VECTO

V edycja · 2022

RAPORT

Cyberbezpieczeństwo w polskich firmach

VECTO

DELL TECHNOLOGIES • PLATINUM PARTNER

NOWY POZIOM

partnerstwa

SPIS treści

WSTĘP

Za nami niemal 2 lata pandemii, która wymusiła na wielu polskich przedsiębiorcach konieczność wprowadzenia zmian w zarządzaniu biznesem i poszukiwania nowych form budowania konkurencyjności. Z pewnością, jedną z tych dróg okazała się szeroko pojęta cyfryzacja, której dynamika w rodzimych firmach jest wyraźnie widoczna. Potwierdzają to również dane Głównego Urzędu Statystycznego. W 2021 roku z usług w chmurze korzystało już prawie 29 proc. przedsiębiorstw. Wzrostom uległ również proces wykorzystania technologii w e-handlu – z uruchomienia internetowego kanału sprzedaży produktów i usług korzysta dziś niemal co piąta firma (18 proc.). Jeszcze lepiej prezentuje się wskaźnik korzystania przez polskie firmy z mediów społecznościowych, bowiem już ponad połowa przedsiębiorstw aktywnie komunikuje się na kanałach social media (55 proc.), a w kategorii dużych firm odsetek wyniósł niemal 70 proc.

Rozwój cyfryzacji jest oczywiście procesem pożądanym i trudno dziś myśleć o sukcesie w biznesie bez wykorzystania narzędzi IT. Rewolucja technologiczna, której jesteśmy świadkami, poza szansami niesie jednak szereg zagrożeń, których niedostrzeganie może być dla każdej firmy druzgocące. Polska jest niezmiennie w gronie państw szczególnie narażonych na aktywność cyberprzestępców. Codzienne doniesienia o próbach lub skutecznych atakach hakerskich na polskie firmy są zresztą tego najlepszym dowodem. Obserwujemy to również w zwiększonej liczbie zapytań, kierowanych do VECTO, odnośnie możliwości zabezpieczenia integralności danych lub ich odzyskania, gdy zasoby IT zostały zainfekowane szkodliwym oprogramowaniem, np. ransomware.

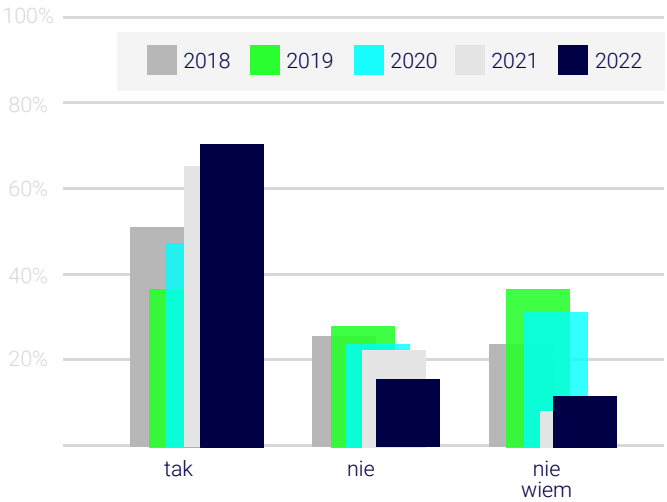
W tegorocznym Raporcie: „Cyberbezpieczeństwo w polskich firmach" ponownie diagnozujemy stan gotowości przedsiębiorstw do przeciwdziałania cyberprzestępczości oraz analizujemy stosowane zabezpieczenia, których zadaniem jest ochrona danych firmowych i systemów IT. Gorąco zachęcam Państwa do lektury tym bardziej, że w badaniu pojawiły się również nowe pytania, a zgromadzona wiedza pozwoli firmom o mniejszej świadomości zagrożeń, obrać właściwy kurs i skutecznie zadbać o bezpieczeństwo informatyczne.

Jakub Wychowański
Prezes Zarządu VECTO Sp. z o.o.

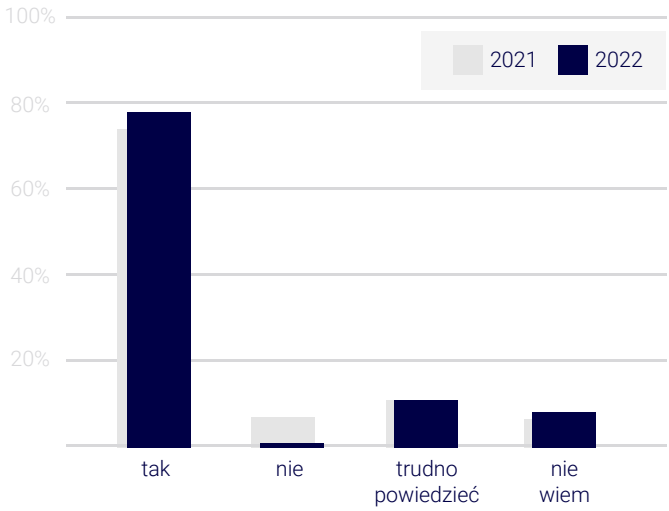
ZACZNIJMY

z wysokiego C

Powszechność wykorzystania narzędzi IT w biznesie przełożyła się bezpośrednio na wzrost liczby groźnych cyberincydentów. W porównaniu z ubiegłorocznym badaniem, zwiększył się odsetek firm, które potwierdziły próbę lub skuteczną ingerencję w bezpieczeństwo danych i wynosi on już 69,93 proc. To znacząca różnica względem danych ubiegłorocznych – o ponad 8 punktów procentowych. Ransomware oraz inne szkodliwe oprogramowanie, ataki hakerskie, blokady systemów i procesów informatycznych to dziś, jak nigdy wcześniej, absolutnie realne zagrożenie dla każdej firmy bez względu na jej wielkość, poziom zatrudnienia czy osiągane wyniki finansowe. Problem ten dotyczy również instytucji, jednostek samorządowych czy nawet urzędów centralnych. Przechwytywanie i publikowanie poufnej korespondencji dotknęło bowiem również członków polskiego rządu, choć w tym przypadku zawiniły przede wszystkim niedoskonałe procedury i brak ostrożności wysokich funkcjonariuszy państwowych wykorzystujących niezabezpieczone skrzynki mailowe.

