrony Danych Osobowych
UNIWERSYTET VIZJA

# Skutki cyberincydentu mogą wykraczać poza utratę danych



KOMENTARZ EKSPERTA

**Adam Łącki,**
prezes Zarządu Krajowego Rejestru Długów
Biura Informacji Gospodarczej SA

Kradzież lub wyciek danych to bezpośrednie zagrożenie dla przychodów firmy. Utrata dostępu do systemu zamówień może zatrzymać dostawy lub realizację usług. Dla klienta liczy się jednak uzgodniony termin. Jeżeli nie może pozwolić sobie na opóźnienie, poszuka innego dostawcy. Przedsiębiorca ryzykuje wtedy utratę bieżącego zamówienia, a także kolejnych zleceń. Skutki takiej przerwy mogą więc być odczuwalne jeszcze długo po przywróceniu działania systemów.

Przestój nie zatrzymuje też bieżących wydatków. Nadal trzeba wypłacić wynagrodzenia, opłacić czynsz i rozliczyć się z dostawcami. Do tego mogą dojść koszty odtworzenia danych i pomocy specjalistów oraz dodatkowa praca przy nadrabianiu zaległości. Firma płaci więc za usunięcie skutków incydentu, a równocześnie może tracić wpływy ze sprzedaży. W efekcie rosnące wydatki i mniejsze przychody utrudniają terminowe regulowanie zobowiązań wobec kontrahentów.

Osobne ryzyko wiąże się z ujawnieniem danych klientów lub poufnych informacji dotyczących współpracy. Partner biznesowy może uznać, że dalsze powierzanie ich firmie jest zbyt ryzykowne i ograniczyć zamówienia albo zakończyć współpracę. Utrata zaufania przekłada się wówczas na konkretną stratę finansową. Dlatego przy ocenie kosztów incydentu trzeba uwzględnić również wartość utraconych kontraktów oraz nakłady na pozyskanie nowych odbiorców. Odbudowa przychodów może trwać dłużej niż usunięcie problemu technicznego.

# Kto pomaga wykrywać cyberzagrożenia?

Wśród firm, które doświadczyły kradzieży danych lub próby ich wyłudzenia, najczęściej wskazywano wykrycie przez specjalistów IT oraz zgłoszenie pracownika. Ostrzeżenia docierały też od klientów i partnerów biznesowych.

