NASK thinkstat

E-transformacja i bezpieczeństwo cyfrowe w polskich przedsiębiorstwach

NASK thinkstat

Dział Badań Rynku i Opinii

Redakcja:

Rafał Lange

Zespół badawczy:

Filip Konopczyński
Mariola Kowalczyk
Karol Leszczyński
Agnieszka Ładna

Opracowanie graficzne:

Tomasz Szladowski
Piotr Klicki
Agnieszka Malinowska

ISBN: 978-83-65448-29-3

NASK Państwowy Instytut Badawczy
Warszawa 2021

Spis treści

Wstęp

Wraz ze wzrostem roli Internetu w obrocie społeczno-gospodarczym zwiększyła się skala ryzyka związanego z bezpieczeństwem informacji, które przy okazji dokonywania transakcji wymieniają między sobą przedsiębiorcy, klienci i inni uczestnicy obrotu gospodarczego. Obok różnorakich korzyści cyfryzacja gospodarki generuje także nowe zagrożenia w zakresie cyberbezpieczeństwa.

Według Głównego Urzędu Statystycznego[1] w 2018 dostęp do szerokopasmowego Internetu posiadało 85,7% przedsiębiorstw w Polsce. W przeprowadzonym przez Polski Instytut Ekonomiczny pod koniec 2019 r. sondażu, aż 88% przedstawicieli polskiego biznesu zadeklarowało, że ich firma wykorzystuje nowoczesne technologie w stopniu średnim lub wysokim[2]. Z urządzeń przenośnych (smartfony, tablety) korzysta ponad 75%, a z podłączonych do sieci komputerów 40% pracowników. W kontekście wysokiego poziomu nasycenia technologiami informacyjnymi w społeczeństwie (86,7% gospodarstw domowych posiada dostęp do szybkiej sieci) nie jest przesadą stwierdzenie, że cyfrowa transformacja w polskiej gospodarce już się dokonała.

Nie oznacza to jednak, że jej efekty rozkładają się równomiernie. Nowoczesne technologie w stopniu wysokim wykorzystuje 69% dużych, 52% średnich, 50% małych i tylko 37% mikro firm[3]. Należy pamiętać, że w Polsce sektor MMŚP stanowi ponad 99,8% wszystkich firm[4]. W 2018r. specjalistów Technologii Informacyjno-Komputerowych zatrudniało 81% dużych, 40% średnich i tylko 18% małych polskich firm . Porównanie stanu zatrudnienia w przedsiębiorstwach różnej wielkości wskazuje, że tylko najwięksi rynkowi gracze mogą pozwolić sobie na zatrudnienie odpowiedniej liczby specjalistów odpowiedzialnych za efektywność i bezpieczeństwo infrastruktury telekomunikacyjnej.

Zagrożenia dla cyberbezpieczeństwa powodują potencjalne problemy zarówno dla przedsiębiorstw jak i ich klientów. Narażenie m.in. na ataki hakerskie, utratę danych, wyłudzenia pieniędzy czy naruszenia dobrego imienia bądź wizerunku zmniejszają efektywność i pewność obrotu gospodarczego. Cyberataki powodują nie tylko wymierne straty ekonomiczne, ale także obniżenie społecznego zaufania do instytucji publicznych odpowiadających za sprawne i bezpieczne funkcjonowanie polskiej gospodarki.

Z powyższych powodów diagnoza stanu przygotowania, kompetencji, świadomości oraz postaw przedstawicieli polskiego biznesu ma strategiczne znaczenie dla rozwoju gospodarczego Polski w ciągu najbliższej dekady. Cyfrowe zabezpieczenia w polskich firmach są przedmiotem badań przede wszystkim firm z sektora prywatnego[5] i charakteryzują się stosunkowo niedużymi populacjami badawczymi. Zróżnicowanie i rozdrobnienie polskiej przedsiębiorczości powoduje uzasadnione wątpliwości natury statystycznej oraz metodologicznej i każe stawiać pytania o wiarygodność i reprezentatywność dostępnych informacji.

Zespół badawczy Thinkstat - Działu Badań Rynku i Opinii NASK Państwowego Instytutu Badawczego przygotował projekt ogólnopolskiego badania poświęconego cyberbezpieczeństwu w polskich przedsiębiorstwach. Celem ewaluacji wypracowanej metodologii w marcu 2020 r. zrealizowane zostało badanie pilotażowe pt. „E-transformacja i bezpieczeństwo cyfrowe w polskich przedsiębiorstwach". Składało się ono z dwóch komponentów: ilościowego (kwestionariusz ankiety) oraz jakościowego (wywiady pogłębione). Objęto nim populację badawczą liczącą 120 (n=120) w przypadku badania ilościowego oraz 12 (n=12) w odniesieniu do badania jakościowego, przedsiębiorców z województw: podlaskiego, wielkopolskiego i lubelskiego. Wyniki badania zostały poddane analizie statystycznej, a rezultaty zaprezentowane w formie poniższego raportu.

1 Wegner M., Gumiński M., Huet M., Jacykowska M., Juszczak K., Kwiatkowska M., Mordan P., Orczykowska M., Społeczeństwo informacyjne w Polsce Wyniki badań statystycznych z lat 2015–2019, 2019, Główny Urząd Statystyczny, 2020.
2 Dębkowska K., Kłosiewicz-Górecka U., Leśniewicz F., Szymańska A, Święcicki I., Ważniewski P., Zybertowicz K., Nowoczesne technologie w przedsiębiorstwach przed, w trakcie i po pandemii COVID-19, Polski Instytut Ekonomiczny 2020 r.
3 Idem.
4 Zakrzewski R., Skowrońska A., Chaber P., Łapiński J., Nieć M., Orlowska J., Widła-Domaradzki Ł., Domaradzka A., Raport o stanie sektora małych i średnich przedsiębiorstw w Polsce , Polska Agencja Rozwoju Przedsiębiorczości, 2019 r.
5 Zob. m. in. Kurek M., Staniek Ł., Strzałek M., Maruszczak M., Barometr cyberbezpieczeństwa, KPMG 2020, Sieńko A., Urban P., Sawiak T., Gęborys P., Sobczyk S., Cyber-uletka po polsku. Dlaczego firmy w walce z cyberprzestępcami liczą na szczęście, PWC 2018, Sondaż Computerworld.pl opublikowany 25.03.2020.

Najważniejsze ustalenia

- Przedstawiciele małych firm najbardziej boją się włamań i kradzieży z elektronicznego konta bankowego lub innych oszustw finansowych. W mniejszym stopniu także kradzieży tożsamości (osoby lub firmy) lub włamania na profile społecznościowe.
- Prawie 2/3 polskich małych przedsiębiorców deklaruje, że w ich firmie w ciągu 12 miesięcy poprzedzających badanie nie było incydentów w zakresie cyberbezpieczeństwa. Wśród podmiotów, w których miały one miejsce przeważnie powodowały one spowolnienie w produkcji, świadczeniu usług, uszkodzenie oprogramowania w firmie, czy problem z komunikacją elektroniczną. Jedynie co trzeci badany wskazał, że podatność na cyberzagrożenia to przede wszystkim wina pracowników.
- Głównym kryterium inwestowania w rozwiązania oparte na technologiach informacyjnych w polskich mikro, małych i średnich firmach jest potrzeba podniesienia konkurencyjności (60,2%). Kolejnymi powodami wydatkowania na ten cel, jest według małych i średnich przedsiębiorstw potrzeba optymalizacji czasu (43,5%), potrzeba poprawy wizerunku firmy (38,9%) oraz zmniejszenie kosztów w firmie (36,1%).
- W aż 3/4 firm nie ma, bądź respondent nie zna, planów inwestycji w cyberbezpieczeństwo. W przypadku wyboru usługi z zakresu cyberbezpieczeństwa dominuje kryterium ceny (prawie 70%), a kwestia ewentualnej skuteczności jest priorytetowa jedynie dla co trzeciego badanego.
- Wiedzę o cyberbezpieczeństwie ponad połowa badanych czerpie z ogólnodostępnych portali informacyjnych, co czwarty z mediów społecznościowych, a co piąty z telewizji.
- Dodatkowo, według ankietowanych, z prawie 4/5 firm, osoby odpowiedzialne za bezpieczeństwo informatyczne nie uczestniczą w szkoleniach z zakresu cyberbezpieczeństwa.
- Zdecydowana większość (83%) firm nie miała przeprowadzonego audytu bezpieczeństwa informatycznego, a także nie wdrożyła w ciągu ostatnich 12 miesięcy nowych rozwiązań w tym obszarze. Aż 3/4 badanych deklaruje, że w ich firmie nie ma dokumentu określającego politykę cyberbezpieczeństwa, a połowa, że ich firma nie realizuje obowiązków wynikających z krajowej strategii cyberbezpieczeństwa.

Implementacja technologii cyfrowych

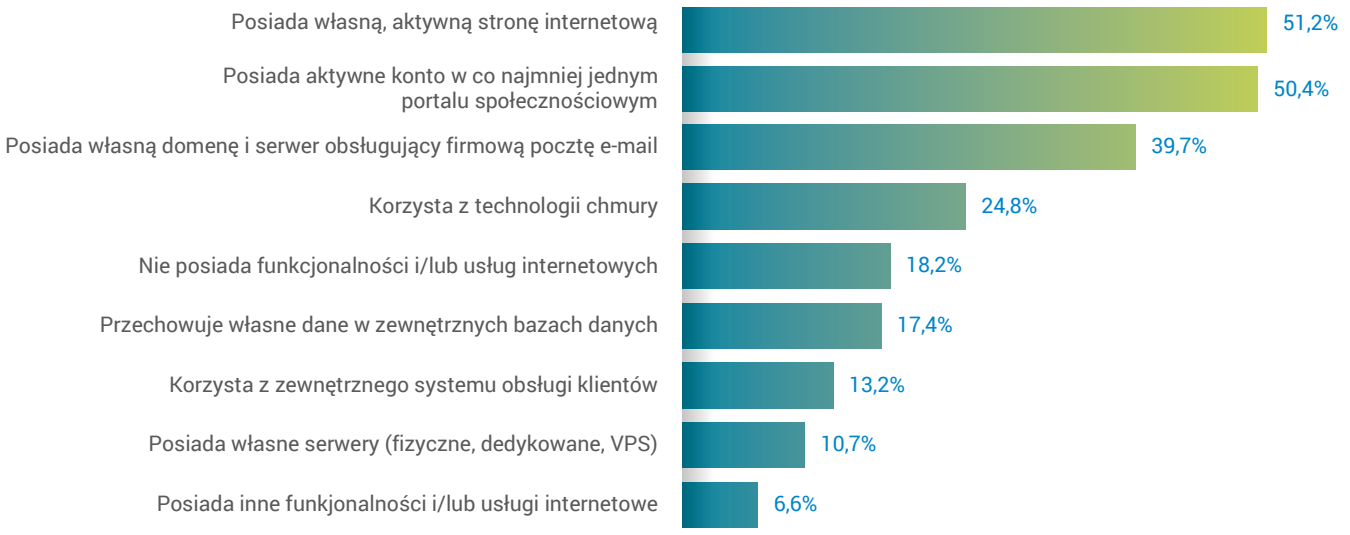
Implementacja technologii cyfrowych

Całościowa diagnoza stanu bezpieczeństwa informacyjnego musi uwzględniać podstawowe parametry wpływające na ogólny poziom cyfryzacji przedsiębiorstwa. Szybki rozwój technologii informacyjnych i komputerowych w ostatnich dekadach sprawił, że coraz więcej firm korzysta z możliwości, które oferuje, w obszarach takich jak m.in. logistyka produkcji i zamówień, budowanie wizerunku i marketing, optymalizacja warunków i kultury pracy czy komunikacji z klientami bądź partnerami. Stopień, w którym działalność firmy opiera się na infrastrukturze teleinformatycznej zależy m.in. od branży, świadomości osób kierujących firmą oraz jej klientów. W innej sytuacji jest np. firma budowlana, która wykorzystuje rozwiązania informacyjno-komunikacyjne w stopniu znikomym, a w innej bazujący na innowacjach start-up, od początku pomyślany jako firma transgraniczna i skalowalna. W celu oszacowania poziomu "zanurzenia" przedsiębiorstw w nową, cyfrową rzeczywistość, respondenci zostali poproszeni o odpowiedź na szereg pytań dotyczących faktycznego zastosowania technologii ICT w ich działalności

Internet spowodował, że przedsiębiorcy funkcjonują w nowej rzeczywistości, oznaczającej pojawienie się min.: nowych modeli biznesowych, ale też nowych wymagań formalnych, które trzeba realizować za pomocą sieci. Internetowe narzędzia warunkują funkcjonowanie firmy w wielu obszarach, dlatego istotne jest określenie zakresu korzystania z nowego medium.

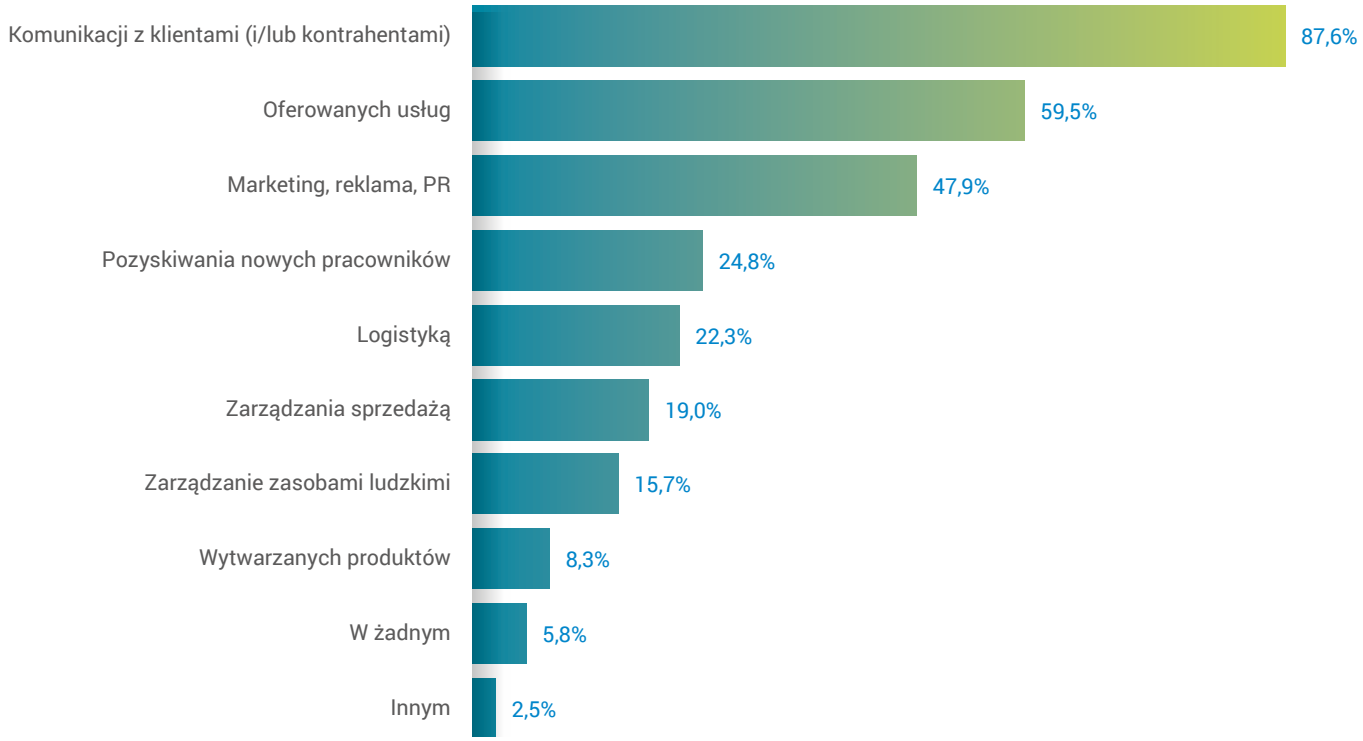
Ponad połowa ankietowanych wskazuje, że posiada własną stronę internetową (51,2%) oraz aktywne konto na co najmniej jednym z portali społecznościowych (50,4%). Znaczna część respondentów wskazuje, że posiada własną domenę i serwer, które obsługują ich firmową pocztę (39,7%), a co czwarty zapytany twierdzi, że firma korzysta w ramach swojej działalności z technologii chmury (24,8%). Wyniki badania wskazują na nieco mniejszą popularność zewnętrznych baz danych (17,4%) oraz zewnętrznych systemów obsługi klientów (13,2%). Zastanawiający jest stosunkowo wysoki wskaźnik braku wykorzystywania internetowych funkcjonalności czy usług. Niemal co piąte (18,2%) mikro i małe przedsiębiorstwo twierdzi, że nie korzysta z nowych technologii, nawet w podstawowym zakresie. Tłumaczyć to mogą odpowiedzi z pogłębionych wywiadów, wskazujące na to, że przedsiębiorstwa najczęściej opierają się na najbardziej dostępnych narzędziach on-line i traktują pocztę e-mail jako podstawę działania biznesowego. Bez względu na formę i obszar działalności, skrzynka pocztowa pełni rolę „komunikatora w biznesie" i służy do realizacji zobowiązań urzędowych, a przede wszystkim do kontaktu z księgową. Mimo, że najczęściej to firmowa strona internetowa uważna jest za niezbędną, bo uwiarygodnia firmę i stanowi jej wizytówkę, to wyniki badania potwierdzają wzrost popularności mediów społecznościowych. Serwisy te stale rozwijają swoje funkcjonalności i pozwalają zastąpić dotychczasowe, statyczne strony internetowe, interaktywnymi kontami. O popularności tego typu serwisów decydują nie tylko niskie wymagania w zakresie kompetencji niezbędnych do tworzenia profilu, ale też gwarancja zasięgu.

Wykres 1. Rozkład procentowy odpowiedzi na pytanie: „Czy przedsiębiorstwo:..?"



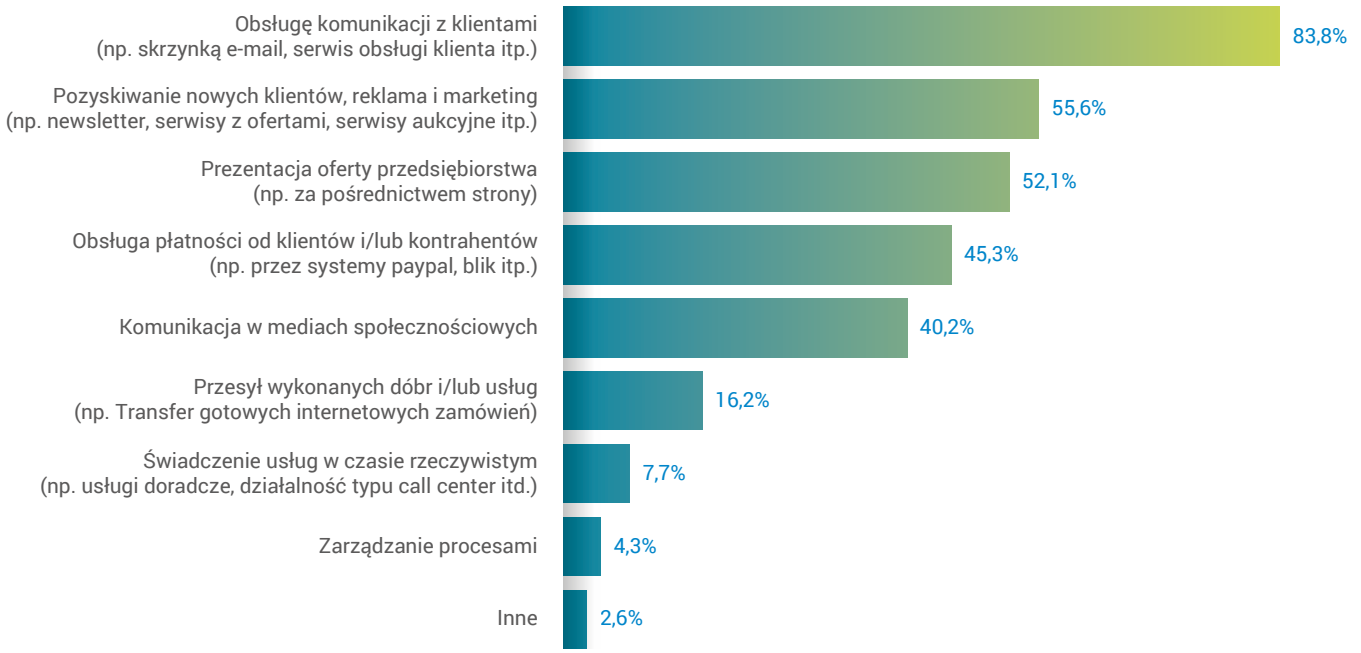
Najczęściej przedsiębiorcy wykorzystują sieć do komunikacji z klientami i kontrahentami (87,6%) oraz do oferowania usług (59,5%) i reklamy (47,9%). Wyniki te wskazują na trend praktycznych zastosowań w biznesie, który jest dominujący w zoptymalizowanym pod względem ponoszonych nakładów finansowych środowisku. Z jednej strony konieczność utrzymania się na rynku i dostosowania do jego wymogów (również technologicznych), z drugiej osiągnięcie tego jak najmniejszym nakładem, gwarantuje dodatni wynik rachunku zysków i strat. Niewątpliwie bez komunikacji internetowej funkcjonowanie nawet najmniejszych firm jest praktycznie niemożliwe. Komunikacja za pomocą internetu jest nie tylko wygodna, ale przede wszystkim nie wymaga dodatkowych nakładów finansowych (darmowa poczta e-mail, darmowe komunikatory, itp.). Wskazania na sieć jako kanał sprzedaży usług i towarów są odzwierciedleniem zmieniającej się rzeczywistości w takich branżach jak handel (który funkcjonuje często w modelu łączonym: handel stacjonarny plus handel on-line). Poza umożliwieniem realizacji wymagań proceduralno-administracyjnych, nowe media oferują nowe możliwości , polegające na niespotykanym w erze analogowej zasięgu i dostępie do potencjalnych klientów. Dodatkowym atutem jest wszechobecność Internetu i malejące ceny urządzeń oraz usług pozwalających na korzystanie z sieci. Wiąże się to z rozwojem kompetencji w zakresie wykorzystywania nowych technologii. Firmy zyskują możliwość powielania rozwiązań stosowanych przez innych, którzy funkcjonują w sieci. Co czwarte przedsiębiorstwo wskazało, że internet pomaga im w poszukiwaniu nowej kadry (24,8%), nieco mniej, że wspiera rozwiązania logistyczne (22,3%) oraz wspomaga zarządzanie sprzedażą (19,0%). Niski wynik dla rozwiązań handlowych jest odzwierciedleniem różnorodności w populacji badawczej, w której znalazły się różne branże. Mimo, że oferowanie usług najczęściej realizuje się również za pośrednictwem internetu, to zarządzanie sprzedażą jest bardziej złożonym procesem i wymaga większych nakładów (np.: zakup specjalnego oprogramowania, serwisowanie tego oprogramowania, szkolenia itp.) stąd mniej wskazań dla tej odpowiedzi.

Wykres 2. W jakim obszarze najczęściej wykorzystywany jest internet w Pana(i) firmie?



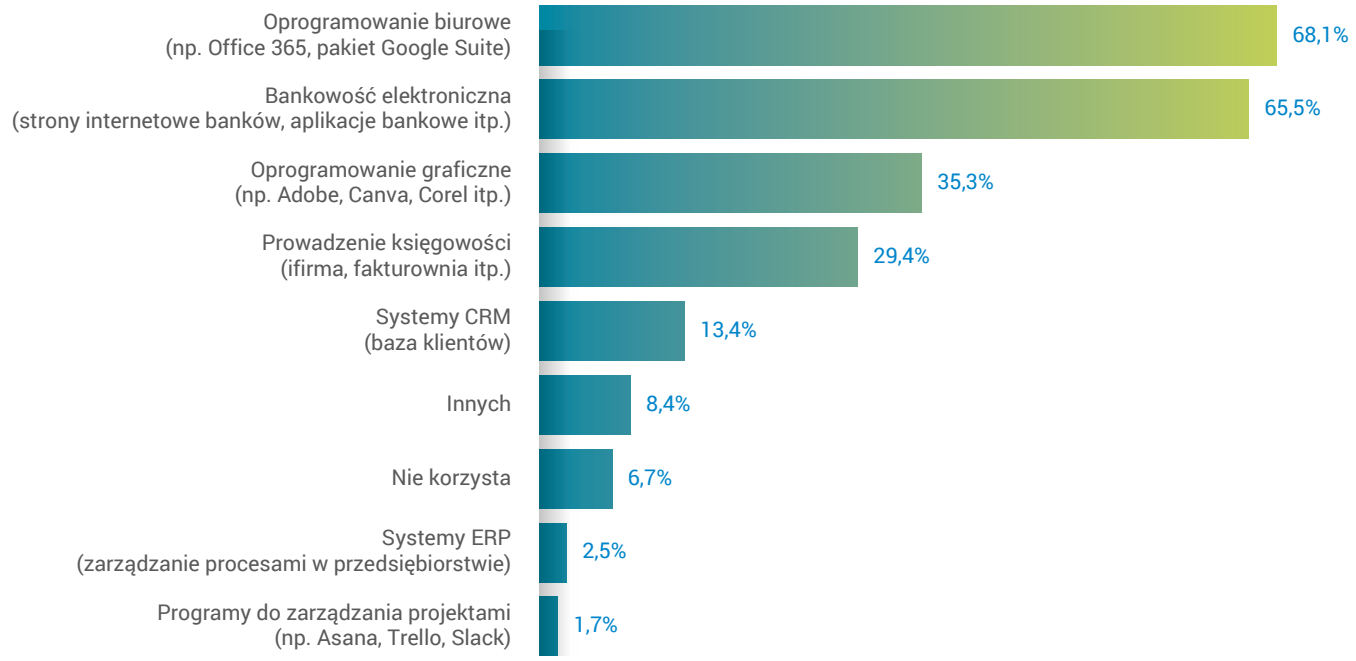
Redukcja kosztów własnych poprzez min.: zoptymalizowanie przestrzeni magazynowej, wyeliminowanie ograniczeń lokalizacyjnych czy całodobową obsługę klienta, to tylko niektóre spośród wielu możliwości jakie daje internet firmom w XXI wieku. Spośród tych opcji, przedsiębiorcy najchętniej korzystają ze skrzynki e-mail oraz serwisów do obsługi klientów (83,8%). Analogicznie do wskazanych obszarów „usieciowienia", ponad połowa ankietowanych poświadcza, że cyfrowe narzędzia pozwalają im na pozyskiwanie nowych klientów i reklamę (55,6%) oraz prezentowanie swojej oferty (52,1%). Powszechne jest też zastosowanie e-usług bankowych i obsługa płatności w firmie (45,3%) oraz komunikacja w mediach społecznościowych (40,2%). Rzadziej wśród ankietowanych firm, nowe technologie wspomagają takie procesy jak: „Przesył wykonywanych dóbr i usług" (16,2%) oraz „Świadczenie usług w czasie rzeczywistym" (7,7%). Dane wskazują na to, że mikro- przedsiębiorcy traktują internet jako niezbędne narzędzie do komunikacji. Odpowiedzi korelują z coraz powszechniejszym wykorzystaniem portali społecznościowych, które stale rozbudowują swoją formułę i dają możliwość skoncentrowania uwagi innych bez konieczności ponoszenia dodatkowych kosztów. Liczebność użytkowników mediów społecznościowych, łatwość obsługi konta na portalu, interaktywne komunikatory i swobodne aktualizacje zamieszczanych treści są niewątpliwym atutem do komercyjnego wykorzystania.

Wykres 3. Jakie usługi i/lub funkcje są realizowane w Pana(i) przedsiębiorstwie za pośrednictwem internetu?



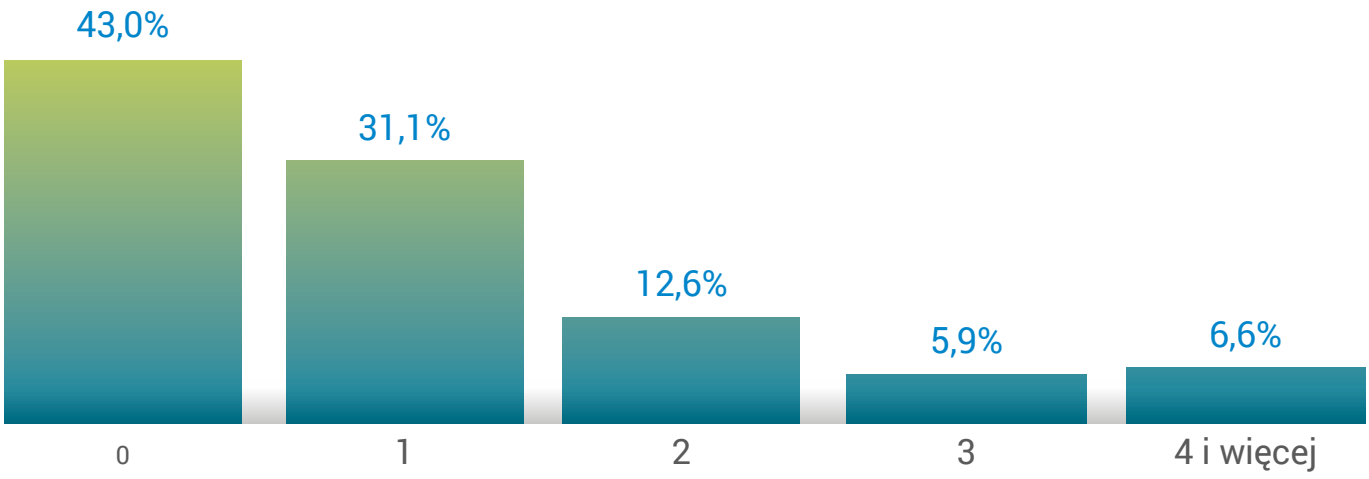
Liczba narzędzi internetowych stale rośnie, również tych wspierających biznes. Firmy mogą wybierać te usprawnienia, które są najbardziej dostosowane do profilu ich działalności i potrzeb. Wśród zapytanych, większość wskazywała na podstawowe oprogramowania biurowe typu: Office 365 czy pakiet Google (68,1%). Prawie tyle samo wskazań odnotowano przy e-bankowości (65,5%), która zdecydowanie ułatwia funkcjonowanie i transfer środków finansowych. Więcej niż co trzecie przedsiębiorstwo (35,3%) korzysta z oprogramowania graficznego takiego jak Adobe czy Canva i niemal tyle samo z księgowości prowadzonej on-line (29,4%). Niewiele ponad 10% przedsiębiorstw wykorzystuje bazy klientów, tzw. systemy CMR (13,4%) oraz pozostałe narzędzia. Dane z pilotażu wskazują na niesłabnącą popularność tradycyjnych narzędzi internetowych. Uzasadnieniem tej popularności może być dostępność, łatwość w obsłudze, niska cena i przede wszystkim gwarancja spełnienia niezbędnego minimum wymogów dyktowanych przez cyfrową teraźniejszość. Podstawowe narzędzia są nie tylko powszechnie znane i stosowane, ale przede wszystkim dają możliwość swobodnego transferu dokumentów i innych treści w edytowalnych formatach. Drugim obszarem aktywności przedsiębiorstw są transakcje finansowe. Jest to jedna z podstawowych czynności biznesowych, które w zdecydowanej większości realizowane są on-line. Gotówkowe rozliczenia są nie tylko obarczone dodatkowym ryzykiem, ale przede wszystkim ograniczone nałożonymi limitami związanymi z prawem podatkowym i sprawozdawczością finansową. Coraz powszechniejsze stały się usługi księgowe realizowane przez internet, choć znaczna część tych najmniejszych firm woli bezpośredni kontakt z księgową, która często pełni również rolę specjalisty finansowo-kadrowego.

Wykres 4. Z jakich narzędzi online korzysta się w Pana(i) przedsiębiorstwie w codziennej działalności?



Specjaliści IT, odpowiadający za tworzenie i obsługę programów informatycznych, są szczególnie cenieni i poszukiwani na rynku pracy. Standardowe zadania na takim stanowisku, poza implementacją narzędzi informatycznych, to monitorowanie poprawności działania systemu, dbanie o cyberbezpieczeństwo oraz nadzór i wsparcie użytkowników. Osoby odpowiedzialne za ten obszar powinny posiadać nie tylko kompetencje uprawniające do korzystania z narzędzi informatycznych, ale też do tworzenia procedur czy raportów. „Mikro" i „mali" przedsiębiorcy najczęściej nie zatrudniają nikogo na takim stanowisku (43,0%), a mniej niż 1/3 wskazuje, że w firmie jest jeden taki pracownik (31,1%). Tylko nieliczni podają, że w firmie odpowiedzialność ta jest scedowana na 2 osoby (12,6%) lub więcej. W zasadzie potrzeby mikro przedsiębiorców zawężają się do powszechnie stosowanych narzędzi, dlatego dodatkowe inwestycje wydają się im zbędne.

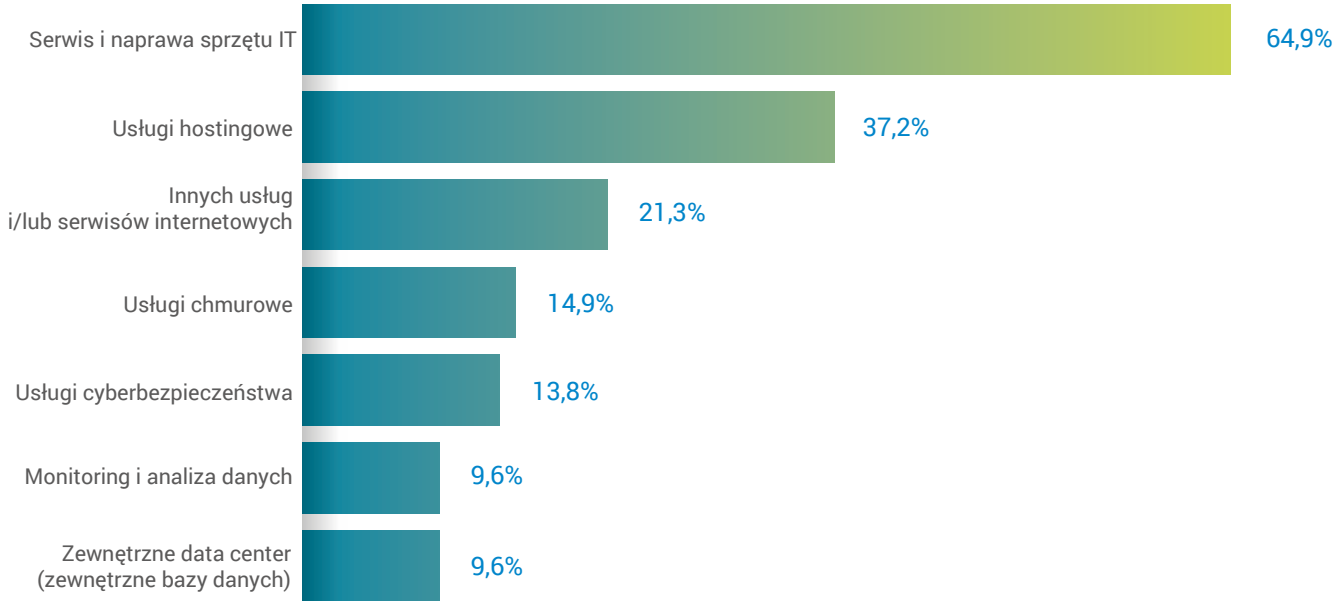
Wykres 5. Ilu pracowników w Pana(i) przedsiębiorstwie odpowiada za tworzenie i/lub obsługę programów lub systemów informacyjnych (programiści, informatycy, specjaliści od cyberbezpieczeństwa itp.)?



Outsourcing zadań teleinformatycznych, polegający na zaangażowaniu zewnętrznej firmy min. w codzienne wsparcie użytkowników IT (helpdesk), pomoc w zakupie sprzętu czy administrowanie sieci i serwerów, stale zyskuje na popularności. Koszt finansowy takiej operacji jest wprost proporcjonalny do zapotrzebowania rynku na takie usługi i jak wynika z danych z badania, zdecydowanie przekracza skromne budżety mniejszych firm. Deklaracje świadczą o tym, że w sektorze o niskim wskaźniku zatrudnienia korzysta się z zewnętrznych usług przede wszystkim wtedy, kiedy zachodzi potrzeba serwisu bądź naprawy sprzętu IT (64,9%). Korzystanie z zewnętrznych usług hostingowych potwierdza prawie 40% respondentów (37,2%). Co piąty respondent wskazał na korzystanie z innych usług lub serwisów (21,3%), zaś „Usługi chmurowe" i „Usługi cyberbezpieczeństwa" były zaznaczane zdecydowanie rzadziej (kolejno: 14,9% i 13,8%).

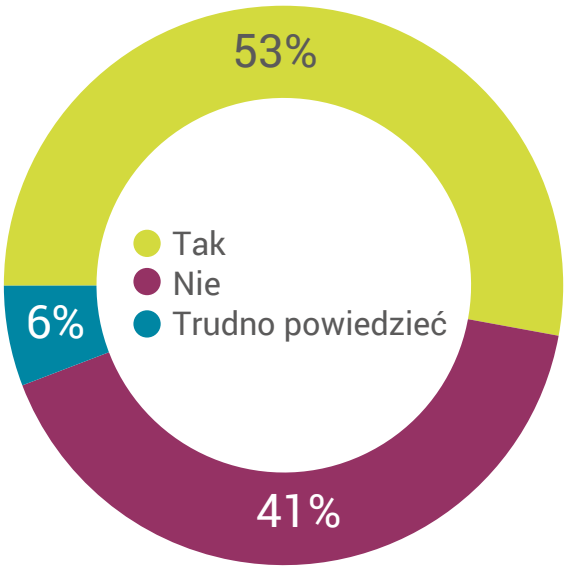
Wyniki potwierdzają konieczność racjonalizowania wydatków na nowe technologie w biznesie. Mniejsze firmy, które nie stosują rozbudowanych systemów do zarządzania, ograniczają się do reagowania na problemy i stosowania podstawowych serwisów sprzętowych ze względów ekonomicznych. Z wywiadów pogłębionych wynika, że najczęściej właściciele małych firm nie widzą potrzeby zapobiegania zagrożeniom i wolą inwestować np.: w podstawowe zasoby sprzętowe i utrzymanie niezbędnej infrastruktury IT niż prognozować i zapobiegać zagrożeniom.

Wykres 6. Czy Pana(i) przedsiębiorstwo korzysta z usług zewnętrznych firm w zakresie..?



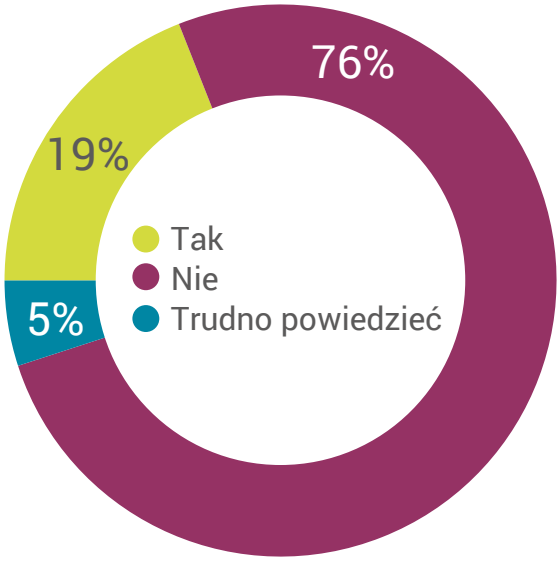
„RODO" pojawiło się jako nowa forma ochrony danych osobowych i jest regulacją dotyczącą dystrybucji i przetwarzania tych danych. W ostatnim czasie jest też popularnym tematem wielu szkoleń i poradników dla przedsiębiorców. Z jednej strony wzbudza niepokój przed karami za niedostosowanie się do nakładanych regulacji, a z drugiej powoduje wiele wątpliwości interpretacyjnych co do zasadności takich regulacji. Z tego powodu duże firmy inwestują w rozbudowane systemy ochrony danych osobowych. Odpowiedzi na pytanie o stosowanie się do rozporządzenia dotyczącego gromadzenia i przetwarzania danych adresowych i osobowych rozkładają się bardzo równomiernie. Niewiele więcej jak połowa zapytanych odpowiedziała „Tak" (52,9%) i niewiele mniej wskazało na „Nie" (41,3%). Rozporządzenie nazywa administratorem danych osobowych każdego przedsiębiorcę, wykorzystującego dane osób fizycznych, które pozwalają na ich identyfikację i nakłada obowiązek stosowania się do wskazanych zasad. W wywiadach właściciele firm, którzy udzielili odpowiedzi twierdzącej, uważają, że stosują się do RODO jak do wszystkich regulacji. Ci, którzy udzielili odpowiedzi przeczącej, często nie mają świadomości, że rozporządzenie dotyczy także małych firm.