## Najczęściej wskazywane sposoby wykrycia

**40 proc.**

wykrycie przez dział IT
lub zewnętrzną firmę informatyczną

**39 proc.**

zgłoszenie
pracownika

## Jak jeszcze wykrywano cyberzagrożenia?

Wśród firm, które doświadczyły kradzieży danych lub próby ich wyłudzenia



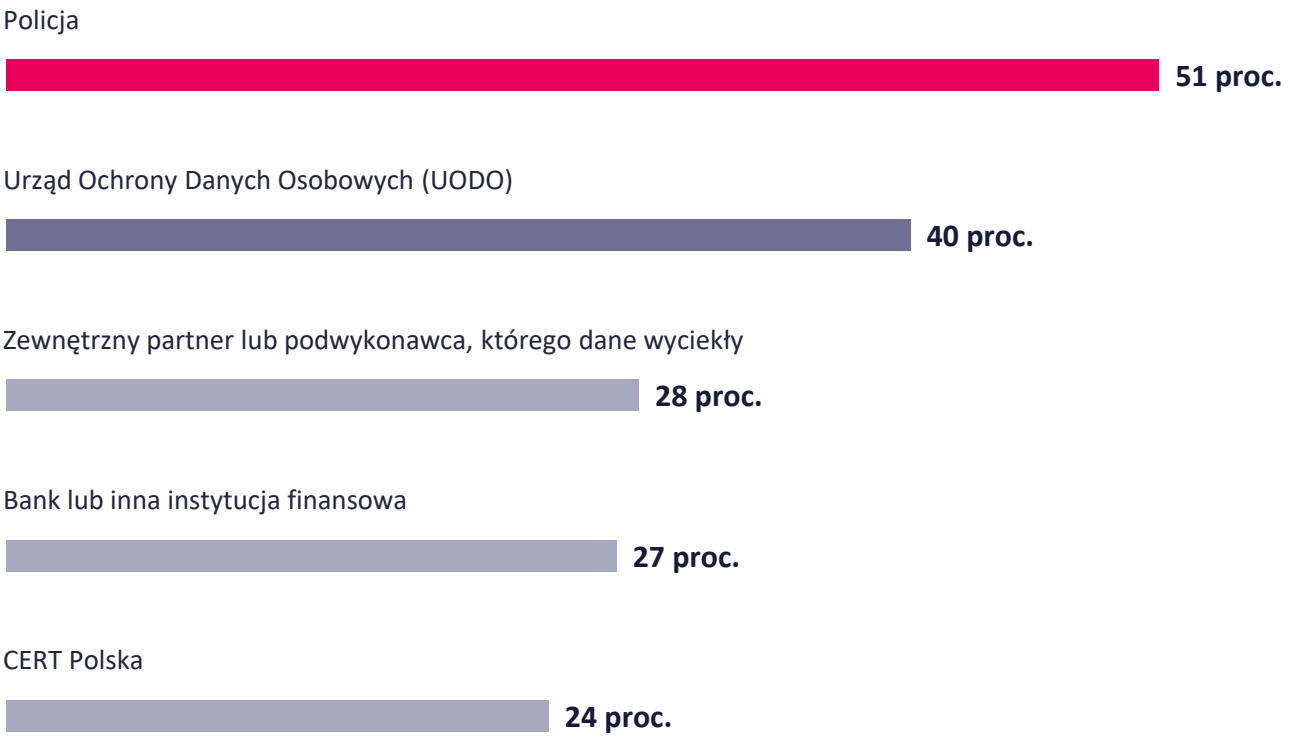

Zgłoszenia pracowników wskazywano niemal tak często jak wykrycie zagrożenia przez informatyków. Warto więc zadbać, aby każdy wiedział, komu przekazać informację o podejrzanej wiadomości lub nietypowym działaniu firmowego systemu.

# Komu firmy zgłaszają incydenty?

Wyniki dotyczą firm, które doświadczyły kradzieży danych lub próby ich wyłudzenia. Informację o takim incydencie przekazywały instytucjom publicznym, bankom i partnerom biznesowym.

## Odbiorcy zgłoszeń

Firmy, które doświadczyły kradzieży danych lub próby ich wyłudzenia




**7 proc.** firm zadeklarowało, że nie zgłosiło zdarzenia nikomu.

Zgłoszenie sprawy policji deklarowano ponad dwa razy częściej niż kontakt z CERT Polska. Przedsiębiorcy informowali również partnerów lub podwykonawców, których dane wyciekły, a więc firmy bezpośrednio dotknięte incydentem.

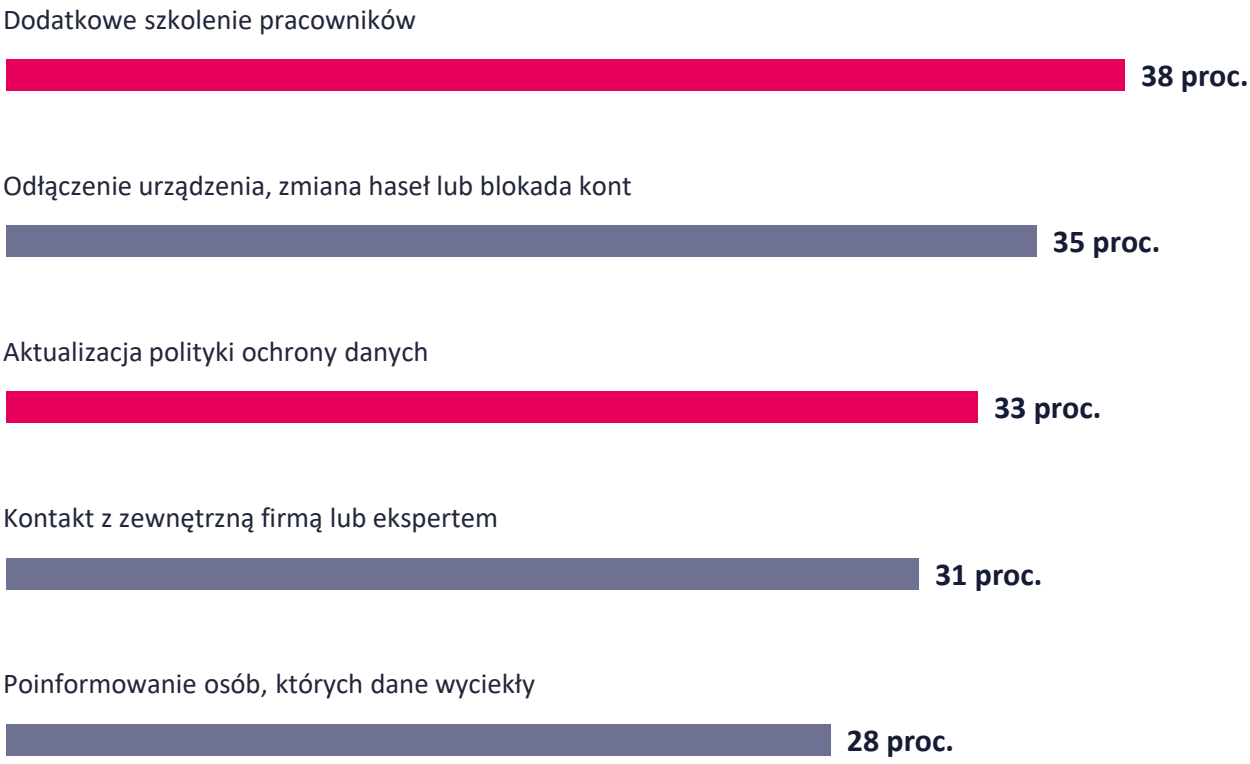
# Jak firmy reagują po wykryciu cyberzagrożenia?