Wykres 7. Czy Pana(i) przedsiębiorstwo samodzielnie gromadzi i/lub przetwarza dane teleadresowe (telefon, adres e- mail) osobowe klientów i/lub kontrahentów (RODO)?



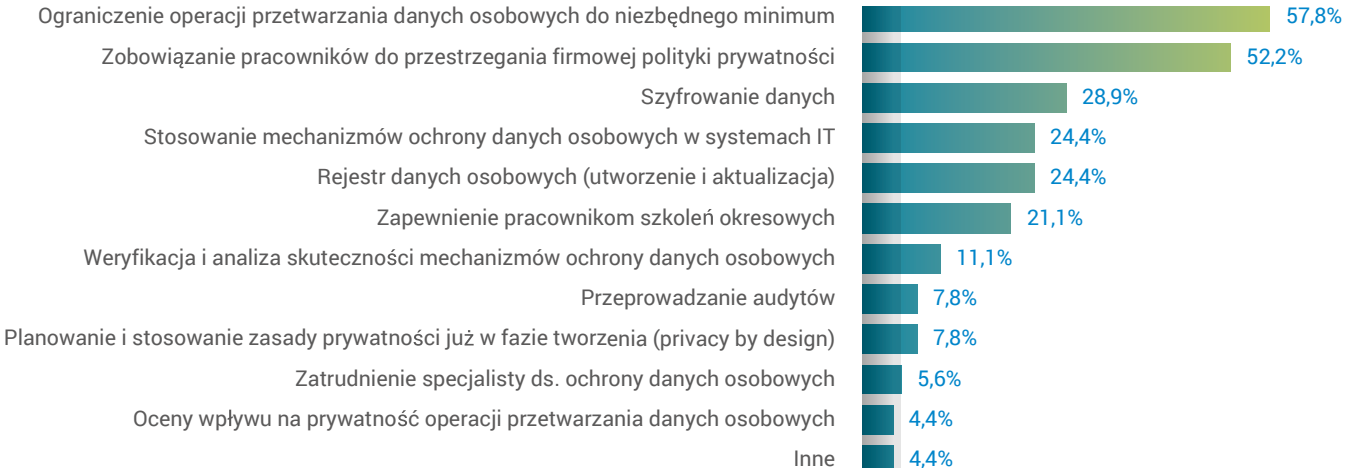
Firmy, poza prowadzeniem działalności w kierunku usług czy produkcji, muszą organizować cały proces komunikacji z odbiorcami czy klientami oraz proces podatkowo rachunkowy. Zarówno w pierwszej jak i drugiej kwestii niezbędne jest podawanie i przesyłanie danych osobowych pomiędzy oferującym, a odbiorcą usług czy produktów. Gromadzenie i przetwarzanie danych osobowych klientów i kontrahentów jest regulowane prawnie w taki sam sposób, bez względu na liczbę osób czy podmiotów, których dotyczy. Zdecydowana większość respondentów twierdzi, że nie przetwarza samodzielnie wrażliwych danych osobowych takich jak treści prywatne wiadomości, czy informacji o poglądach politycznych czy stanie zdrowia (76,0%). Tylko 19% potwierdza, że samodzielnie organizuje taki proces. Wyniki są powiązane z rodzajem prowadzonej działalności oraz obawą przed karami za niestosowanie się do ustawy. Firmy, które oferują usługi budowalne, fryzjerskie czy prowadzą działalność handlową, nie mają potrzeby zbierania danych wrażliwych. Wśród mikroprzedsiębiorców znajdują się jednak branże, które posiadają takie dane, ze względu na potrzebę uwzględnienia ich w obsłudze klienta. Przykładem są firmy obsługujące imprezy rodzinne (wesela, komunie itp.), które dostosowują menu do szczególnych obostrzeń diety nie tylko ze względu na upodobania, ale też uwarunkowania zdrowotne niektórych uczestników. Bezpośrednie rozmowy z właścicielami firm wskazują , że określenie „samodzielne przetwarzanie wrażliwych danych osobowych" kojarzy im się z dużymi biznesami oraz firmami medycznymi a nie z małą przedsiębiorczością.

Wykres 8. Czy Pana(i) przedsiębiorstwo samodzielnie gromadzi i/lub przetwarza wrażliwe dane osobowe klientów i/lub kontrahentów (np. treść prywatnych wiadomości, informacje o stanie zdrowia, poglądach politycznych, itp.)?



Sama znajomość obowiązków w zakresie ochrony danych osobowych nie pozwala na ocenę sytuacji, dlatego zadano pytanie o to jakie zabezpieczenia dotyczące tej kwestii, funkcjonują w firmie. Przedsiębiorcy twierdzą, że przede wszystkim ograniczają liczbę operacji przetwarzania danych osobowych (57,8%) i zobowiązują pracowników do przestrzegania zasad firmowej polityki dotyczącej prywatności (52,2%). Następnie wskazywali, że szyfrują dane (28,9%), stosują dedykowane mechanizmy IT (24,4%) i prowadzą rejestr danych osobowych (24,4%). Co piąty przedsiębiorca zapewnia, że zadbał o szkolenia okresowe dla pracowników (21,1%). Zdecydowanie rzadziej wskazywana była weryfikacja i audyty skuteczności mechanizmów ochrony (kolejno: 11,1% i 7,8%), oraz tworzenie przypisanych systemów ochrony (7,8%). Z unijnych rozporządzeń wynika, że każda firma zatrudniająca mniej jak 250 osób podlega takim samym dyrektywom w kontekście RODO. Taki podział powoduje, że zarówno firmy mające więcej niż 200 pracowników jak i te, które mają status jednoosobowych muszą sprostać takim samym wymaganiom w kwestii RODO. Implementacja rozwiązań rynkowych z zakresie przetwarzania danych osobowych jest bardzo kosztowna z punktu widzenia małej przedsiębiorczości (systemy bądź koszty osobowe) dlatego najczęściej wskazywane przez respondentów rozwiązania mają formę, która nie wymaga takich nakładów.

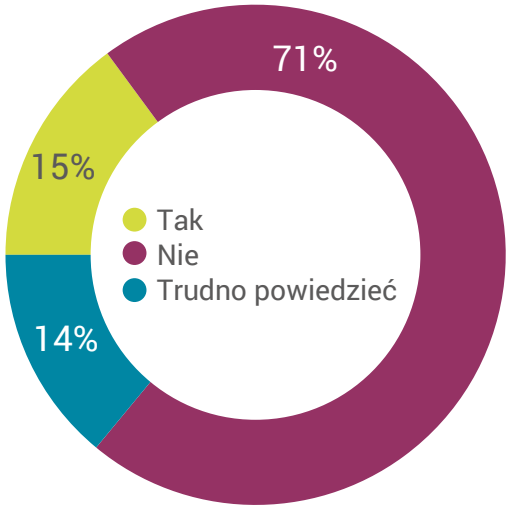
Wykres 9. Jakie zabezpieczenia danych osobowych funkcjonują w Pana(i) przedsiębiorstwie?



Zintegrowane systemy informatyczne do zarządzania relacjami z klientami czy kontrahentami, do niedawna były dedykowane przede wszystkim średnim i dużym przedsiębiorstwom, a teraz są skalowalne na potrzeby mikroprzedsiębiorców.

Z badania wynika, że zdecydowana większość małych firm (71,1%) nie stosuje rozwiązań systemowych a tylko nieliczni wspomagają się nimi (14,9%). Interesujące są odpowiedzi tych, którym trudno określić czy działają w oparciu o taki system (14,0%). W większych firmach rozwiązania pozwalające na zaawansowane planowanie i monitorowanie procesów są często niezbędnym elementem funkcjonowania ze względu na liczebność wykonywanych operacji. W przypadku minimalizowania wydatków i stosowania maksymalnie uproszczonych procesów w mniejszych firmach, wydają się być zbędnym nakładem finansowym. Tylko branże, których działalność jest związana z koniecznością wykonywania licznych (niekoniecznie dużych) transakcji tak jak np.: hurtownie, firmy transportowe, sprzedaż detaliczna – dają uzasadnienie do stosowania takich udogodnień. Dla niektórych pracowników i właścicieli każda innowacja związana z informatyzacją jest określana jako system wspomagający. Wahania w odpowiedziach mogą być powodowane min. sytuacjami kiedy firma korzysta z usług zewnętrznych, wspieranych takimi rozwiązaniami. Zewnętrzna obsługa księgowa z której najczęściej korzystają małe firmy, wykorzystuje systemy informatyczne min. do gromadzenia danych na temat firmy, przesyłania powiązanych dokumentów, czy do kontaktowania się i załatwiania w imieniu klientów spraw urzędowych. Dlatego przedsiębiorcy mogą wskazać, że taki system jest wykorzystywany do realizowania obsługi kadrowej i księgowo-rachunkowej choć w firmie nie ma zaimplementowanego systemu informatycznego.

Wykres 10. Czy w Pana(i) przedsiębiorstwie funkcjonuje zintegrowany system informatyczny do współpracy z kontrahentami i/lub klientami?



Podsumowanie

W świetle wyników badania można zaobserwować wyraźną polaryzację polskich mikro, małych i średnich firm pod względem zakresu i zaawansowania w użytkowaniu technologii informacyjnych.

Zdecydowana większość rodzimych firm wykazuje się umiarkowanym poziomem wykorzystywania potencjału technologii cyfrowych. Ich właściciele i pracownicy korzystają przede wszystkim z podstawowych funkcji oferowanych przez Internet. Najczęściej jest to komunikacja z klientami za pomocą poczty e-mail lub portali społecznościowych, czy używanie sieciowych pakietów narzędzi biurowych (oferowanych m.in. przez Microsoft czy Google). Ok 2/3 badanych biznesmenów za pośrednictwem internetu obsługuje także firmowe płatności oraz umożliwia swoim klientom dokonywanie zakupów online oferowanych przez nich dóbr i usług.

Jednocześnie, aż połowa badanych firm nie posiada własnej strony internetowej, ani nie prowadzi sieciowych kampanii reklamowych. Około połowa z badanych przedstawicieli polskiego biznesu deklaruje, że gromadzi dane osobowe (np. numery telefonów) klientów. W co piątym przypadku zbierane dane obejmują także informacje o charakterze wrażliwym lub poufnym. Tylko niewielka część z badanych firm korzysta z rozwiązań takich jak usługi oparte na technologii chmury obliczeniowej. Usługi w czasie rzeczywistym za pośrednictwem sieci świadczy prawie co dwunaste przedsiębiorstwo. Mniej niż jedna na dziesięć badanych firm korzysta z systemów ochrony danych w obszarze cyberbezpieczeństwa dedykowanych ich działalności, a co siódma posiada infrastrukturę informatyczną, która pozwalałaby na stabilny rozwój i potencjalne skalowanie swojej działalności.

W objętej badaniem próbie wyróżnia się mniejszą grupę przedsiębiorstw, które z powodzeniem wykorzystują narzędzia biznesowe oferowane przez współczesną technikę informacyjno-komputerową. Posiadają one nie tylko rozbudowane kanały www (strona, adresy email czy profile w serwisach), ale także za pomocą internetu realizują kampanie reklamowe, obsługę klienta czy zintegrowane systemy płatności. Można domniemywać, że to właśnie te firmy są najlepiej przygotowane do radzenia sobie z gospodarczymi trudnościami oraz rosnącą konkurencją - w szczególności ze strony dużych i zasobnych w kapitał, międzynarodowych firm.

Inwestycje w transformację cyfrową

Inwestycje w transformację cyfrową

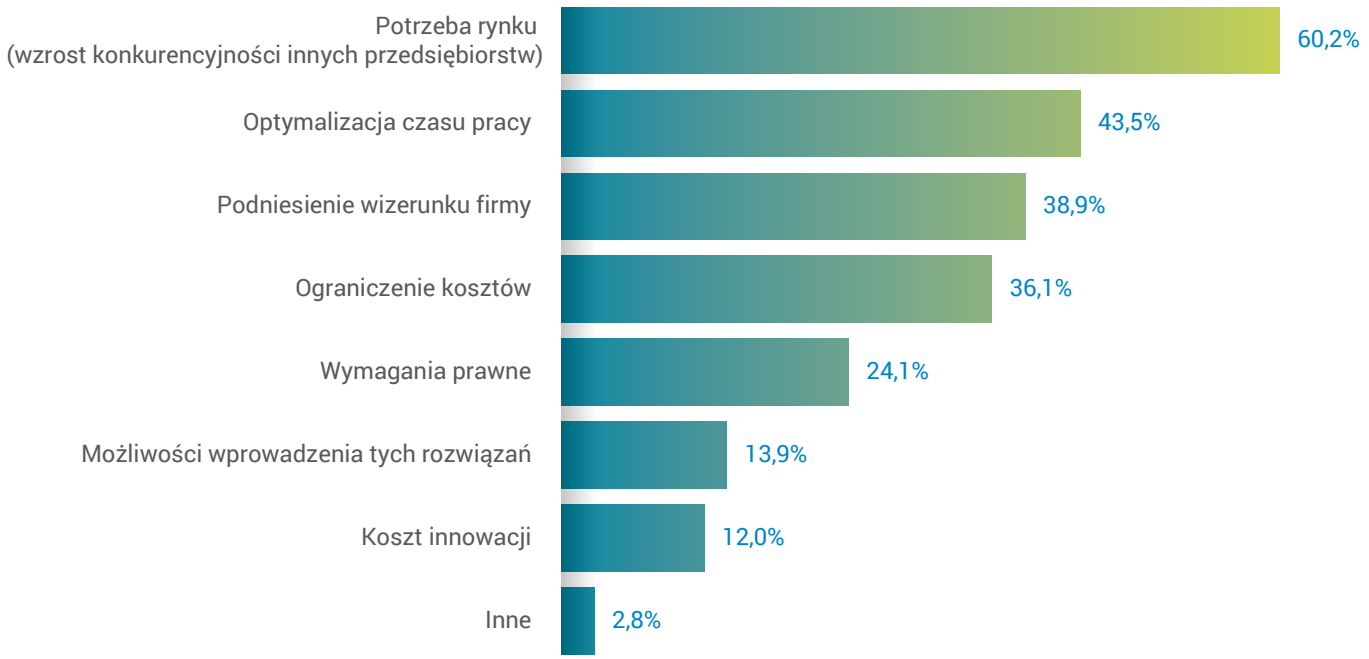
W zglobalizowanej gospodarce opartej na nowych technologiach wydatki na innowacje cyfrowe przestają być pozycją opcjonalną, w coraz większym stopniu stając się koniecznością. Pozwalają one nie tylko na uniknięcie niepożądanych zdarzeń (np. cyberataków, utraty danych czy problemów z obsługą klientów), ale także są okazją do ograniczenia lub lepszego zagospodarowania bieżących zasobów organizacji.

Polskie przedsiębiorstwa charakteryzują się niewielkimi na tle krajów rozwiniętych nakładami na badania i rozwój[6]. Mimo wzrostu nakładów w ostatnich latach[7], polskie firmy wciąż na R&D przeznaczają zaledwie 0,6% PKB – mniej niż ich odpowiednicy m.in. w Słowenii, Czechach czy na Węgrzech. Jednocześnie sektor technologii informacyjnych i komputerowych wskazywany jest jako jeden z największych potencjałów naszej gospodarki, a jego rola w całości eksportu systematycznie rośnie[8].

Celem oszacowania świadomości przedstawicieli polskich firm w zakresie strategii inwestycyjnych w obszarze cyberbezpieczeństwa kwestionariusz badania sondażowego zawierał baterię pytań dotyczących postaw, priorytetów, zachowań i opinii związanych z wydatkowaniem środków przedsiębiorstwa na osoby i narzędzia z obszaru bezpieczeństwa cyfrowego.

Ze wskazań wynika, że głównym kryterium inwestowania w rozwiązania oparte na technologiach informacyjnych jest potrzeba podniesienia konkurencyjności (60,2%). Kolejnymi powodami wydatkowania na ten cel, jest według małych i średnich przedsiębiorstw potrzeba optymalizacji czasu (43,5%), potrzeba poprawy wizerunku firmy (38,9%) oraz zmniejszenie kosztów w firmie (36,1%). Niemal co czwarty respondent twierdził, że jednym z podstawowych kryteriów są wymagania prawne (24,1%). Działania w tym kierunku rzadziej były uzasadniane możliwościami implementacji dedykowanych rozwiązań (13,9%) czy ich kosztami (12,0%). Takie deklaracje potwierdzają kierunek priorytetów w mniejszych firmach. Kiedy wydatek jest zasadny, to nie cena a możliwość dostosowania się dzięki tym nakładom do rynku, odgrywa najważniejszą rolę. Można wnioskować, że świadomość tego jakie możliwości daje wdrożenie nowych technologii w biznesie decyduje o ich implementacji.

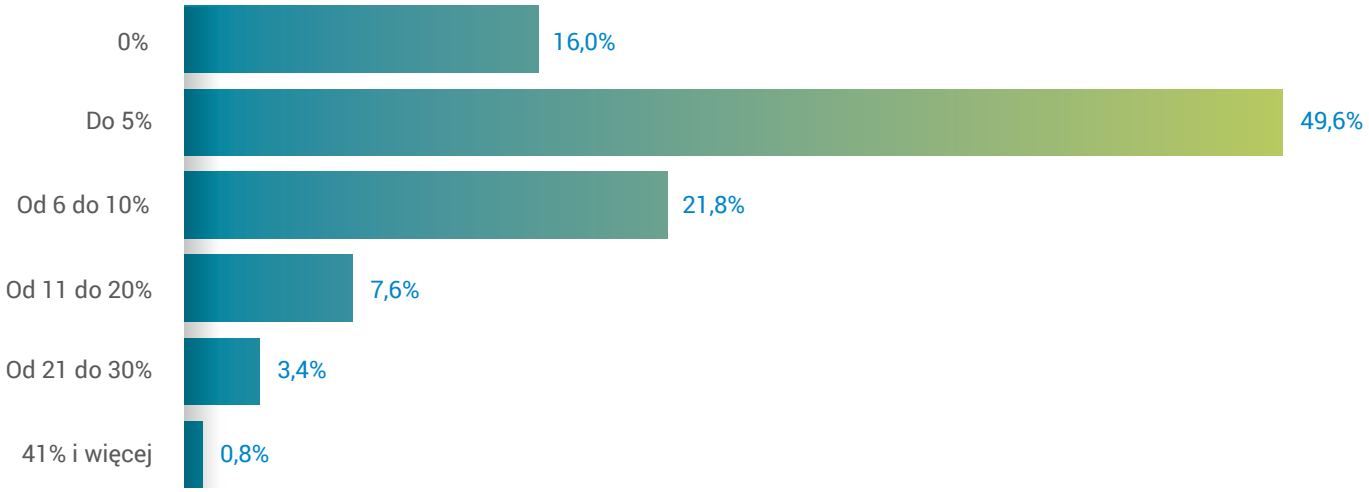
Wykres 11. Co w Pana(i) przedsiębiorstwie jest głównym kryterium inwestowania w rozwiązania oparte na technologiach informacyjnych?



6 Potencjał innowacyjny gospodarki: uwarunkowania, determinanty, perspektywy, Narodowy Bank Polski, 2016
7 B+R Dostępne narzędzia i nowe możliwości, Polski Instytut Ekonomiczny, 2019
8 Polskie B+R Dostępne narzędzia i nowe możliwości, Polski Instytut Ekonomiczny, 2019

W latach 2014-2020 sektor MŚP miał wiele możliwości pozyskiwania środków z funduszy unijnych na wdrażanie innowacji i informatyzację. Mimo, że mali przedsiębiorcy są siłą napędową gospodarki i odpowiadają za 50% PKB to jednak nie inwestują w nowe technologie, co potwierdzają deklaracje większości respondentów. Prawie połowa (49,6%) twierdzi, że wydała na ten cel nie więcej jak 5% budżetu w 2019 roku, a 16% nie odnotowało takiego wydatku. W co piątym przedsiębiorstwie (21,8%) są to większe wydatki, ale nie przekraczające 10% budżetu. Tylko nieliczni wskazywali, że innowacyjne rozwiązania oparte na nowych technologiach pochłaniają większą część budżetu. Brak inwestycji jest blokadą rozwoju biznesowego bo warunkuje konkurencyjność. Przedsiębiorcy mogą postrzegać jednak inwestycje w innych kategoriach jak finansowe. Rozwój technologii cyfrowych czyni je coraz bardziej dostępnymi, dlatego niewielkie budżety na ten cel nie muszą oznaczać rezygnacji z korzystania z nich. Zarówno oprogramowania jak i aplikacje w podstawowych wersjach (bez dodatkowych funkcjonalności) są coraz częściej darmowe i szczególnie najmniejsze firmy mogą z nich z powodzeniem korzystać. Szacowanie wartości inwestycji w IT na poziomie 5% może wynikać z trudności określenia tej kwoty i podania bezpiecznego, w odczuciu respondentów, zakresu.