Po kradzieży danych lub próbie ich wyłudzenia przedsiębiorcy wskazywali działania dotyczące samego incydentu oraz zmiany na przyszłość. Najczęściej wymieniali dodatkowe szkolenie pracowników. Wyniki dotyczą firm, które doświadczyły co najmniej jednego z tych zdarzeń.

## Wybrane działania po incydencie

Firmy, które doświadczyły kradzieży danych lub próby ich wyłudzenia

**Zmiany na przyszłość** **Reakcja na zdarzenie**




Po opanowaniu incydentu warto sprawdzić, co wymaga zmiany w codziennej ochronie danych. Kolejna część raportu pokazuje, jakie zabezpieczenia firmy stosują i jak przygotowują pracowników do rozpoznawania zagrożeń.



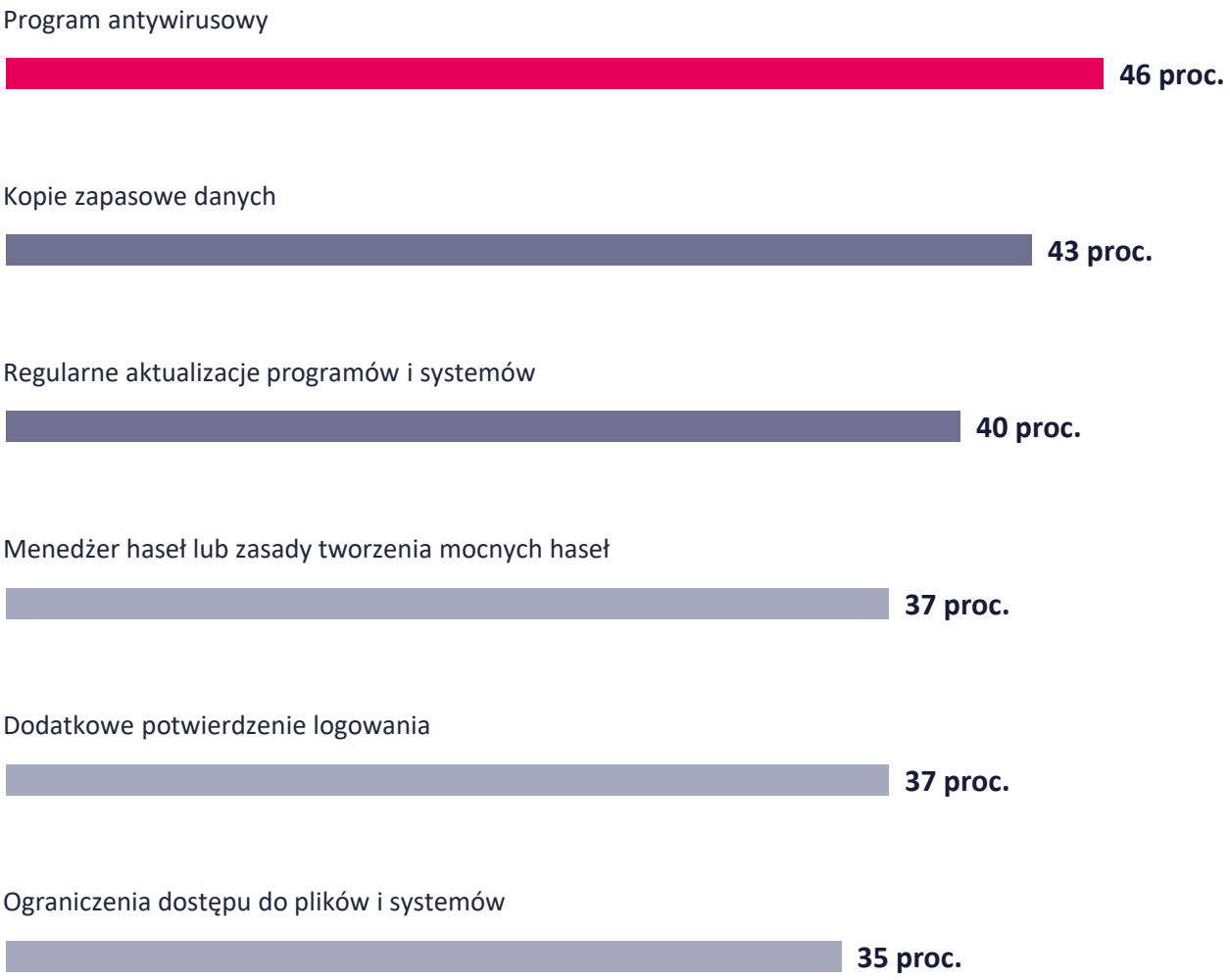
CHRONPESEL.PL
KRAJOWY REJESTR DŁUGÓW
Instytut Prawa Ochrony Danych Osobowych
UNIWERSYTET VIZJA

# Jak firmy zabezpieczają dane i systemy?

Najczęściej deklarowanymi zabezpieczeniami były program antywirusowy i kopie zapasowe danych. Przedsiębiorcy wskazywali również aktualizowanie oprogramowania oraz rozwiązania dotyczące logowania i dostępu do firmowych zasobów.

## Najczęściej stosowane przez firmy zabezpieczenia

Odsetek wszystkich badanych firm




Korzystanie z programu antywirusowego deklarowała mniej niż połowa badanych firm. Jeszcze rzadziej wskazywano rozwiązania dotyczące haseł, dodatkowego potwierdzania logowania oraz ograniczania dostępu do plików i systemów.

# Rzadziej stosowane zabezpieczenia

Filtrowanie podejrzanych wiadomości i stron wskazywano częściej niż blokowanie wysyłania poufnych plików poza firmę. Szyfrowanie oraz ochronę fizyczną, np. zamykane pomieszczenia czy alarmy, deklarowano równie często.

## Pozostałe deklarowane zabezpieczenia

Odsetek wszystkich badanych firm




## Stały nadzór zewnętrznej firmy

Odsetek firm danej wielkości

**14 proc.**
Mikrofirmy

**23 proc.**
Małe firmy

**36 proc.**
Średnie przedsiębiorstwa

Monitorowanie wycieków danych w Internecie wskazywała mniej niż jedna piąta firm. Stały nadzór zewnętrznej firmy deklarowano częściej w średnich i małych przedsiębiorstwach niż w mikrofirmach.



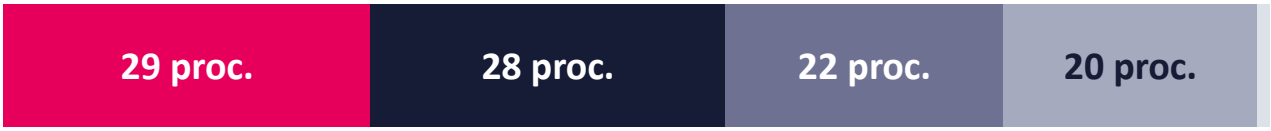
CHRONPESEL.PL
KRAJOWY REJESTR DŁUGÓW
Instytut Prawa Ochrony Danych Osobowych
UNIWERSYTET VIZJA

# Prywatne urządzenia w sprawach służbowych

Korzystanie z prywatnych telefonów lub komputerów na określonych zasadach deklarowano niemal równie często jak pracę wyłącznie na sprzęcie służbowym. Osobną grupę stanowią firmy dopuszczające własne urządzenia tylko w wyjątkowych sytuacjach.

## Zasady korzystania ze sprzętu

Odsetek wszystkich badanych firm




- Z jasnymi zasadami i zabezpieczeniami
- Wyłącznie sprzęt służbowy
- Prywatny sprzęt tylko w wyjątkowych sytuacjach
- Korzystanie bez szczególnych zasad
- Trudno powiedzieć (1 proc.)

Co piąta firma deklarowała korzystanie z prywatnych telefonów lub komputerów bez szczególnych zasad. Zbliżony odsetek dopuszczał własny sprzęt tylko w wyjątkowych sytuacjach.

# Ryzyko i obowiązki przedsiębiorców



KOMENTARZ EKSPERTA

**Maciej Gawroński**
radca prawny, partner zarządzający GP Partners Gawroński, Biernatowski sp. k.

Od dawna uważam, że osiągnięcie całkowitego bezpieczeństwa informatycznego jest praktycznie niemożliwe. Systemy składają się z wielu wzajemnie zależnych warstw, a współczesna działalność wymaga korzystania z globalnej sieci. Wraz z postępującą cyfryzacją przybywa elementów narażonych na cyberatak i powiązań, nad którymi pojedyncza firma nie ma pełnej kontroli.

Zastrzeżenia budzi również podejście unijnego prawodawcy. Przedsiębiorcy mają zapewnić ochronę odpowiednią do ryzyka, a gdy okaże się ona niewystarczająca, muszą liczyć się z karą. Jednocześnie nakłada się na nich liczne obowiązki proceduralne, których realizacja bywa poważnym obciążeniem finansowym dla MŚP. Moim zdaniem lepiej byłoby rozliczać firmy ze skuteczności zabezpieczeń niż wymagać tworzenia rozbudowanej dokumentacji.

Na tym tle RODO oceniam łagodniej. Kluczowe znaczenie ma w nim art. 32, poświęcony bezpieczeństwu przetwarzania. Stosowanie tego przepisu wiąże się jednak w praktyce z analizą ryzyka i rozpoznaniem procesów, w których wykorzystywane są dane osobowe. Znacznie większy problem widzę w obowiązkach nakładanych przez akt o cyberodporności na objęte nim MŚP.

# Technologia i zarządzanie bezpieczeństwem

## Maciej Gawroński — ciąg dalszy komentarza

Przewagą mniejszych przedsiębiorstw jest rzadsze korzystanie ze starszych systemów informatycznych, które trudno aktualizować i dostosowywać do nowych potrzeb. Firmy te często sięgają też po usługi chmurowe. Ich dostawcy dysponują większymi środkami i specjalistyczną wiedzą, a zarazem muszą szczególnie dbać o bezpieczeństwo świadczonych usług. Nawet im zdarzają się jednak poważne awarie. Pokazały to zakłócenia w działaniu platformy Microsoft 365 w pierwszej połowie listopada 2026 r.