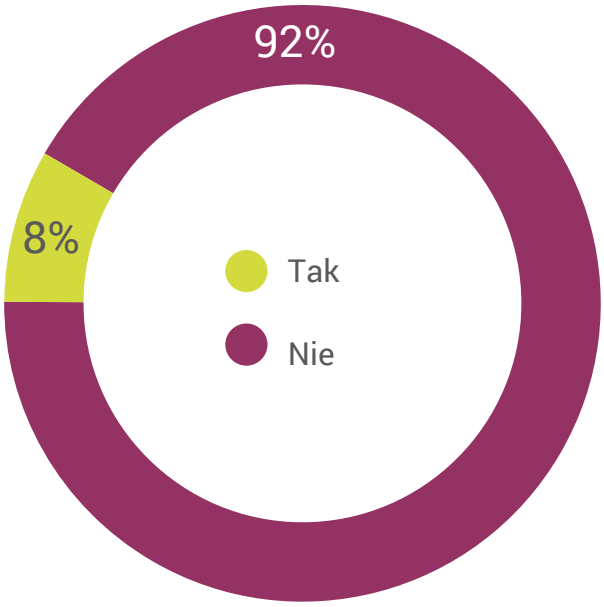
Wykres 12. Jaka część budżetu Pana(i) przedsiębiorstwa, w przybliżeniu, przeznaczona była w 2019 roku na usługi, urządzenia i/lub programy oparte na technologiach informacyjnych?



Nowoczesne technologie dają możliwości rozwoju, ale też stanowią źródło wielu zagrożeń. Przed niebezpieczeństwem chronią dedykowane rozwiązania, których implementacja jest powiązana z potrzebami wynikającymi z profilu firmy oraz regulacji prawnych. Podstawowe wymagania związane z ochroną danych osobowych (RODO) generują potrzebę zabezpieczeń stosowanej infrastruktury informatycznej poprzez pseudonimizację (operacja uniemożliwiająca powiązanie danych z konkretna osobą) czy szyfrowanie danych. Prawie wszyscy przedsiębiorcy (91,7%). twierdzą, że nie napotykają barier związanych z inwestycjami w bezpieczeństwo cyfrowe (91,7%).

Mając na uwadze odpowiedzi na temat planów i inwestycji w cyberbezpieczeństwo, wskazujące na znikome zainteresowanie takimi rozwiązaniami, można wnioskować, że właściciele lekceważą zagrożenia i nie widzą barier bo uważają, że cyberzagrożenia nie dotyczą ich firmy. Brak rozbudowanych systemów usprawniających, czy też sama wielkość przedsiębiorstwa, zdaniem respondentów wyklucza takie ryzyko.

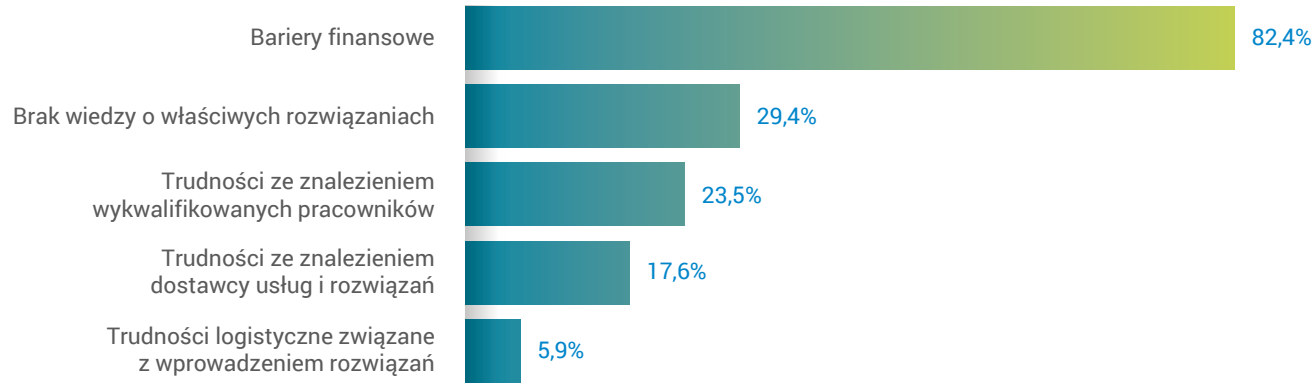
Wykres 13. Czy Pana(i) przedsiębiorstwo napotyka bariery związane z inwestycjami w bezpieczeństwo cyfrowe?



Nieliczni spośród wskazujących na bariery inwestycyjne w cyberbezpieczeństwo zaznaczają, że widzą taką potrzebę i chcieliby zabezpieczać swoją infrastrukturę, ale nie mają możliwości ze względu na braki finansowe (82,4%). Prawie co trzeci z tej grupy twierdzi, że nie inwestuje ze względu na „Brak wiedzy o właściwych rozwiązaniach" (29,4%), a niemal co czwarty dlatego, że ma „Trudności ze znalezieniem wykwalifikowanych pracowników" (23,5%). Mniej wskazań dotyczy odpowiedzi „Trudności ze znalezieniem dostawcy usług i rozwiązań" (17,6%).

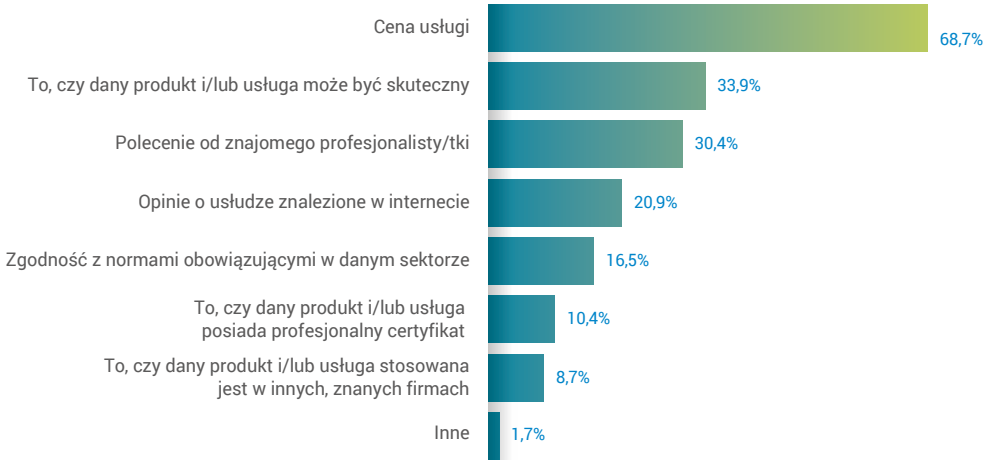
Rozwiązania bezpieczeństwa IT w firmach wymagają inwestycji, a w sytuacji kiedy preferowane są działania optymalizujące koszty, łatwiej uzasadnić wydatki na problemy istniejące niż na profilaktykę. Te firmy, które nie pracują na złożonych systemach informatycznych, nie posiadają wiedzy o produktach ochrony – adekwatnych do zakresu wykorzystywanych narzędzi. Niemniej dane dotyczące barier inwestycji w zabezpieczenia IT odnoszą się do zbyt małej grupy aby wnioskować na populację.

Wykres 14. Jakie są największe bariery związane z inwestycjami w cyberbezpieczeństwo w Pana(i) przedsiębiorstwie?



Tu odpowiedzi potwierdzają merkantylny stosunek przedsiębiorców do cyberochrony. Bezpieczeństwo jest ważne, ale w zakresie subiektywnie określanego ryzyka. Decydując się na konkretne usługi czy produkty cybrebezpieczeństwa najczęściej firmy kierują się ceną (68,7%). Co trzecia firma wskazuje też na skuteczność systemu chroniącego (33,9%) i prawie tyle samo na to, że przy wyborze polega na poleceniu przez znajomego profesjonalistę w tej dziedzinie (30,4). Zaufanie do opinii zamieszczonych w internecie przez innych użytkowników, deklaruje co piąta firma (20,9%), a pozostałe wskazania dotyczą zgodności z normami (16,5%), certyfikatami (10,4%) czy też zastosowania produktów/usług przez inne, znane firmy (8,7%). Kryterium cenowe jako fundament wyborów potwierdzają odpowiedzi na pytania o skalę inwestowania i bariery implementacji. Okazuje się też, że zaufanie do nadawanych certyfikatów w przypadku małych firm nie potwierdza się, tak samo jak zastosowanie produktu w dużych firmach. Obie dane mogą kojarzyć się małym firmom z dużym biznesem i być traktowane jako czynnik zniechęcający, bo oznaczający niedopasowanie do ich skali biznesu.

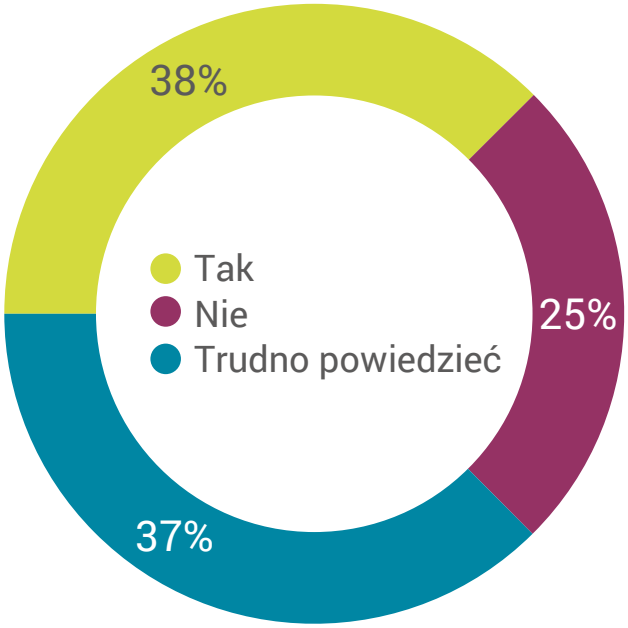
Wykres 15. Co najczęściej jest powodem blokowania wdrożenia nowych rozwiązań w zakresie cyberbezpieczeństwa w Pana(i) przedsiębiorstwie?



Inwestycje w infrastrukturę IT nie wystarczą aby sprawnie i bezpiecznie funkcjonowała firma. Działania takie jak szkolenia czy tworzenie procedur korzystania z użytkowanych systemów są ważne, ale niewystarczające aby uchronić się przed cyberprzestępczością czy innymi zagrożeniami. Technologia stale się rozwija i razem z nią sposoby nadużyć wykorzystujących cybernarzędzia. Żadne zabezpieczenia nie są na stałe, należy je aktualizować. Częściej niż co trzecia firma (37,5%) zamierza zastosować nowe rozwiązania w zakresie cyberbezpieczeństwa. Tyle samo respondentów (37,5%) nie umie określić jednoznacznie czy będą wdrażać nowe środki zapobiegające zagrożeniom. Co czwarty przedsiębiorca (25,1%) nie ma planów na implementację produktów czy usług cyberochronny. Technologia usprawnia funkcjonowanie, a w przypadku niektórych branż (np.: handel) warunkuje działanie. Dlatego nie zaskakują odpowiedzi części tych firm, które widzą potrzebę zabezpieczenia infrastruktury IT i deklarują, że będą takie rozwiązania stosować. Warto zwrócić uwagę na wysoki odsetek odpowiedzi „Trudno powiedzieć" (37%), które mogą wynikać z przyjętego sposobu działania polegającego na reagowaniu na już zaistniałe problemy a nie zapobieganie im. Aby przeciwdziałać trzeba mieć świadomość zagrożeń, wynikającą z wiedzy na temat nowych technologii. Często mikroprzedsiębiorstwo to jednoosobowa działalność gospodarcza, co nie sprzyja inwestowaniu w wiedzę z zakresów nie będących przedmiotem prowadzenia firmy.

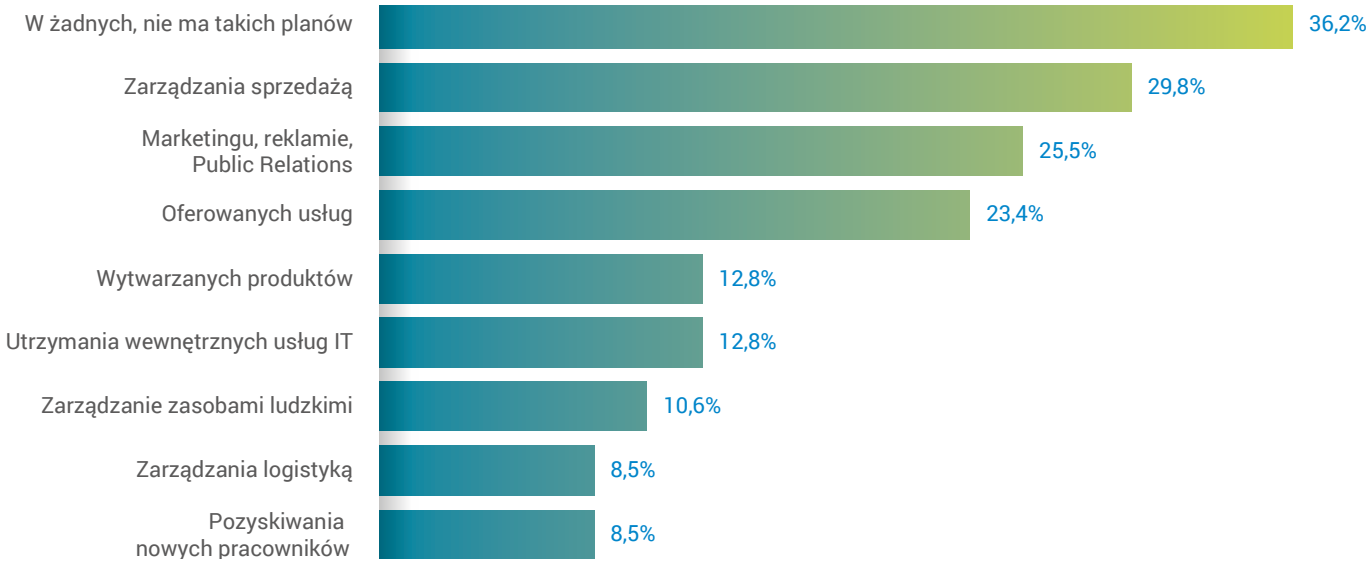
Świadomość zagrożeń powoduje potrzebę przeciwdziałania. Zastosowanie ochrony infrastruktury IT minimalizuje ryzyko strat. Odpowiedzi potwierdzają niezdecydowanie przy pytaniu o plany zastosowania nowych produktów ochrony IT. Co trzecia firma wskazuje na to, że nie ma takich planów (36,2%). Ci którzy deklarują wdrożenie nowych rozwiązań wskazują

Wykres 16. Czy w najbliższych 12 miesiącach, Pana(i) przedsiębiorstwo zamierza zastosować nowe rozwiązania w zakresie cyberbezpieczeństwa?



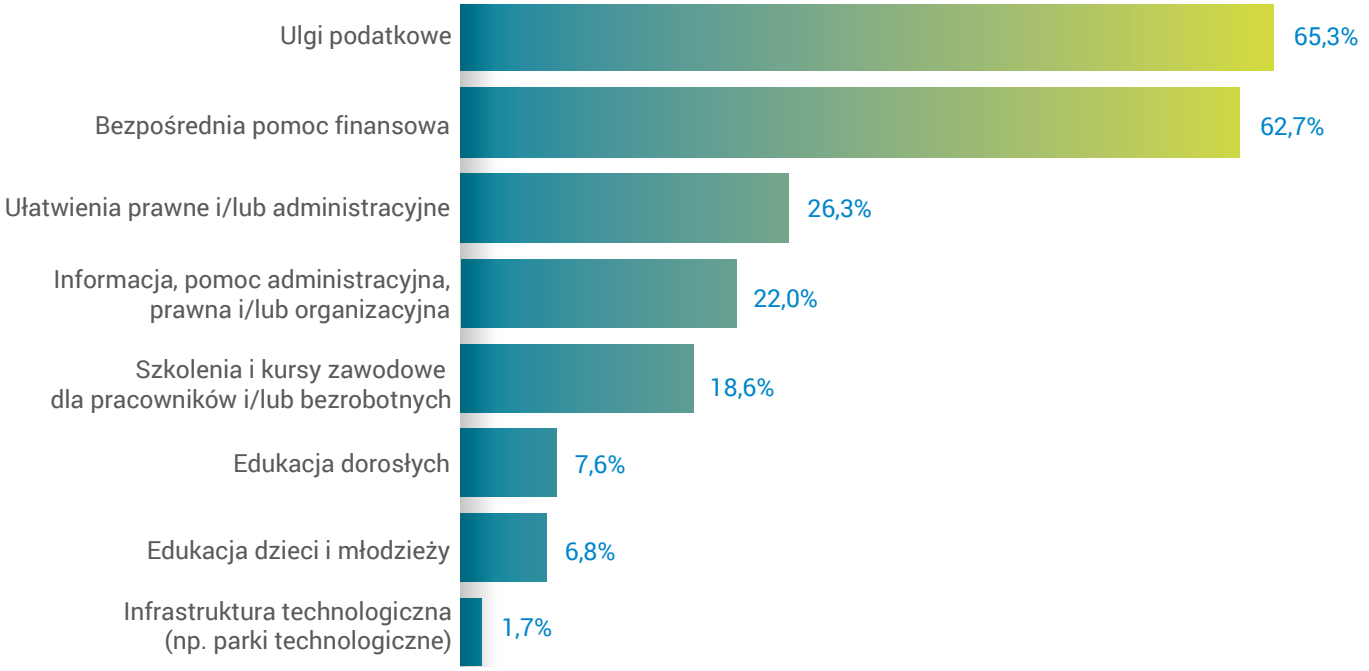
najczęściej na „Zarządzanie sprzedażą" (29,8%), „Marketing, reklamę i Public Relations" (25,5%) oraz „Oferowanych usług" (23,4%). Część firm zamierza implementować nowe narzędzia w zakresie „Wytwarzanych produktów" (12,8%), „Utrzymania wewnętrznych usług IT" (12,8%) i :„Zarządzania zasobami ludzkimi" (10,6%). W przypadku realizacji procesu sprzedaży za pomocą internetu, system obsługi jest podstawowym narzędziem, które należy chronić przed zagrożeniami, bo oznacza to blokadę działania, a skutki mogą być bardzo dotkliwe. Wskazanie na reklamę i oferowane usługi jest zgodne ze wskazaniami na temat obszarów w jakich małe firmy wykorzystują IT.

Wykres 17. W jakich obszarach Pana(i) przedsiębiorstwo zamierza zastosować rozwiązania z zakresu cyberbezpieczeństwa?



Najmniejsze firmy najszybciej reagują na zawirowania gospodarki, a ta elastyczność jest gwarancją sukcesu. Właściciele takich firm stale muszą aktualizować swoją ocenę ryzyka działania i wskazywać priorytety – też inwestycyjne. Operatywność zarządzającym takimi firmami pozwala min. pozyskiwać środki na kluczowe cele. Przedsiębiorcy są obok samorządów jednymi z największych beneficjentów funduszy unijnych na projekty badawcze i wdrażanie innowacji. Zapytani o to, jakie formy pomocy publicznej zachęciłyby ich do inwestowania w rozwiązania w zakresie cyberbezpieczeństwa, wskazywali przede wszystkim „Ulgi podatkowe" (65,3%) oraz „Bezpośrednia pomoc finansowa" (62,7%). „Ułatwienia prawne i/lub administracyjne" motywowałyby co czwartego przedsiębiorcę (26,3%). Przedstawiciele firm uważają też, że dobrym wsparciem byłyby formy propagowania informacji na temat dedykowanych rozwiązań czy wsparcie administracyjno-prawne (22%) raz szkolenia czy kursy zawodowe (18,6%). Wskazania odzwierciedlają problemy mikrofirm związane z obciążeniami podatkowo składkowymi. Stanowią one dużą część wszystkich kosztów, a w połączeniu z nieregularnością dochodów czy odroczeniami płatności, zagrażają płynności finansowej (cash flow) MŚP. Ułatwienia prawne czy administracyjne są oczekiwanym wsparciem małych firm, bo swoje działania i wydatki mają mocno skoncentrowane na bieżącej działalności i brakuje im kompetencji, zasobów osobowych czy finansowych na realizacje polityki bezpieczeństwa.