Różnorodność środowisk, platform i aplikacji przez długi czas stanowiła dla mniejszych przedsiębiorstw pewną barierę przed cyberatakami. Przestępcy dysponowali ograniczonymi zasobami i kompetencjami, dlatego skupiali się na większych celach. Nie zapewniało to jednak pełnej ochrony. Wśród naszych klientów są firmy, które padły ofiarą ataków hakerskich, w tym wieloetapowych operacji zaplanowanych z myślą o konkretnym przedsiębiorstwie. Dziś sprawcy wykorzystują też sztuczną inteligencję. W tych warunkach główną linią obrony wielu MŚP wciąż pozostaje nadzieja, że zostaną uznane za nieatrakcyjny cel, a przestępcy wybiorą kogoś innego.

Brakuje również jednej uniwersalnej instrukcji technicznej, którą można zastosować w każdym przedsiębiorstwie. Standardy zarządzania wskazują, jakie kwestie należy przeanalizować i jak uporządkować związane z tym zadania. Nie zastępują jednak decyzji o wyborze konkretnych usług, budowie systemów czy nadawaniu uprawnień. Osoby odpowiedzialne za IT w średnich firmach niekiedy reagują niechętnie na propozycje zewnętrznego wsparcia. Obawiają się, że taka współpraca ujawni słabości zabezpieczeń i rzeczywistą skalę wynikających z nich zagrożeń. Luk bywa tak wiele, że trzeba ustalić kolejność ich usuwania.

Mimo tych zastrzeżeń uważam, że warto uzyskać **certyfikat ISO 27001**. Nie daje on gwarancji uniknięcia ataku lub awarii, ale może pomóc ograniczyć ich skutki. W przypadku jednego z naszych klientów pomógł również uniknąć kary administracyjnej.



CHRONPESEL.PL
KRAJOWY REJESTR DŁUGÓW
Instytut Prawa Ochrony Danych Osobowych
UNIWERSYTET VIZJA

# Jak firmy szkolą pracowników?

Przedsiębiorcy częściej deklarowali szkolenia na początku zatrudnienia niż wielokrotny udział pracowników w takich zajęciach. Brak takich działań zgłaszano częściej w mikrofirmach niż w małych i średnich przedsiębiorstwach.