Wykres 18. Jakie formy pomocy publicznej zachęciłyby Pana(i) przedsiębiorstwo do inwestowania w rozwiązania w zakresie cyberbezpieczeństwa?



Podsumowanie

Głównym kryterium inwestowania w rozwiązania oparte na technologiach informacyjnych w polskich mikro, małych i średnich firmach jest potrzeba podniesienia konkurencyjności (60,2%). Kolejnymi powodami wydatkowania na ten cel, jest potrzeba optymalizacji czasu (43,5%), potrzeba poprawy wizerunku firmy (38,9%) oraz zmniejszenie kosztów w firmie (36,1%). Jednak firmy nie inwestują w nowe technologie, co potwierdzają deklaracje większości respondentów. Prawie połowa (49,6%) twierdzi, że wydała na ten cel nie więcej jak 5% budżetu w 2019 roku, a 16% nie odnotowało takiego wydatku. W co piątym przedsiębiorstwie (21,8%) są to większe wydatki, ale nie przekraczające 10% budżetu. Prawie wszyscy przedsiębiorcy (91,7%). twierdzą, że nie napotykają barier związanych z inwestycjami w bezpieczeństwo cyfrowe. Najczęściej wskazywanym ograniczeniem są kwestie finansowe. Także w przypadku wyboru usługi z zakresu cyberbezpieczenstwa dominuje kryterium ceny (prawie 70%), a kwestia ewentualnej skuteczności jest priorytetowa jedynie dla co trzeciego badanego. Tylko niecałe 40% firm planowało w ciągu 12 miesięcy wdrożyć nowe rozwiązania mające na celu zwiększenie bezpieczeństwa cyfrowego, a w aż 3/4 nie ma takich planów, bądź respondent nic o takowych nie wiedział. Wśród przedsiębiorstw, które planują takie działania, według deklaracji, miały zostać nimi objęte przede wszystkim systemy sprzedaży, marketingu oraz świadczone usługi. Zapytani o najlepsze ich zdaniem formy wsparcia publicznego, przedsiębiorcy wskazali na ulgi podatkowe oraz bezpośrednie dotacje.

Doświadczenia cyberzagrożeń

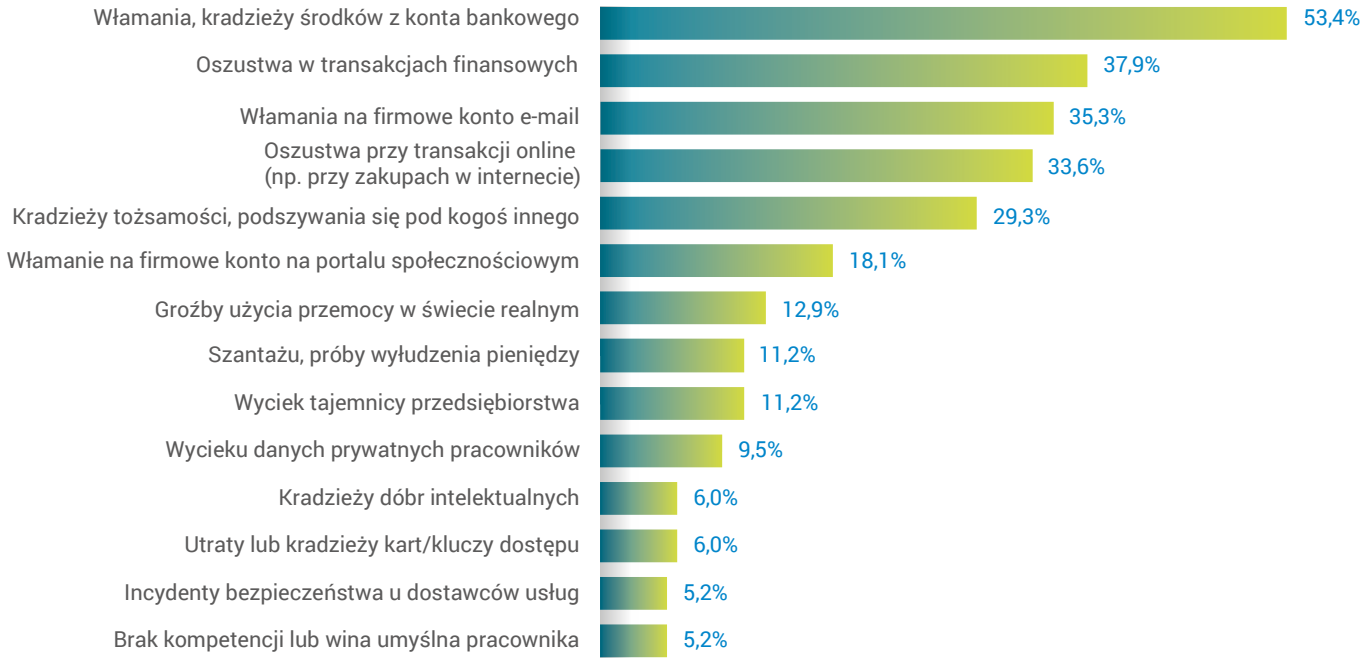
Doświadczenia cyberzagrożeń

Ze względu na zróżnicowaną strukturę polskich firm odpowiedzialność za faktyczne bezpieczeństwo informacyjne może spoczywać albo na samym przedsiębiorcy, albo na osobach przez niego formalnie delegowanych do tego zadania. W każdym wypadku jednak, to na przedsiębiorstwie (a więc osobie lub osobach ponoszących odpowiedzialność w świetle m.in. regulacji prawa cywilnego, karnego, administracyjnego czy spółek handlowych) spoczywa ostateczna odpowiedzialność za ewentualne problemy. Odpowiedzialność może mieć charakter prawny - np. kiedy efektem zaniedbań jest incydent narażający dane prywatne klientów na ujawnienie (co reguluje m.in. Rozporządzenie o Ochronie Danych Osobowych), finansowy (gdy w grę wchodzą wyłudzenia lub oszustwa finansowe) lub wizerunkowy (gdy zdarzenia nie powodują skutków prawnych, a jedynie pogarszają postrzeganie firmy na rynku).

Badanych reprezentantów polskich firm poproszono o odpowiedź na serię pytań poświęconych wiedzy o zagrożeniach dla cyberbezpieczeństwa, z którymi spotkali się w ramach swojego zaangażowania w działalność przedsiębiorstwa.

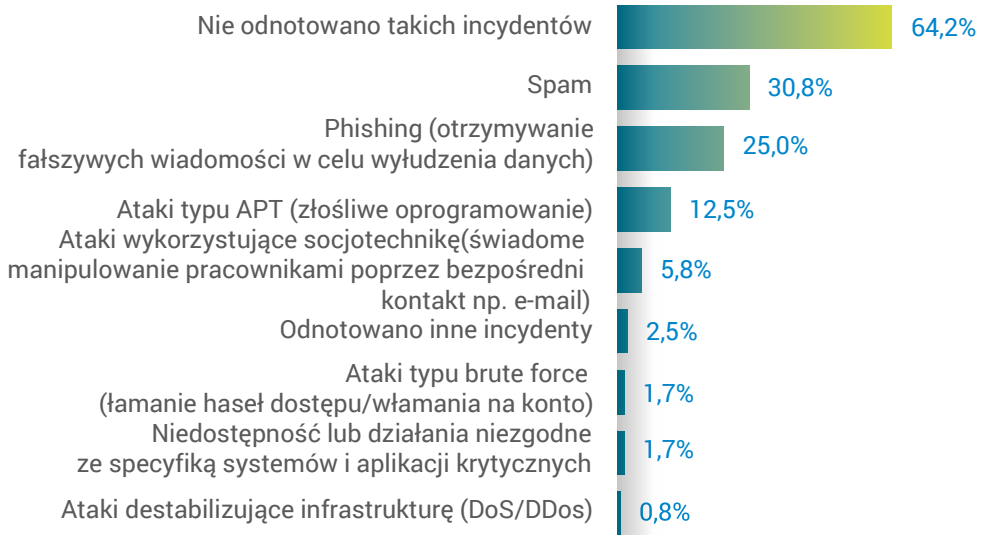
Ataki phishingowe i ransomware nastawione na wyłudzenie danych czy blokujące sieć ataki DDoS są bardzo poważnym zagrożeniem nawet dla małych przedsiębiorstw. Powodują nie tylko wyciek danych, ale mogą w szybkim tempie zablokować sieć firmową – unieruchamiając wszystkie działania. Polityka zabezpieczenia przed skutkami takich ataków powinna być jednym z priorytetów firm. Z odpowiedzi na pytanie o to, które z incydentów są największym zagrożeniem - wynika, że mały biznes boi się przede wszystkim utraty środków finansowych: „Włamania, kradzieży środków z konta bankowego" (53,4%) oraz „Oszustwa w transakcjach finansowych" (37,9%) i „Transakcjach on-line" (33,6%). Jednym z realnych zagrożeń jest też według respondentów „Włamanie na firmowe konto e-mail" (35,3%) oraz „Kradzież tożsamości, podszywanie się pod kogoś innego" (29,3%) oraz „Włamanie na firmowe konto na portalu społecznościowym" (18,1%). Rozkład deklaracji wskazuje postrzeganą lokację priorytetowych zasobów firmy. Najpoważniejszą stratą dla MŚP jest utrata środków finansowych, bo nawet małe kwoty mogą zaburzyć prawidłowe funkcjonowanie, opóźnić realizacje zobowiązań i narazić firmę na poważne kłopoty. Poza płynnością finansową najważniejsze w mikrobiznesie są narzędzia do komunikacji, które służą nie tylko do przesyłania wiadomości, ale też dokumentów czy realizowania formalności. Skrzynka e-mail jest traktowana jak swoista baza kontaktów, danych i ważnych załączników. Często przedsiębiorcy traktują ją jako podstawowy „system" informatyczny w firmie z chronologicznym zapisem wydarzeń i możliwością odtworzenia historii danej sprawy.

Wykres 19. Które z poniższych incydentów są według Pana(i) największym zagrożeniem dla Pana(i) przedsiębiorstwa?



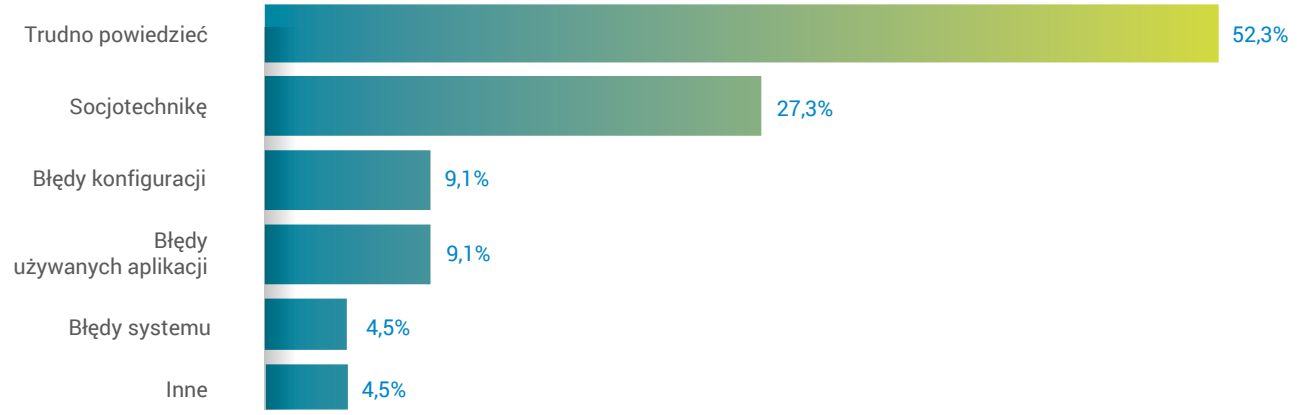
Branża bezpieczeństwa systemów IT proponuje wiele programów do monitorowania pracy urządzeń cyfrowych. Pozwalają one na wykrywanie incydentów, analizę szczegółów i podejmowanie adekwatnych działań. Na pytanie o to, czy w ostatnim czasie w firmie odnotowano naruszenia bezpieczeństwa cyfrowego, większość przedstawicieli MŚP odpowiedziała, że nie (64,2%). Ci którzy zidentyfikowali problem w swojej organizacji, zaznaczali „Spam" (30,8%) oraz „Phishing (otrzymywanie fałszywych wiadomości w celu wyłudzenia danych)" (25,0%). Niewiele ponad 10% przedsiębiorców miało problemy spowodowane złośliwym oprogramowaniem (12,5%), a tylko nieliczni z atakami wykorzystującymi socjotechnikę (5,8%). Takie odpowiedzi obrazują rzeczywisty stan infrastuktury IT w najmniejszych firmach, gdzie jest ona zawężona najczęściej do podstawowych narzędzi systemowych. Umiejętność identyfikacji takich zdarzeń jest powiązana z kompetencjami użytkowników. W firmie, gdzie jedna osoba odpowiada za całą firmę, nie ma działu IT, cyberataki mogą być nierozpoznane, jeśli tylko nie zablokują działania podstawowych narzędzi takich jak skrzynka e-mail itp. Potwierdzają to badania i analizy z których wynika, że skala ataków na małą przedsiębiorczość stale rośnie, choć nie wszystkie są skuteczne . Można założyć, że sposoby działania hakerów ewoluują, a brak kompetencji w rozpoznaniu incydentów czyni małe firmy najbardziej dogodnym celem ataków.

Wykres 20. Czy w ostatnich 12 miesiącach w Pana(i) przedsiębiorstwie odnotowano któryś z poniższych incydentów bezpieczeństwa cyfrowego?



Weryfikacja mechanizmów incydentów pozwala na zastosowanie odpowiednich środków zaradczych. Od właściwej identyfikacji problemu zależy strategia obsługi. Aby szybko rozwiązać sprawę i przywrócić ciągłość działania, należy określić ryzyko jakie wiąże się ze zdarzeniem. Ponad połowa respondentów nie była w stanie jednoznacznie odpowiedzieć na pytanie o dookreślenie szczegółów zaistniałych incydentów w firmie, i zaznaczała „Trudno powiedzieć" (52%). Następnie wskazywano, że problemy pojawiły się w następstwie działań wykorzystujących „Socjotechnikę" (27,3%). Według respondentów „Błędy konfiguracji" i „Błędy używanych aplikacji" rzadziej przyczyniają się do naruszeń bezpieczeństwa (kolejno: 9,1% i 9,1%). Taki rozkład odpowiedzi może oznaczać, że w mikroprzedsiębiorstwach pracownicy nie mają wiedzy z tego zakresu, na co wskazują też odpowiedzi na pytanie o doświadczenie cyberataków.

Wykres 21. Czy odnotowane w Pana(i) przedsiębiorstwie incydenty bezpieczeństwa wykorzystywały, któreś z poniższych?



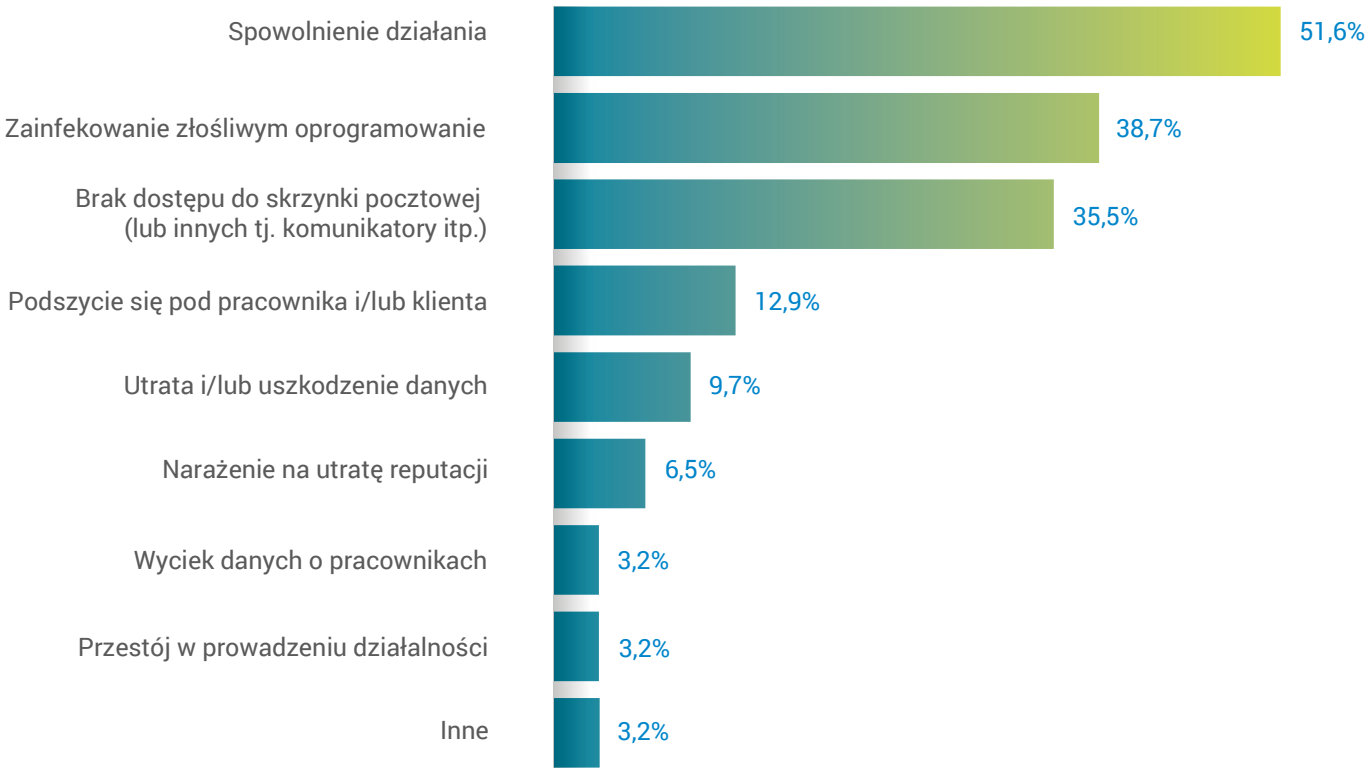
Może to być konsekwencją postawy jaką sugerują wskazania przedsiębiorców na temat implementacji nowych rozwiązań w zakresie cyberbezpieczeństwa. Większość firm nie uwzględnia tego w swoich planach, bo nie widzi takiej potrzeby, bo nie identyfikuje problemu i ryzyka.

Incydenty bezpieczeństwa są groźne nie tylko dla dużych firm, które inwestują w rozbudowaną infrastrukturę IT. W przypadku organizacji z wydzielonymi działami do spraw cyfrowego bezpieczeństwa stosowane są profilaktyczne rozwiązania, których przestrzeganie gwarantuje, w przypadku zaistnienia incydentu, zminimalizowanie strat. Większa firma tworzy kopie zapasowe i może odtworzyć dane, a mała firma traci to co zostało zaatakowane. W tym przypadku nawet małe zdarzenie może pociągnąć za sobą poważne konsekwencje zagrażające funkcjonowaniu firmy. Z deklaracji wynika, że incydenty bezpieczeństwa powodują przede wszystkim „Spowolnienie działania" (51,6%).

Cyberataki przyczyniają się w małych firmach także do „Zainfekowania złośliwym oprogramowaniem" (38,7%) oraz „Braku dostępu do skrzynki pocztowej (lub innych tj: komunikatory)" (35,5%). Pozostałe wskazane skutki cyberwypadków to: „Podszycie się pod pracownika lub klienta" (12,9%) oraz „Utrata lub uszkodzenie danych" (9,7%).

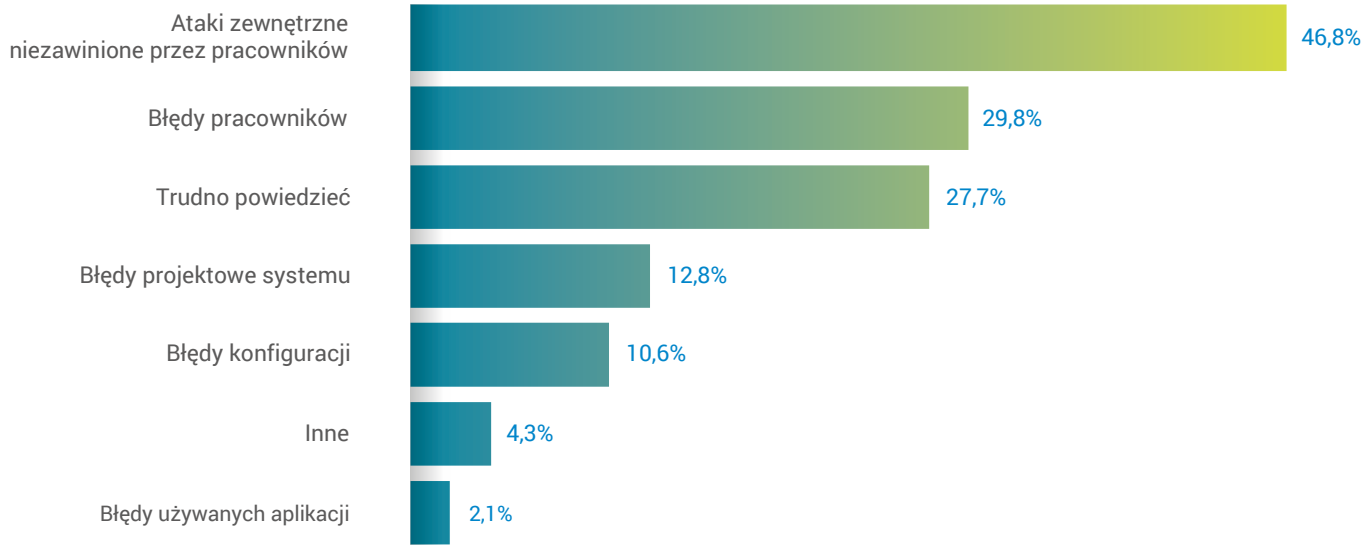
Wielkość firmy koreluje z zasobami narzędzi cyfrowych. Mikroinfrastruktura i chętnie wykorzystywane darmowe rozwiązania, generują najbardziej powszechne, przypisane do takich narzędzi, problemy. Dlatego spowolnienie jest pierwszą zauważalną konsekwencją. Brak w większości małych firm monitoringu zabezpieczeń, inwestycji w antywirusy, firewall itp., jest powodem podatności na złośliwe oprogramowania. Deklaracje badanych są konsekwencją tego czy skutki są zauważalne i odczuwalne.

Wykres 22. Czy w ostatnich 12 miesiącach w wyniku cyberataku przedsiębiorstwo doświadczyło któregoś z niżej wymienionych problemów?



Według przedsiębiorców głównym źródłem incydentów bezpieczeństwa są przede wszystkim „Ataki zewnętrzne, niezawinione przez pracowników" (46,8%). Niemal co trzeci respondent wskazuje na „Błędy pracowników" (29,8%). Zdecydowanie rzadziej firmy są skłonne przypisać odpowiedzialność za problemy architektom systemów dlatego zaznaczają „Błędy projektowe systemu" (12,8%) oraz „Błędy konfiguracji" (10,6%).

Wykres 23. Co według Pana(i) jest głównym źródłem incydentów bezpieczeństwa w Pana(i) przedsiębiorstwie?



Mimo trudności z identyfikacją źródła problemów związanych z funkcjonowaniem wykorzystywanych narzędzi informatycznych przedsiębiorcy dość jednoznacznie wskazują na potencjalne zagrożenia.

Według nich najczęstszymi błędami popełnianymi przez pracowników, jest „Otwieranie e-mail od nieznanych nadawców" (69,2%), „Przenoszenie niezaszyfrowanych informacji" (43,6%) oraz „Udostępnianie nazwy użytkownika" (41,0%). Domniemanym zagrożeniem jest też „Instalowanie oprogramowania z Internetu" (35,9%), „Pozostawianie stanowiska pracy w trybie zalogowania do systemu" (33,3%). Co czwarty respondent uważa, że problematyczne są sytuacje, kiedy pracownicy nie oddzielają środowiska pracy od prywatnego (25,6%) i nie stosują się do podstawowych zasad poufności danych logowania (23,1%).

Łatwość identyfikacji potencjalnych zagrożeń generowanych przez pracowników jest często powiązana z cechami małych społeczności w pracy. W dużej firmie, gdzie jest duża grupa użytkowników danego systemu, trudno wskazać nie tylko kto przyczynił się do błędu, ale też w jaki sposób. Mogą zaistnieć sytuacje ukrywania incydentów w obawie przed konsekwencjami. Komunikacja wewnętrzna i przepływ informacji w małych firmach pozwalają na to, że wszyscy są zorientowani w bieżących wydarzeniach, też problemach technicznych IT.

Wykres 24. Jakie są najczęstsze błędy popełniane prze pracowników firmy, które są potencjalnym zagrożeniem cyberbezpieczeństwa?

Podsumowanie

Na podstawie badania można stwierdzić, że polski biznes jedynie w ograniczonym stopniu zdaje sobie sprawę ze skali i specyfiki ryzyka, z którym wiąże się użytkowanie sieci.

Prawie 2/3 polskich drobnych przedsiębiorców deklaruje, że w ich firmie, w ciągu 12 miesięcy poprzedzających badanie, nie było incydentów w zakresie cyberbezpieczeństwa. Wśród podmiotów, w których miały one miejsce przeważnie powodowały one spowolnienie w produkcji lub świadczeniu usług, uszkodzenie oprogramowania w firmie, czy problem z komunikacją elektroniczną.

Przedsiębiorcy na ogół lokują odpowiedzialność za ataki poza firmą: tj. u cyberprzestępców lub złośliwym oprogramowaniu. Jedynie co trzeci badany wskazał, że podatność na cyberzagrożenia to przede wszystkim wina pracowników.

Przedstawiciele niedużych firm najbardziej boją się włamań i kradzieży z elektronicznego konta bankowego lub innych oszustw finansowych, a w mniejszym stopniu także kradzieży tożsamości (osoby lub firmy) lub włamania na profile społecznościowe.

Polityka cyberbezpieczeństwa

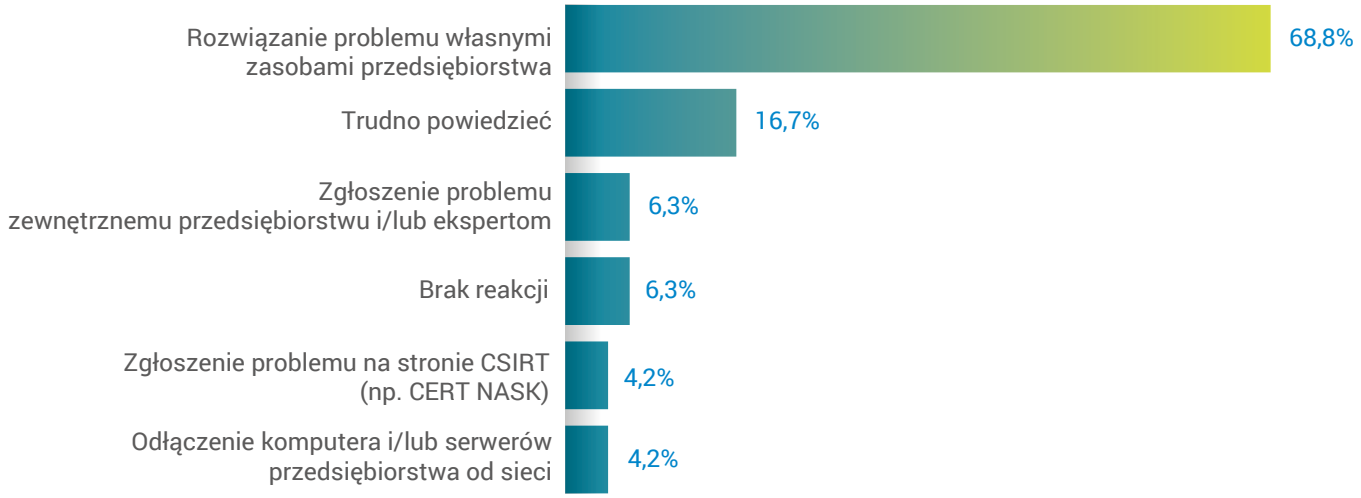
Polityka cyberbezpieczeństwa

Bezpieczeństwo cyfrowe firm i ich klientów zależy od procedur i zasad, które organizacja stosuje w celu ochrony swoich cyfrowych zasobów. To one określają typy i sposoby reagowania w sytuacjach zaistnienia incydentów lub innych zagrożeń dla bezpieczeństwa danych. W praktyce gospodarczej spotyka się dwa modele odpowiedzi na to wyzwanie. Część firm, szczególnie tych zatrudniających większą liczbę pracowników, regulaminy i modele działania przygotowuje samodzielnie, tj. za pośrednictwem własnych pracowników i rozwiązań technicznych. Alternatywną, często spotykaną w mniejszych firmach, praktyką jest outsourcing, tj. przekazywanie maksymalnie dużej części zadań, związanych z bezpieczeństwem cyfrowym wyspecjalizowanym w tym zakresie firmom i osobom.

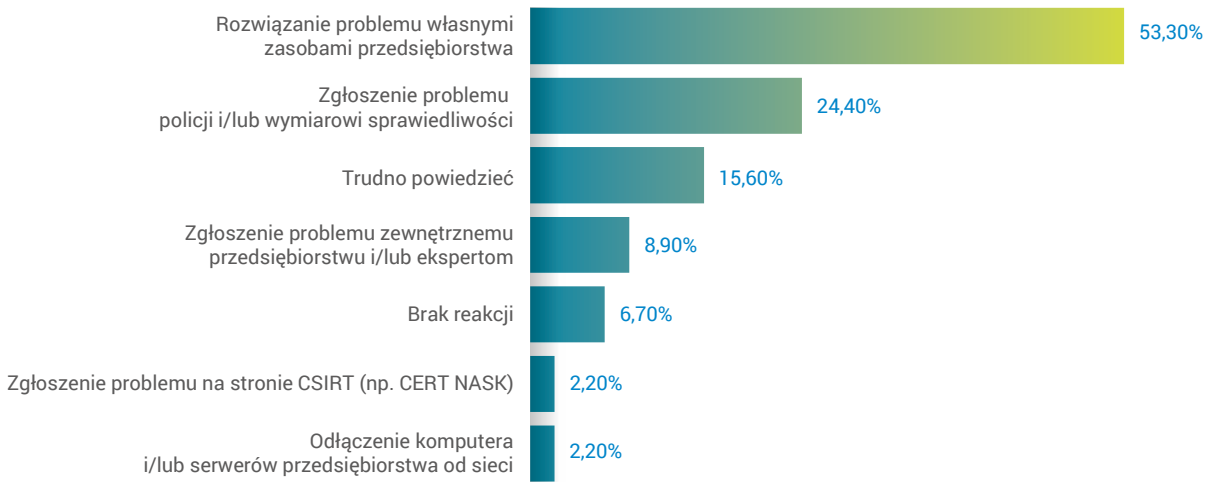
Przedsiębiorcy zostali zapytani w jaki sposób reagują na poszczególne incydenty bezpieczeństwa. Z deklaracji wnika, że małe firmy preferują rozwiązania problemów własnymi zasobami. W taki sposób reagują na „Podejrzane załączniki" (68,8%), „Próbę oszustwa, podszywania się" (53,3%), „Złośliwe oprogramowanie (np.: wirusy)" (57,4%), czy „Nielegalne treści (brutalne, pedofilskie itp.)" (35,7%). Tylko w przypadku błędów oprogramowania w pierwszej kolejności zlecają problem podmiotom zewnętrznym (63,3%). W przypadku nielegalnych treści 31,0% ankietowanych uważa, że najwłaściwszą reakcją jest zgłoszenie sprawy Policji tak jak w przypadku nadużyć polegających na próbie oszustwa (24,4%).

Małe i średnie firmy reagują adekwatnie do inwestycji w systemy IT, i to co jest możliwe rozwiązują wewnętrznie. Tylko w przypadku kiedy sprawa dotyczy kompetencji w zakresie programowania to zlecają naprawę na zewnątrz, bo nie potrafią tego samodzielnie zrobić.

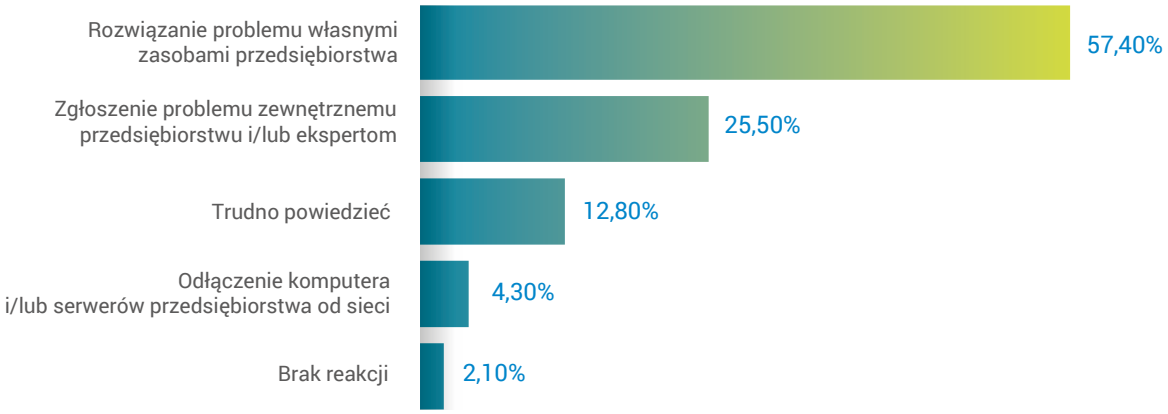
Wykres 25. W jaki sposób w Pana(i) przedsiębiorstwie reaguje się na poniższe incydenty w zakresie cyberbezpieczeństwa? Podejrzane załączniki.



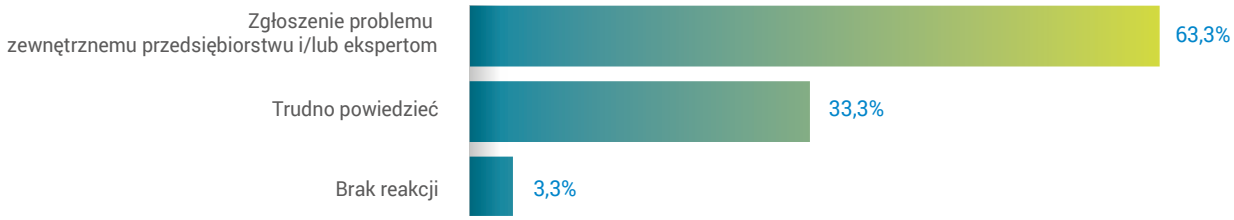
Wykres 26. W jaki sposób w Pana(i) przedsiębiorstwie reaguje się na poniższe incydenty w zakresie cyberbezpieczeństwa? Próba oszustwa, podszywanie się.



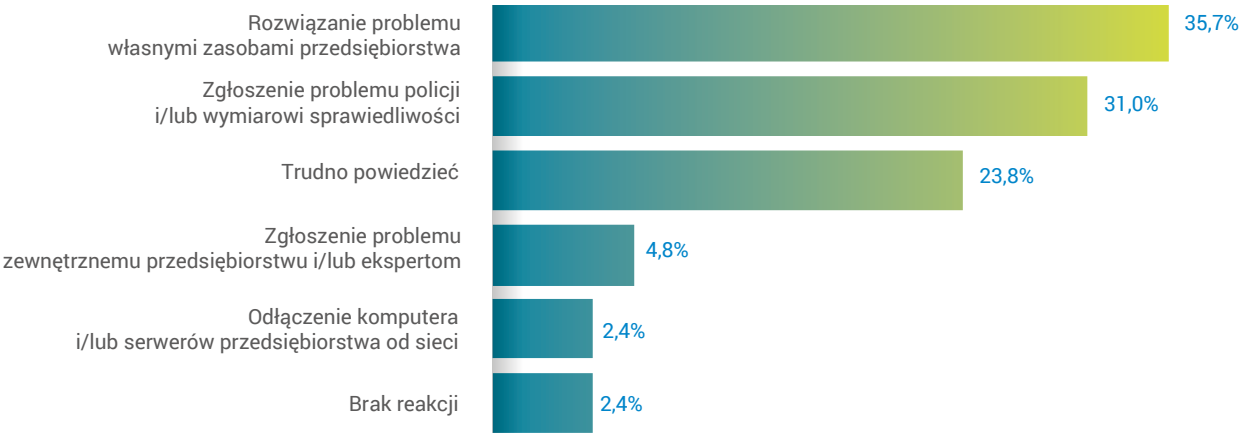
Wykres 27. W jaki sposób w Pana(i) przedsiębiorstwie reaguje się na poniższe incydenty w zakresie cyberbezpieczeństwa? Złośliwe oprogramowanie (np. wirusy).



Wykres 28. W jaki sposób w Pana(i) przedsiębiorstwie reaguje się na poniższe incydenty w zakresie cyberbezpieczeństwa? Podatności (np. błędy oprogramowania).



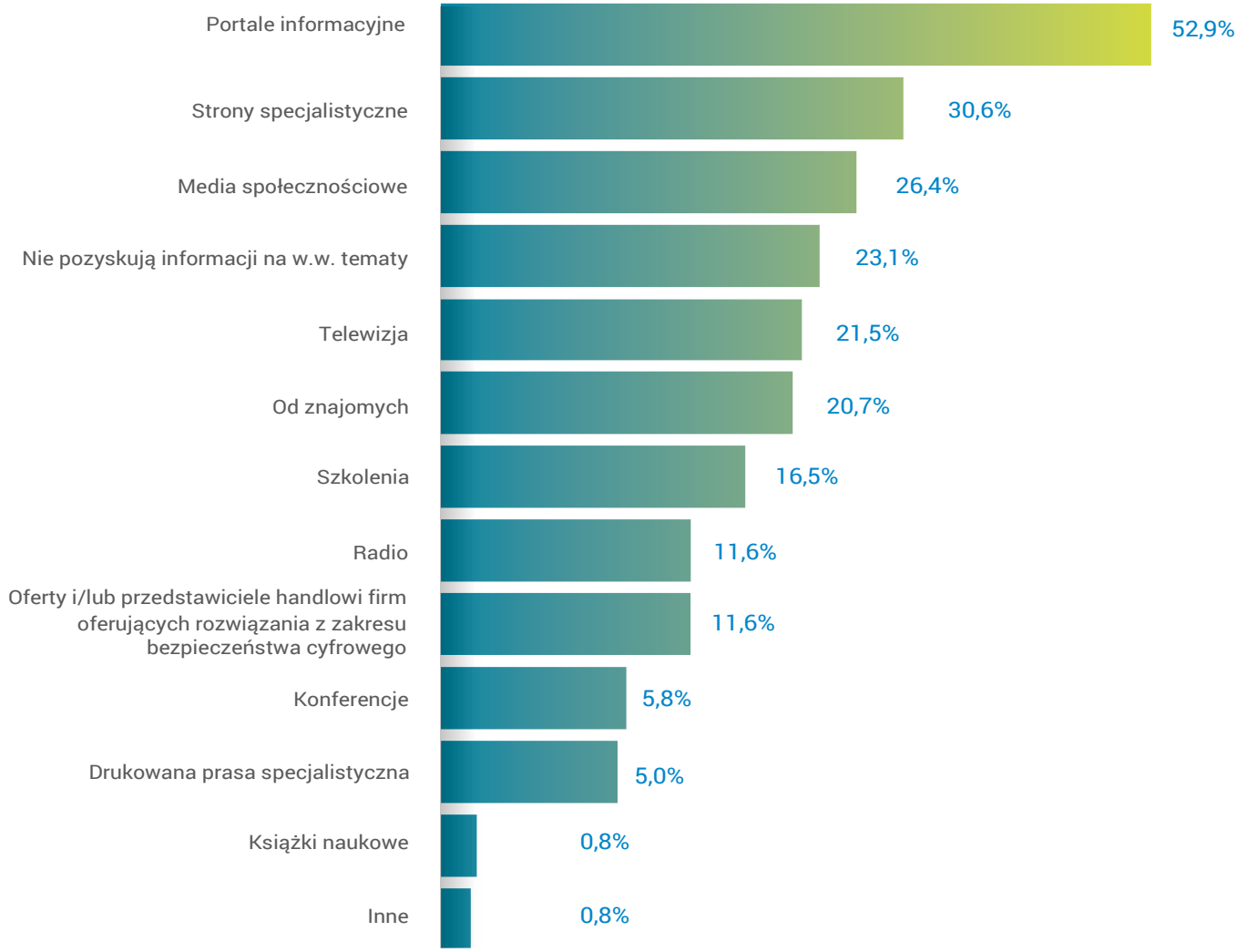
Wykres 29. W jaki sposób w Pana(i) przedsiębiorstwie reaguje się na poniższe incydenty w zakresie cyberbezpieczeństwa? Nielegalne treści (brutalne, pedofilskie itp.).