## Szkolenia z ochrony danych osobowych

**45 proc.**

szkolenia na początku zatrudnienia

**36 proc.**

wielokrotne szkolenia w czasie zatrudnienia

**15 proc.**

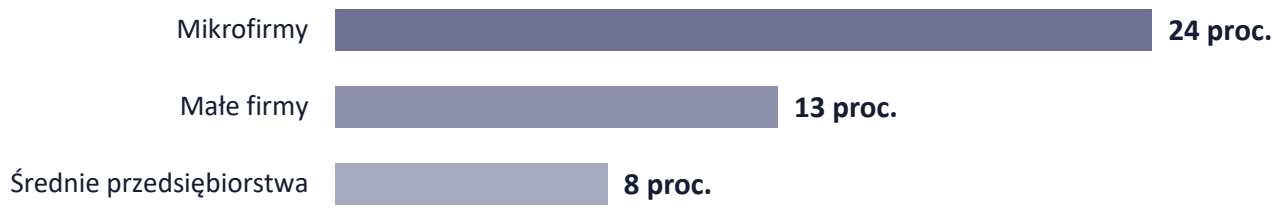
brak szkoleń

**4 proc.**

trudno powiedzieć

## Brak szkoleń według wielkości firmy

Odsetek firm danej wielkości



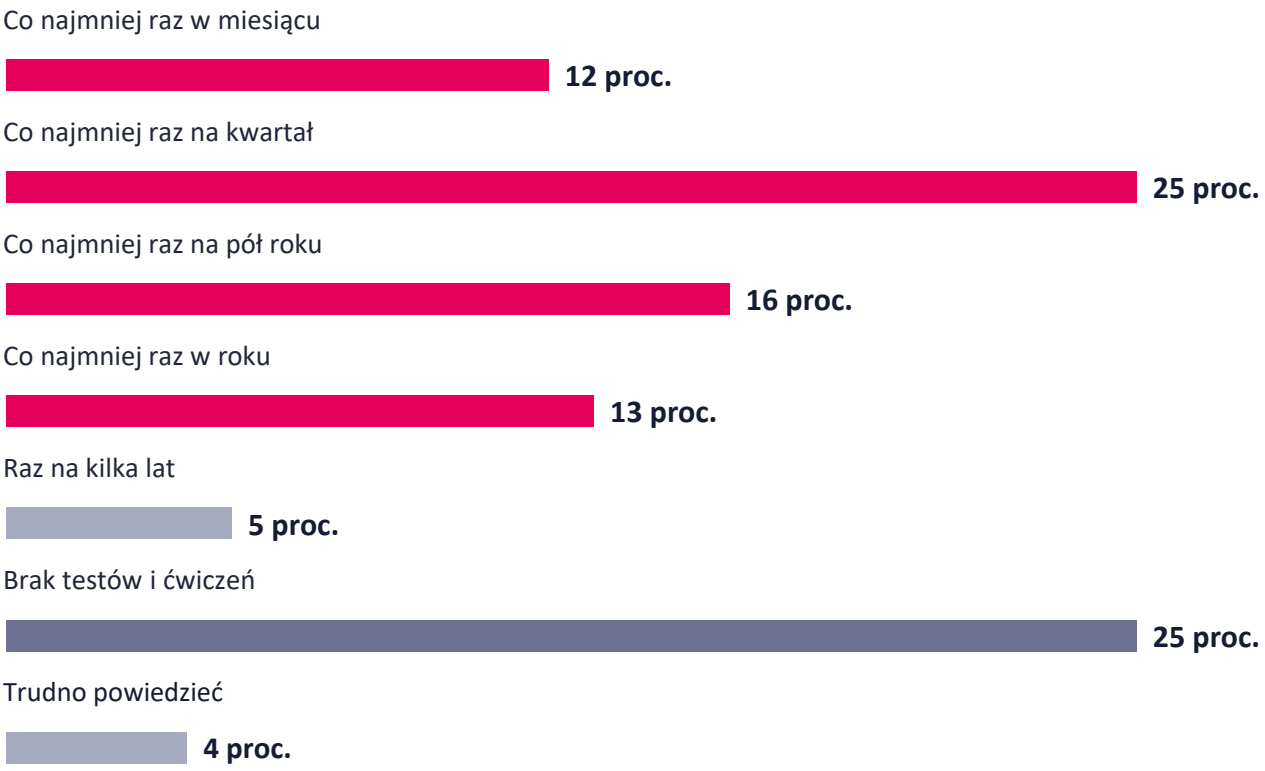

Brak szkoleń deklarowano w mikrofirmach niemal dwukrotnie częściej niż w małych firmach, a w porównaniu ze średnimi przedsiębiorstwami różnica była trzykrotna.

# Czy firmy ćwiczą reagowanie na zagrożenia?

Testy lub ćwiczenia co najmniej raz w roku zadeklarowało 65 proc. badanych firm. Jednocześnie 25 proc. wskazało, że nie przeprowadza ich w ogóle. Brak takich działań częściej deklarowały mikrofirmy niż małe i średnie przedsiębiorstwa.

## Częstotliwość testów i ćwiczeń

Odsetek wszystkich badanych firm




## Brak testów i ćwiczeń

Odsetek firm danej wielkości

**36 proc.**
Mikrofirmy

**26 proc.**
Małe firmy

**13 proc.**
Średnie firmy

Ponad co trzecia firma deklarowała testy lub ćwiczenia co najmniej raz na kwartał.



CHRONPESEL.PL
KRAJOWY REJESTR DŁUGÓW
Instytut Prawa Ochrony Danych Osobowych
UNIWERSYTET VIZJA

# Co trzecia firma ma spisany plan znany pracownikom

Łącznie 32 proc. badanych firm nie ma obecnie planu postępowania na wypadek kradzieży lub wycieku danych. W tej grupie są zarówno przedsiębiorstwa, które zamierzają go opracować, jak i te, które nie wskazały takiego zamiaru.

## Plan na wypadek kradzieży lub wycieku danych

Odsetek wszystkich badanych firm




- Plan jest spisany i znany pracownikom
- Plan ma charakter nieformalny
- Brak planu, ale firma zamierza go opracować
- Brak planu i brak deklaracji jego opracowania
- Trudno powiedzieć (6 proc.)

Pracownik potrzebuje jasnej informacji, komu zgłosić incydent i jakie działania podjąć w pierwszej kolejności. Plan powinien być łatwo dostępny wtedy, gdy trzeba z niego skorzystać.

# Do zasad ochrony danych warto wracać w trakcie zatrudnienia



KOMENTARZ EKSPERTA

**Bartłomiej Drozd,**
ekspert serwisu ChronPESEL.pl

Szkolenie na początku zatrudnienia ma przygotować pracownika do sytuacji, z którymi zetknie się przy wykonywaniu obowiązków. Przykładowo osoba obsługująca zamówienia powinna umieć zweryfikować nietypową prośbę kontrahenta. Przesyłając dokumenty klientów, trzeba wiedzieć, jakie informacje wolno udostępnić. Takie zagadnienia warto omawiać na przykładach z codziennej pracy.

Do zasad ochrony danych trzeba wracać, gdy zmieniają się narzędzia lub sposób wykonywania zadań. Tematem kolejnego spotkania mogą być również wątpliwości zgłaszane przez zespół. Jeśli pracownicy nie wiedzą, jak sprawdzić nadawcę albo komu przekazać podejrzaną wiadomość, warto przećwiczyć właśnie te czynności. W mikrofirmie może to być krótka rozmowa właściciela z pracownikami, zakończona ustaleniem jasnego sposobu działania.