Straty poniesione wskutek przestępstw teleinformatycznych stanowią poważne zagrożenie dla firm. Dlatego organizowane są liczne kampanie mające na celu zwiększenie świadomości takich zagrożeń. Każda regulacja, taka jak obowiązek ochrony danych osobowych (RODO) oznacza, że na rynku szkoleń pojawiają się nowe produkty mające na celu poszerzenie wiedzy w tym zakresie. Z badań wynika, że wiedzę z zakresu bezpieczeństwa cyfrowego pracownicy małych firm pozyskują przede wszystkim z portali informacyjnych (52,9%), dedykowanych stron (30,6%) i mediów społecznościowych (26,4%). Niemal co czwarty ankietowany wskazał, że „Nie pozyskują informacji na ww tematy" (23,1%). Dość popularnym źródłem jest „Telewizja" (21,5%) i wiedza zaczerpnięta „Od znajomych" (20,7%). Tylko 16,5% badanych wskazuje na szkolenia przypisane bezpieczeństwu cyfrowemu.

Nowe technologie są powszechnie stosowane iłatwo można odnieść wrażenie, że wiedzę na temat ich bezpieczeństwa pozyskuje się z równie powszechnych źródeł. Najpopularniejsze portale informacyjne, czy nawet serwisy społecznościowe, są coraz częściej podstawowymi źródłami informacji. Małe inwestycje na szkolenia czy konferencje łatwo wytłumaczyć kosztami jakie one generują. Przedsiębiorcy, żeby zainwestować muszą ocenić ryzyko związane z niewiedzą.

Wykres 30. Z jakich źródeł najczęściej pozyskują wiedzę z zakresu bezpieczeństwa cyfrowego pracownicy firmy?



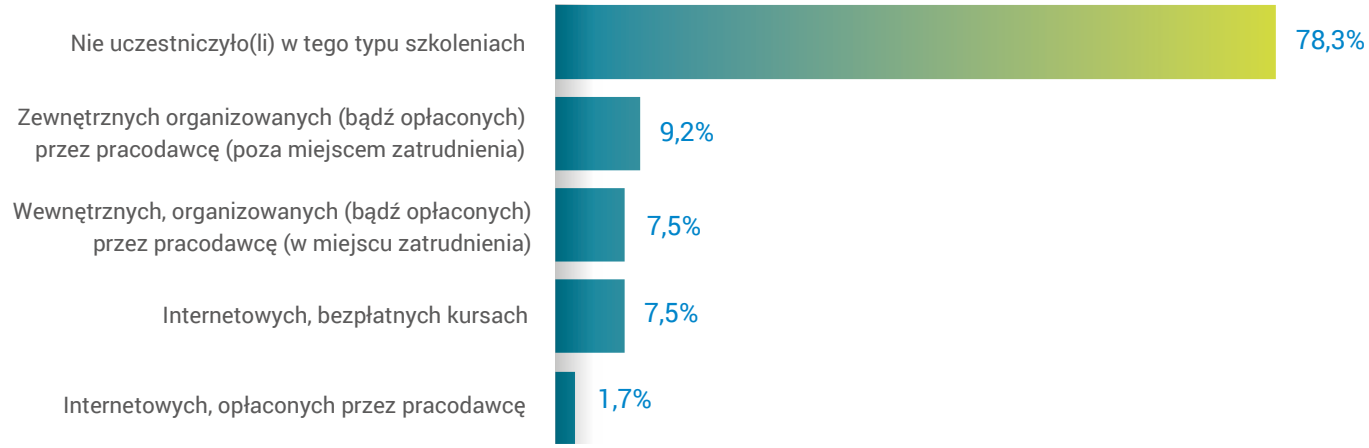
Audyty, kursy i warsztaty z cyberbezpieczeństwa są kierowane nie tylko do dużych organizacji. Szkolenia mają rozmaite formy i dostosowują zakres do potrzeb poszczególnych branż. Poza stacjonarnymi wersjami coraz większą popularność zdobywają szkolenia e-learningowe, które eliminują problemy związane z odległością.

Z danych wynika, że przedsiębiorcy nie inwestują w szkolenia i nie uczestniczą w nich (78,3%). Mniej niż co dziesiąty przedstawiciel firmy, w ostatnich 12 miesiącach, uczestniczył w szkoleniach bądź kursach „Zewnętrznych organizowanych (bądź opłaconych) przez pracodawcę (poza miejscem zatrudnienia)" (9,2%) lub „Wewnętrznych, organizowanych (bądź opłaconych) przez pracodawcę (w miejscu zatrudnienia)" (7,5%).

Nawet darmowe formy szkoleń internetowych nie są popularne wśród ankietowanych (7,5%).

To, że kursy dedykowane bezpieczeństwu są według małych firm zbędnym wydatkiem i nie ma powodu aby angażować na nie czas pracowników, można wytłumaczyć wskazaniami na pytanie o źródła wiedzy. Jeśli takie informacje można czerpać z ogólnie dostępnych portali informacyjnych i mediów społecznościowych, to nie ma powodu aby dodatkowo angażować się w kursy i szkolenia.

Wykres 31. Czy w ostatnich 12 miesiącach kierownictwo firmy (i/lub osoby odpowiedzialne za cyberbezpieczeństwo) uczestniczyło(li) w kursach i/lub szkoleniach z zakresu bezpieczeństwa cyfrowego?

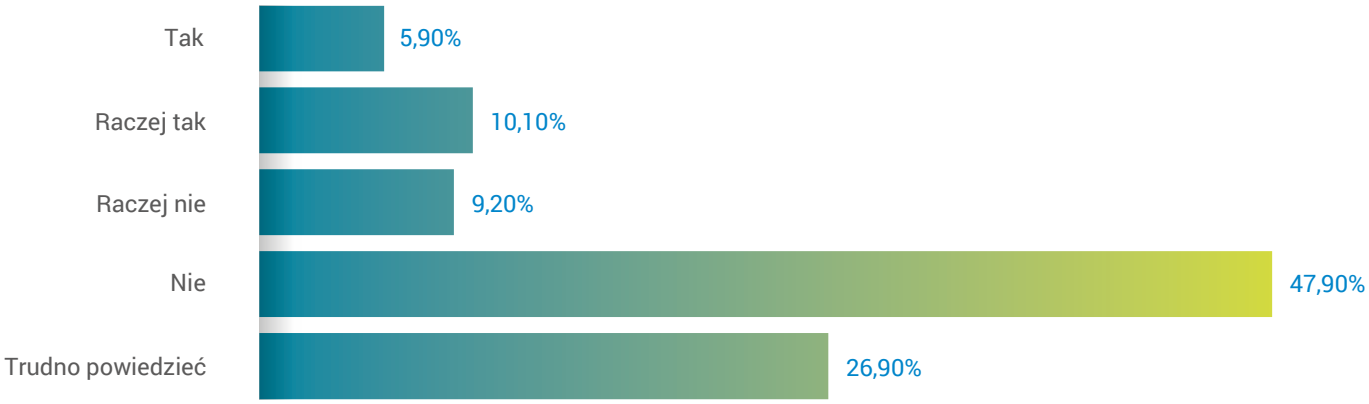


Strategia Cyberbezpieczeństwa Rzeczypospolitej Polskiej na lata 2017-2022 jest kontynuacją działań podejmowanych w przeszłości przez administrację rządową i ma na celu zapewnienie wspólnego wysokiego poziomu bezpieczeństwa sieci i informacji. W odniesieniu do przedsiębiorstw z branż, które nie są uznane za strategiczne, procedura nie powoduje nałożenia nowych obowiązków ani sankcji za ewentualne zagrożenia dla cyberbezpieczeństwa. Strategia natomiast w sposób niewiążący wskazuje cel ogólny – podniesienie świadomości w zakresie bezpieczeństwa cyfrowego.

Do niestosowania Strategii Cyberbezpieczeństwa Rzeczypospolitej Polskiej na lata 2017-2022 przyznaje się więcej jak połowa ankietowanych (57,1%), a częściej niż co czwarty przedsiębiorca, nie jest w stanie tego określić (26,90%). Tylko 16,0% przedsiębiorców deklaruje stosowanie się do wymogów.

Takie odpowiedzi potwierdzają brak wiedzy na temat tego, które regulacje prawne wynikają ze strategii, która w sensie faktycznym wywołuje skutki prawne jedynie dla wąskiej grupy firm, współpracujących z podmiotami publicznymi w ramach realizacji zadań istotnych dla bezpieczeństwa publicznego. Można domniemywać zatem, że świadomość przyjęcia i wdrażania Strategii wśród badanych firm MMŚP jest niewielka.

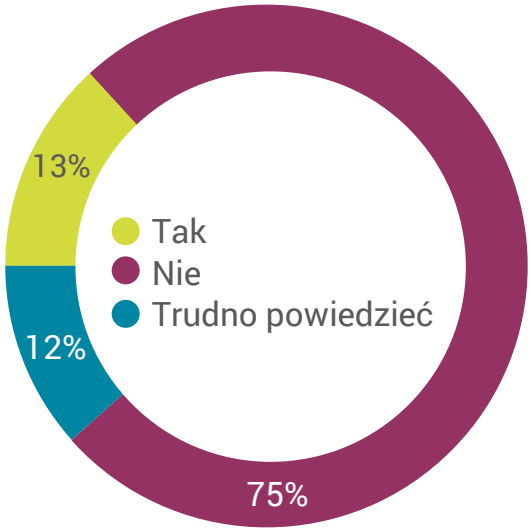
Wykres 32. Czy w Pana(i) przedsiębiorstwie stosuje się zasady wynikające ze Strategii Cyberbezpieczeństwa Rzeczypospolitej Polskiej na lata 2017-2022?



Scenariusze reagowania na incydenty oraz ochrona danych i systemów minimalizuje ryzyko naruszenia bezpieczeństwa. W tym tworzone są dokumenty regulujące politykę cyberbezpieczeństwa. Powinny one mieć spisany cel, strategię i działania określające sposób zarządzania danymi. Takie dokumenty pozwalają podnosić świadomość pracowników na temat zagrożeń i związanego z nimi ryzyka. W małych przedsiębiorstwach nie ma takich dokumentów, na co wskazuje ¾ ankietowanych (75,2%). Tylko nieliczni tworzą takie wewnętrzne regulacje (13,2%), a pozostali nie są pewni czy taki dokument istnieje w ich firmie (11,6%).

Wyniki potwierdzają wcześniejsze deklaracje dotyczące traktowania cyberbezpieczeństwa jako problemu ważnego tylko dla dużych organizacji. Dopiero większe firmy, z wyspecjalizowanymi działami, pokazują, że mają świadomość i wprowadzają procedury, zasady bezpieczeństwa oraz dbają o własne dane.

Wykres 33. Czy w Pana(i) przedsiębiorstwie istnieje dokument regulujący politykę firmy w zakresie cyberbezpieczeństwa?

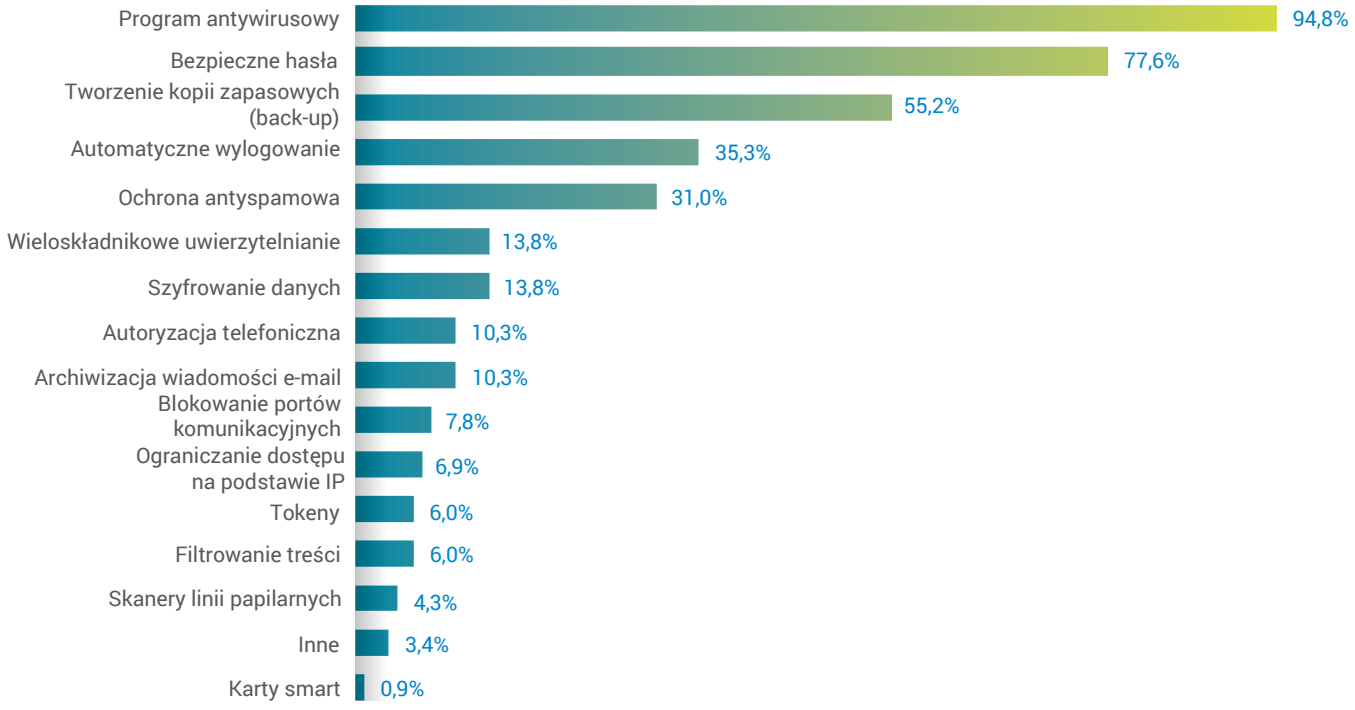


Wybór odpowiednich zabezpieczeń technicznych pozwala na minimalizowanie niebezpieczeństwa utraty zasobów w sieci. Same procedury i rozwiązania systemowe nie są dostateczną ochroną. W danym środowisku funkcjonuje użytkownik i najczęściej to on jest najsłabszym ogniwem zabezpieczenia. Dlatego w oferowanych na rynku rozwiązaniach wskazuje się nie tylko na dopasowanie do wymogów branżowych, ale też ryzyko błędów ludzkich.

Najpopularniejszą formą ochrony danych w małych firmach jest instalowanie programów antywirusowych (84,8%) i stosowanie bezpiecznych haseł (77,6%). Tworzenie zapasowych kopii (back up) deklaruje ponad połowa ankietowanych (55,2%), a więcej jak 30% wskazuje na „Automatyczne wylogowanie" (35,3%) oraz „Ochronę antyspamową" (31,0%). Wszystkie pozostałe sposoby ochrony są zdecydowanie rzadziej stosowane.

Przekonanie o skuteczności programów antywirusowych potwierdzają dane z pogłębionych wywiadów. Tylko respondenci z większych firm uważają za zasadne rozszerzanie strategi bezpieczeństwa o inne narzędzia i wprowadzanie polityki bezpieczeństwa cyfrowego. Dla pozostałych inwestowanie w ten obszar jest zbędne.

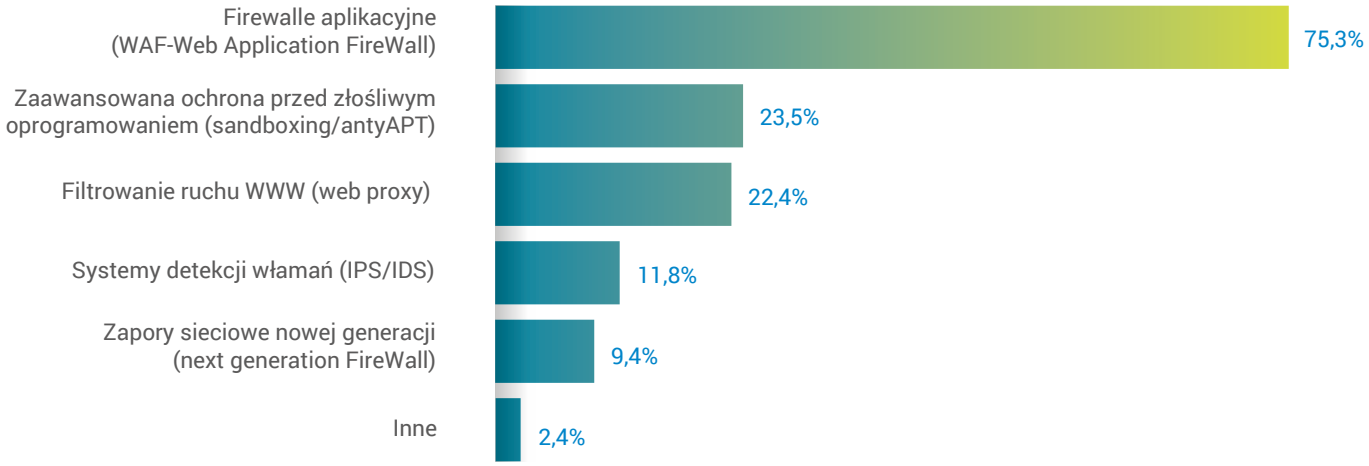
Wykres 34. Jakie formy ochrony bezpieczeństwa danych stosuje się w Pana(i) przedsiębiorstwie?



Przedsiębiorcy, jako administratorzy danych, muszą dostosować do regulacji prawnych nie tylko procedury wewnętrzne, ale też narzędzia. W treści rozporządzenia RODO wiele przesłanek wskazuje na wymogi funkcjonalne dotyczące interfejsu użytkownika, oprogramowania, systemów do backupu i archiwizacji danych oraz poziomu bezpieczeństwa. W większości mikrofirm (75,3%) wykorzystuje się systemy ochrony aplikacji webowych (stron internetowych). Więcej jak 1/5 tych firm korzysta z zaawansowanych rozwiązań ochrony antywirusowej (23,5%) oraz „Funkcji filtrowania ruchu www." (22,4%). Korzystanie z systemów detekcji włamań deklaruje 13,8%, a z zapór sieciowych nowej generacji 9,4%.

Wybór "firewalli" wydaje się być oczywisty nie tylko ze względu na przedmiot ochrony, ale też ze względu na liczbę rozwiązań tego typu na rynku. Miedzy innymi dostępne są uniwersalne rozwiązania komercyjne, dające użytkownikom swobodę działania. Natomiast złośliwe oprogramowania stanowią realne zagrożenie, dlatego należy się odpowiednio przed nimi zabezpieczyć, a według przedsiębiorców wystarczającą ochroną są inwestycje w droższe systemy zabezpieczające.

Wykres 35. Jakie narzędzia ochrony bezpieczeństwa danych stosuje się w Pana(i) przedsiębiorstwie?

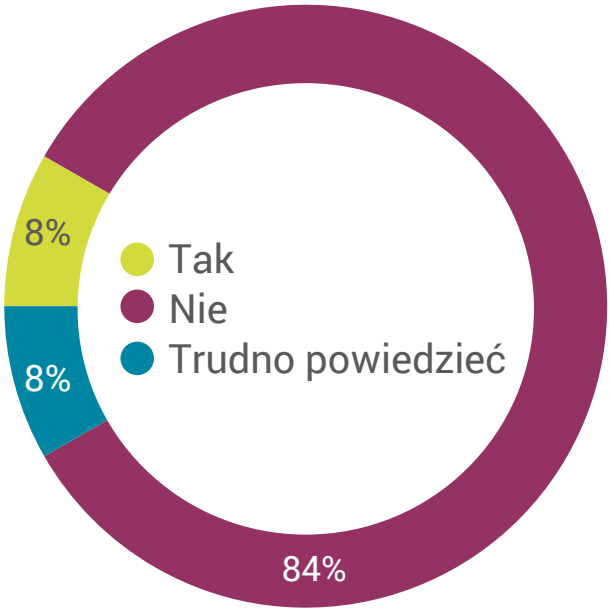


Audyt rozumiany jako porównanie stanu rzeczywistego z określonym wzorcem jest stosowany również do określania poziomu cyberbezpieczeństwa. Regulacje takie jak wewnętrzne procedury, strategie czy polityka cyfrowa firmy są punktem odniesienia w procesie kontroli. Weryfikacja rozwiązań technicznych i organizacyjnych jest niezbędna do określenia czy system informatyczny spełnia wymogi bezpieczeństwa i nie ma „luk", które mogą spowodować utratę danych. Większość, bo aż 83,5% ankietowanych, zaprzecza aby audyty bezpieczeństwa cyfrowego miały miejsce w ich firmie w ostatnich 12 miesiącach. Potwierdza takie działania tylko 8,3% respondentów.

Wynik tłumaczą odpowiedzi na pytania o inwestycje w infrastrukturę i jej ochronę. W mikorprzedsiębiorstwie nie ma potrzeby użytkowania rozbudowanych systemów, które należy chronić i z tego powodu przeprowadzenie audytu wydaje się bezzasadne.

Zarządzanie uprawnieniami użytkowników w systemie informatycznym chroni przed niepożądanym dostępem do danych. W dużych firmach jest naturalnym następstwem centralnego zarządzania procesami i przypisywania poszczególnych uprawnień adekwatnym do zakresu obowiązków i pełnionej funkcji. Generuje jednocześnie problemy takie jak złamania kodów dostępu czy np.: podszywanie się pod inne

Wykres 36. Czy w ostatnich 12 miesiącach w przedsiębiorstwie został przeprowadzony audyt bezpieczeństwa cyfrowego?



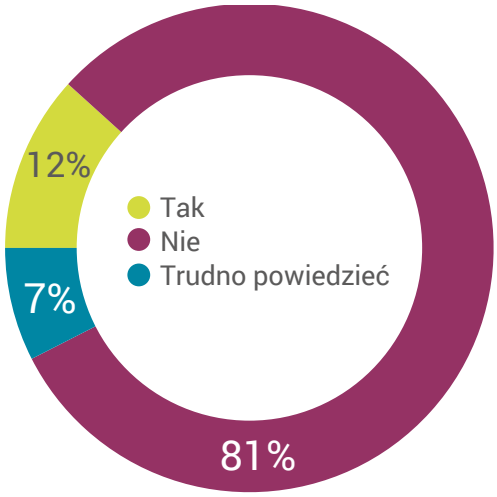
osoby. W małych przedsiębiorstwach prawie nie stosuje się takich rozwiązań (80,8%). Jest to niewątpliwie związane z mikroinfrastrukturą IT i małą liczebnością zatrudnienia. Jeśli w firmie pracuje kilka osób to nie ma potrzeby stosowania cyfrowych zabezpieczeń, bo nie występują takie systemy, które są rozbudowaną bazą danych.

Systemy informatyczne nie tylko składają się z wielu powiązanych ze sobą komponentów, ale przede wszystkim stale się przekształcają. Na rynku powstają nowe rozwiązania i w tym samym czasie powstają nowe zagrożenia. To generuje potrzebę monitorowania i modyfikacji infrastruktury cyfrowej. Jednak ponad 70% respondentów stwierdziła, że w ciągu ostatnich 12 miesięcy w ich firmie nie wprowadzono nowych rozwiązań w obszarze bezpieczeństwa cyfrowego (77,7%). Z pogłębionych wywiadów wynika, że dbałość o wdrażanie nowych rozwiązań jest bezpośrednio związana z wielkością firmy, czasem funkcjonowania i rodzajem branży. Im większa firma tym chętniej i częściej wdraża nowe produkty bezpieczeństwa. Bez względu na wielkość i czas funkcjonowania na rynku, firmy z branży IT dbają o bezpieczeństwo.

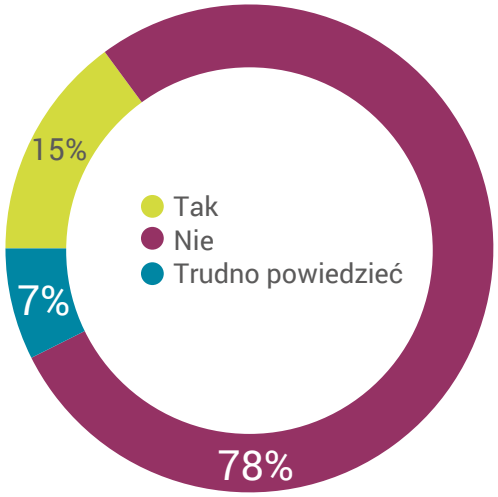
Największą motywacją do zachowania bezpieczeństwa cyfrowego są dla firmy „Przepisy prawa narzucające standardy" (52,3%). Kolejnym predykatorem jest obawa przed cyberprzestepczością (36,7%), chęć utrzymania wysokiego poziomu bezpieczeństwa w firmie (28,4%) i subiektywna ocena ryzyka (28,4%). „Wymagania kontrahentów" nie są już tak mocnym stymulatorem (16,5%) podobnie jak „Wymagania rynku (konkurencja)" (10,1%).

Przedsiębiorcy reagują w pierwszej kolejności na obligacje prawne bo, niestosowanie się do zobowiązań może skutkować karami finansowymi i stanowić zagrożenie funkcjonowania. Cyberprzestepczość również generuje ryzyko utraty zasobów (finansowych czy innych aktywów) i to jest w ich odczuciu realne niebezpieczeństwo.

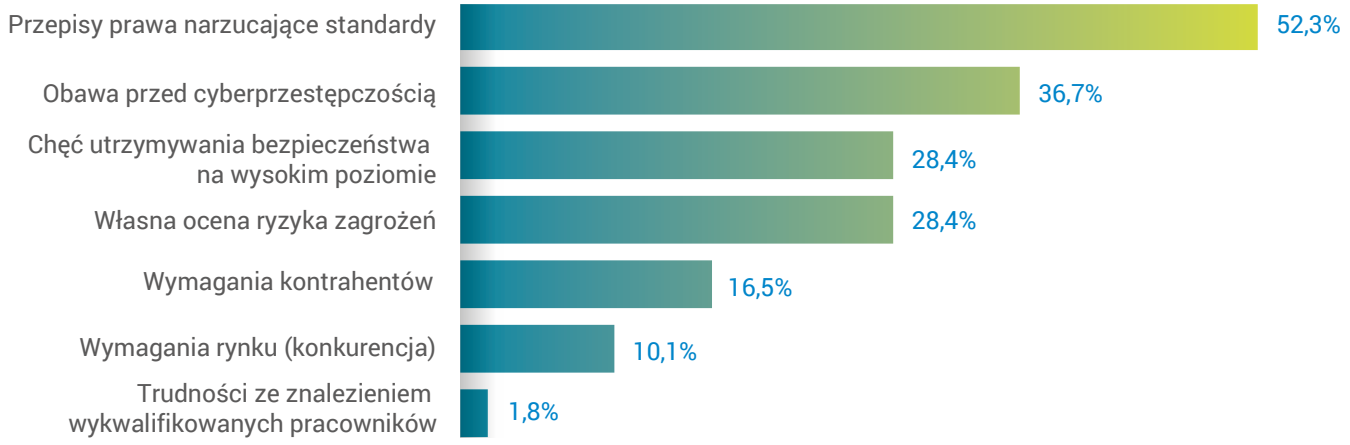
Wykres 37. Czy w Pana(i) przedsiębiorstwie funkcjonują procedury zarządzania tożsamością cyfrową (różne poziomy uprawnień cyfrowych w ramach organizacji)?



Wykres 38. Czy w ciągu ostatnich 12 miesięcy wprowadzono w Pana(i) przedsiębiorstwie nowe rozwiązania w obszarze bezpieczeństwa cyfrowego?



Wykres 39. Co według Pana(i) w największym stopniu wpływa na motywację do zachowania bezpieczeństwa cyfrowego w Pana(i) przedsiębiorstwie?"



Podsumowanie

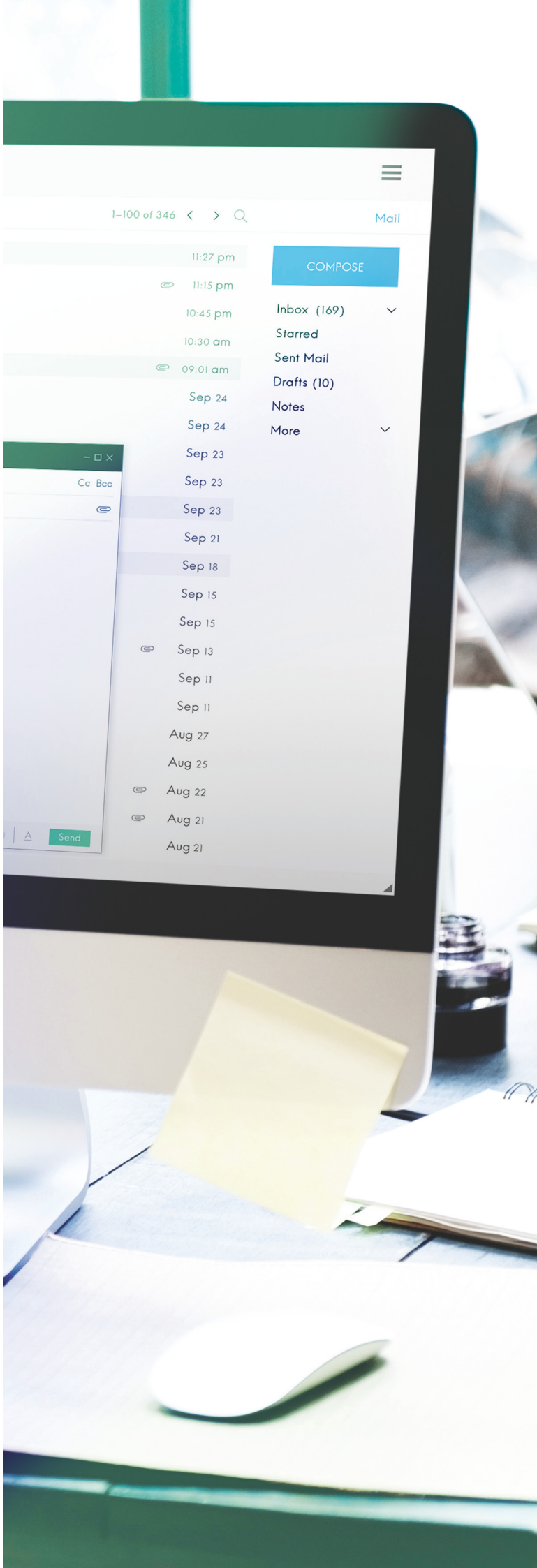
Prawie 70% badanych przedstawicieli drobnego biznesu deklaruje, że samodzielnie radzi sobie z problemem potencjalnie niebezpiecznych załączników w korespondencji elektronicznej. Nieco ponad połowa podobnie rozwiązuje problemy z kwestiami podejrzanej bądź fałszywej tożsamości kontrahentów, a sprawę policji lub odpowiednim służbom zgłasza ok ¼ firm. W przypadku problemów z oprogramowaniem, większość firm w rozwiązaniu problemu szuka wsparcia zewnętrznych firm i specjalistów.

Wiedzę o cyberbezpieczeństwie ponad połowa badanych czerpie z ogólnodostępnych portali informacyjnych, co czwarty z mediów społecznościowych, a co piąty z telewizji.

Mniej niż co trzeci badany korzysta w tym celu z internetowych serwisów specjalistycznych, a jedynie co siódmy rozwija swoją wiedzę i umiejętności w ramach zorganizowanych kursów. Dodatkowo, według badanych z prawie 4/5 firm osoby odpowiedzialne za bezpieczeństwo informatyczne nie uczestniczą w tego typu szkoleniach.

Zdecydowana większość (83%) firm nie miała także przeprowadzonego audytu bezpieczeństwa informatycznego, a także nie wdrożyło w ciągu 12 miesięcy przed badaniem nowych rozwiązań w tym obszarze ¾ badanych firm. Ponad połowa badanych deklaruje, że w ich firmie nie ma dokumentu określającego politykę cyberbezpieczeństwa, a połowa, że ich firma nie realizuje obowiązków wynikających z krajowej strategii cyberbezpieczeństwa.

Zapytani o główne motywacje stojące za ochroną bezpieczeństwa informatycznego firmy i jej klientów, respondenci wskazali przede wszystkim na konieczność dostosowania się do regulacji prawnych oraz lęk przed cyberprzestępcami.

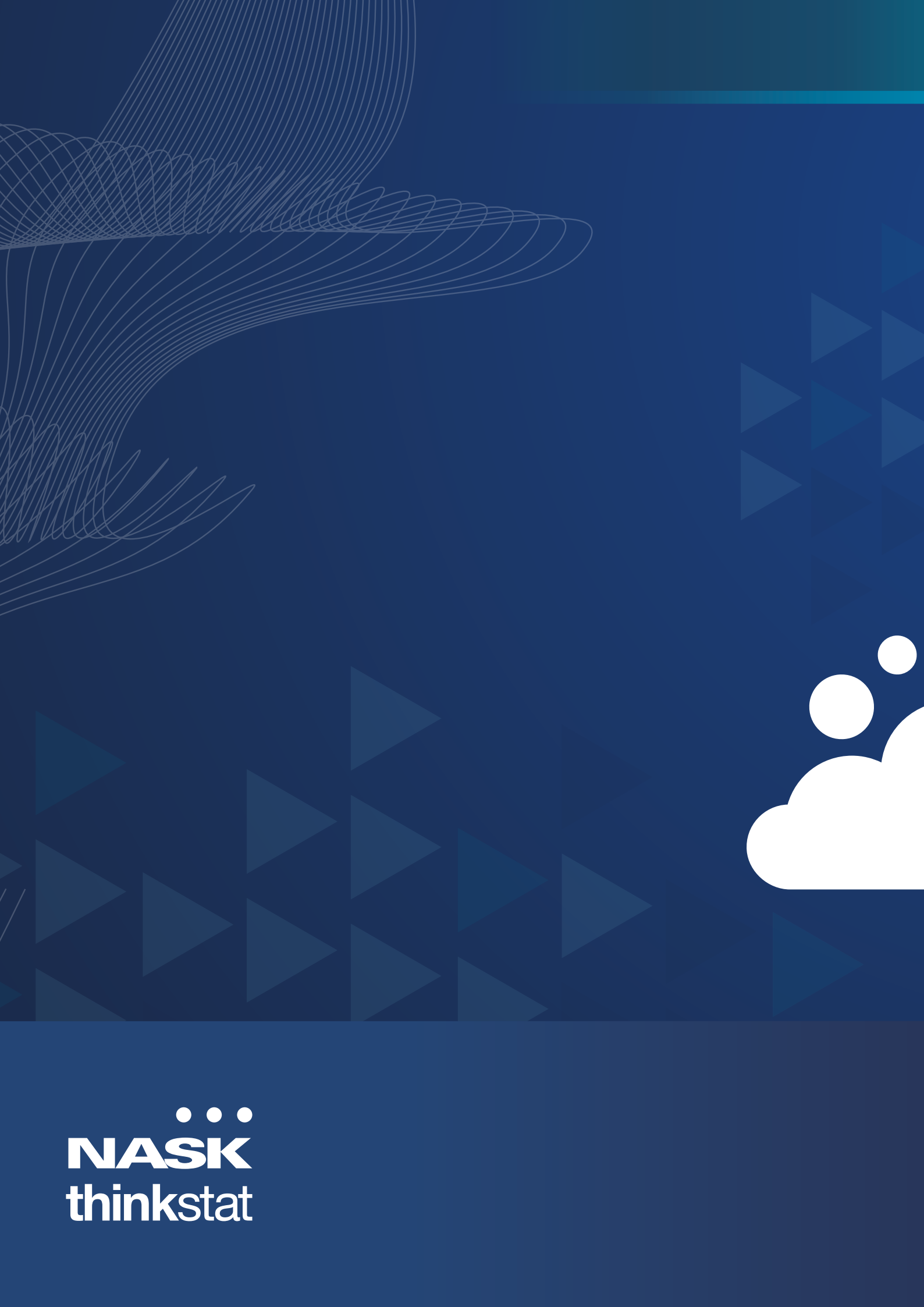


Zakończenie

We współczesnej gospodarce rozwiązania oparte na gromadzeniu i przetwarzaniu danych mają coraz większe znaczenie dla rentowności oraz rynkowej pozycji przedsiębiorstw. Sektor MMŚP w Polsce, w którego skład wchodzą podmioty zatrudniające poniżej 250 osób to przeważająca większość wszystkich przedsiębiorstw. W tej populacji najliczniejszą grupą są mikroprzedsiębiorcy, ponad 2 mln (96,5%), a ich liczba z roku na rok rośnie. Rozwój gospodarki 4.0, czyli transformacji w ramach tzw. czwartej rewolucji przemysłowej, nie jest oparty wyłącznie na komputeryzacji przedsiębiorstw, ale obejmuje integrację szeregu funkcji i procesów: od produkcji, przez logistykę, sferę pracowniczą po marketing czy relacje klientami. Obserwując współczesne trendy ekonomiczne i rynek pracy oraz rozwój innowacji technologicznych należy ocenić, że polskie mikro, małe i średnie przedsiębiorstwa są na ogół za tymi zmianami daleko w tyle. Większość z nich nie weszła nawet jeszcze w pełni w trzecią (tj. komputerowo-internetową) erę rewolucji przemysłowej. Wynika to przede wszystkim z dwóch barier: kapitałowej i kompetencyjnej.

Z badań NASK wynika, że większość przedstawicieli drobnego biznesu ma świadomość stojących przed nimi wyzwań. Dla przykładu, spotykając się z problemami z oprogramowaniem, firmy szukają wsparcia u profesjonalistów, tj. zewnętrznych firm i specjalistów ICT. Większość firm od wielu lat korzysta także często z usług informatycznych w rodzaju fachowego oprogramowania, zdalnego wsparcia technicznego czy pomocy w serwisowaniu sprzętu. Pytani o motywację do ochrony i bezpieczeństwa informacyjnego firmy czy klientów, badani odpowiadali, że jest to warunkowane szczególnie koniecznością dostosowania się do regulacji prawnych oraz lęk przed cyberprzestępcami. Uczestnicy badania deklarują również, że rozwijają swoją wiedzę na tematy z dziedziny cyberbezpieczeństwa, czerpiąc ją głównie z ogólnodostępnych portali informacyjnych, mediów społecznościowych i telewizji.

Niestety, wiele kwestii związanych z prowadzeniem firmy w erze cyfrowej wymaga poprawy. Polscy przedsiębiorcy w coraz większym zakresie gromadzą, przetwarzają i wykorzystują dane osobowe przy użyciu nowych technologii. Jednak analizując wypowiedzi przedstawicieli różnych sektorów i branż można stwierdzić, że bardzo często jako jedyne systemy wspomagające używające przestarzałych i niezintegrowanych procesów kadrowych czy finansowo-księgowych. Drobni przedsiębiorcy nie zdają sobie sprawy z wielu potencjalnych zagrożeń i problemów nie tylko w zakresie rentowności produkcji czy ryzyka bycia zdystansowanym przez konkurencję, ale przede wszystkim w dziedzinie gromadzenia danych osobowych. Dostosowanie się do nowego krajobrazu globalnej i lokalnej gospodarki wymagać będzie dużej sprawności adaptacyjnej oraz umiejętności korzystania ze wsparcia zewnętrznego. Może być ono dostarczane zarówno w formie kapitałowej jak i postaci know-how (nowe procedury, kompetencje itp.) przez instytucje publiczne czy unijne. Jeśli polski sektor MMŚP nie będzie efektywnie korzystał z tego rodzaju zasobów, prawdopodobnie nie będzie w stanie sprostać rosnącej konkurencji, czego owocem będzie utrata dotychczasowej bazy klientów, ich usług lub produktów.


NASK
thinkstat