Wiedzę zdobytą podczas szkoleń można sprawdzić w praktyce, wysyłając np. testową wiadomość e-mail od rzekomego kontrahenta z prośbą o zatwierdzenie dokumentów zamówienia w nowym panelu. Ćwiczenie pokaże, czy odbiorca zweryfikuje tę prośbę i zgłosi podejrzaną korespondencję. Wynik podpowie, co wymaga ponownego wyjaśnienia.

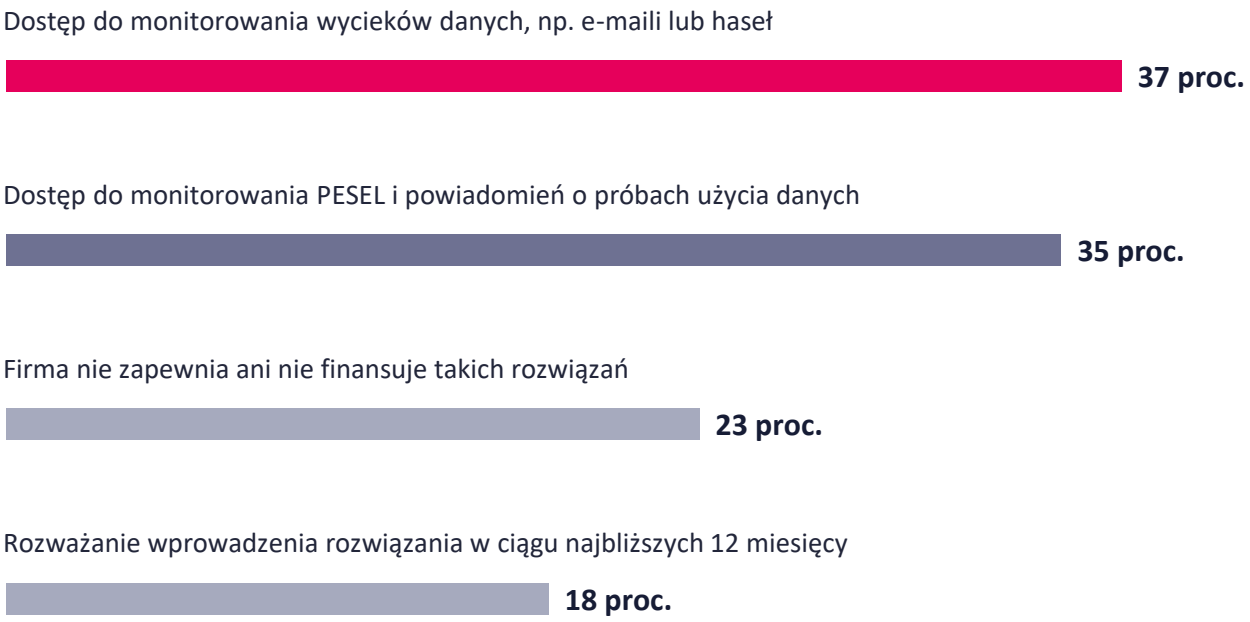
Pracownik musi też wiedzieć, co zrobić po własnej pomyłce, np. po wpisaniu hasła na fałszywej stronie. Powinien od razu przekazać informację osobie, która zajmie się sprawą. W małej firmie może to być właściciel lub obsługujący ją informatyk. W zgłoszeniu warto podać szczegóły zdarzenia, np. jakie informacje pracownik przekazał i czy pobrał plik.

# Jak firmy wspierają ochronę danych pracowników?

Przedsiębiorcy częściej deklarowali zapewnianie pracownikom dostępu do monitorowania wycieków danych, np. adresów e-mail lub haseł, niż do monitorowania numeru PESEL. Pracodawca może opłacać taką usługę w całości lub pokrywać część kosztów korzystania z niej.

## Wybrane formy wsparcia

Odsetek wszystkich badanych firm




## Dostęp do monitorowania wycieków danych

Odsetek firm danej wielkości

**27 proc.**
Mikrofirmy

**36 proc.**
Małe firmy

**48 proc.**
Średnie firmy

Dostęp do monitorowania wycieków deklarowano częściej wraz ze wzrostem wielkości firmy. W średnich przedsiębiorstwach odsetek ten był o 21 punktów procentowych wyższy niż w mikrofirmach.

# Większość firm przekazuje dane podmiotom zewnętrznym

Obsługa księgowości, kadr czy innych zadań może wymagać przekazywania partnerom informacji o pracownikach lub klientach. Przedsiębiorcy deklarowali różne formy takiej współpracy: z jednym odbiorcą, z kilkoma podmiotami lub tylko w wyjątkowych sytuacjach.

**80 proc.** firm przekazuje dane pracowników lub klientów podmiotom zewnętrznym

## Przekazywanie danych podmiotom zewnętrznym

Odsetek wszystkich badanych firm




- Regularnie kilku podmiotom zewnętrznym
- Jednemu podmiotowi zewnętrznemu
- Sporadycznie, w wyjątkowych sytuacjach
- Dane przetwarzane wyłącznie wewnątrz firmy
- Trudno powiedzieć (3 proc.)

Najliczniejszą grupę stanowią firmy przekazujące dane jednemu partnerowi. Taki model współpracy deklarowano prawie dwa razy częściej niż sporadyczne udostępnianie informacji.

# Czy przedsiębiorcy obawiają się naruszeń u partnerów?

Ponad połowa przedsiębiorców przekazujących dane partnerom zewnętrznym obawia się ich naruszenia. Częściej deklarowano przy tym odpowiedź „raczej tak” niż „zdecydowanie tak”.

**52 proc.**
Obawia się naruszenia

**27 proc.**
Nie wyraża obaw

**21 proc.**
Trudno powiedzieć

## Obawy o naruszenie danych u partnerów

Odsetek firm przekazujących dane podmiotom zewnętrznym




- Zdecydowanie tak
- Raczej tak
- Trudno powiedzieć
- Raczej nie
- Zdecydowanie nie (1 proc.)

Obawy deklarowano niemal dwa razy częściej niż ich brak. Odpowiedzi negatywne to przede wszystkim „raczej nie”, a zdecydowane „nie” należało do rzadkości.

# Ochrona danych we współpracy z dostawcami



KOMENTARZ EKSPERTA

**Jakub Groszkowski**
zastępca prezesa UODO
w latach 2022–2024,
honorowy prezes Instytutu Prawa
Ochrony Danych Osobowych

Ochrona danych osobowych zaczyna się od ustalenia roli firmy oraz celu i podstawy prawnej ich przetwarzania. Trzeba też określić, jakie informacje posiada przedsiębiorstwo, komu je udostępnia i kiedy je usuwa. Stosowane zabezpieczenia techniczne i organizacyjne powinny odpowiadać ryzyku dla osób, których dane dotyczą, a ich skuteczność należy regularnie sprawdzać. Jeżeli dostawca usług przetwarza dane w imieniu naszej firmy, mamy obowiązek zweryfikować, czy zapewnia odpowiednie gwarancje ich ochrony, oraz zawrzeć właściwą umowę powierzenia. Jej podpisanie nie kończy jednak obowiązków administratora ani podmiotu przetwarzającego. O bezpieczeństwo informacji trzeba dbać stale.

Małe firmy mogą dzięki usługom chmurowym uzyskać dostęp do zaawansowanych zabezpieczeń, a za pomocą sztucznej inteligencji usprawnić obsługę zapytań i analizę dokumentów. Przed wdrożeniem warto ustalić, gdzie dostawca przetwarza dane i czy wykorzystuje przesłane treści do trenowania modeli. Firma powinna też określić, z jakich narzędzi wolno korzystać, co można do nich wprowadzać i kto sprawdza wyniki. AI ułatwia jednak także tworzenie przekonujących wiadomości phishingowych i podrabianie głosu. Dlatego zachowujmy szczególną ostrożność i pamiętajmy o podstawowych zasadach cyberhigieny.

# Autorzy raportu i patroni

## Autorzy raportu

CHRONPESEL.PL

Serwis wspiera ochronę danych osobowych i pomaga ograniczać ryzyko kradzieży tożsamości oraz wyłudzeń. Powiadamia o sprawdzeniu numeru PESEL w bazie KRD oraz umożliwia monitorowanie wycieków danych w Internecie. Prowadzi również działania edukacyjne o aktualnych zagrożeniach i zasadach bezpiecznego korzystania z danych osobowych.

KRAJOWY REJESTR DŁUGÓW www.krd.pl

Najstarsze w Polsce biuro informacji gospodarczej, działające od 2003 roku i należące do Kaczmarski Group. Udostępnia informacje o sytuacji płatniczej firm i konsumentów oraz narzędzia wspierające ocenę wiarygodności kontrahentów. Pomaga przedsiębiorcom ograniczać ryzyko niezapłaconych faktur i podejmować decyzje o współpracy. Z jego usług korzystają firmy różnej wielkości.

## Patroni

IPODO
Instytut Prawa Ochrony Danych Osobowych

Instytut upowszechnia wiedzę o prawie ochrony danych i promuje dobre praktyki przetwarzania informacji. Prowadzi badania i publikuje raporty. Zajmuje się też edukacją oraz doradztwem dla przedsiębiorstw i instytucji. Skupia ekspertów, praktyków i naukowców, uczestnicząc w pracach nad regulacjami i rozwiązaniami służącymi ochronie prywatności.

UNIWERSYTET VIZJA

Niepubliczna uczelnia akademicka w Warszawie, działająca od 2001 roku. Kształci studentów m.in. w dziedzinie prawa, ekonomii, psychologii i informatyki, łącząc dydaktykę z badaniami naukowymi. Rozwija współpracę z biznesem i partnerami zagranicznymi oraz wspiera inicjatywy społeczne. W jej strukturze działa Instytut Prawa Ochrony Danych Osobowych.