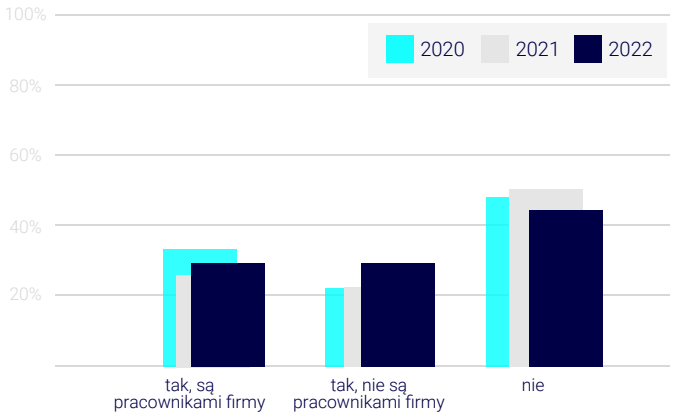


Czy twoja firma zetknęła się kiedykolwiek z cyberatakiem?



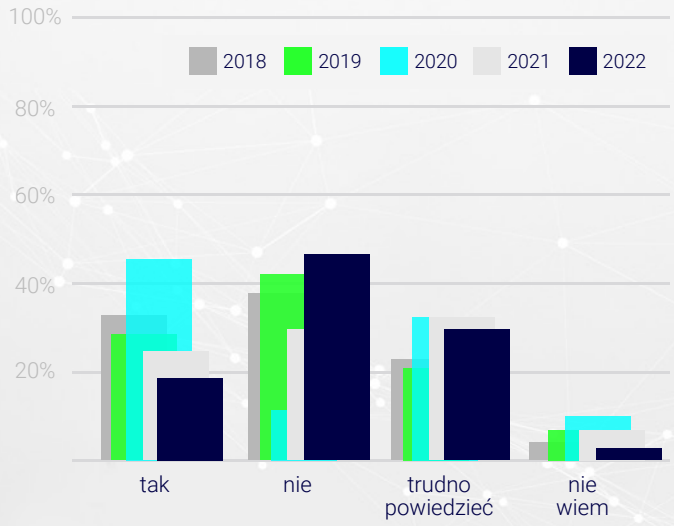
Czy uważasz, że zabezpieczenie danych informatycznych w firmie jest ważne?

Z pewnością zwiększona liczba cyberincydentów przekłada się na wzrost świadomości użytkowników infrastruktury IT w badanych firmach. Choć w zdecydowanej większości uważają oni, że zabezpieczenie informatyczne jest ważne dla każdej firmy (78,16 proc.), to jednak niemal 44 proc. ankietowanych przyznaje, że ich firma nie korzysta z usług ekspertów od cyberbezpieczeństwa – nie zatrudnia informatyków lub wyspecjalizowanych w tym zakresie podmiotów zewnętrznych.

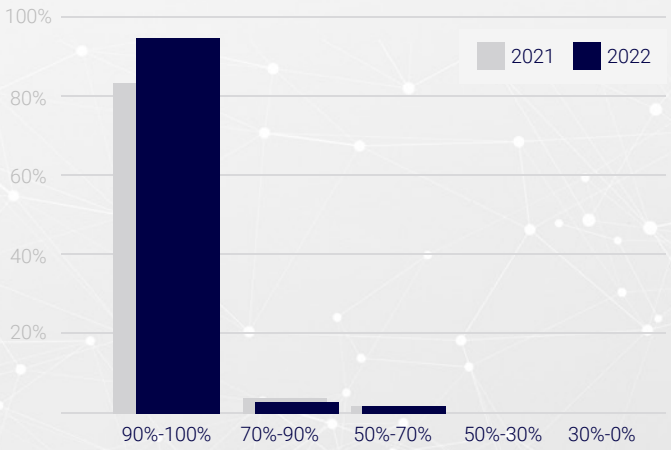


Czy twoja firma zatrudnia specjalistę od bezpieczeństwa danych?

Prawie identyczny odsetek badanych wskazał, że ich firmowa sieć nie jest prawidłowo zabezpieczona, co może nasuwać wniosek, że brak dostępu do wyspecjalizowanych usług wpływa na poczucie bezpieczeństwa samych użytkowników. W porównaniu z wynikami poprzedniego Raportu spadł również odsetek badanych, którzy uważają, że zasoby IT w ich firmach są dobrze chronione – wyniósł on niecałe 20 proc. Jest to o tyle istotne, że już 94,98 proc. osób potwierdza, że 90-100 proc. pracowników ma dostęp do infrastruktury informatycznej, co również dowodzi, jak dynamicznie zmienia się stopień cyfryzacji polskich przedsiębiorstw (wzrost o 3,5 proc. względem badania 2021). Z pewnością wpływ na te wyniki ma upowszechnienie modelu pracy zdalnej, którego skuteczność jest uwarunkowana dostępem do firmowej infrastruktury IT.



Czy uważasz, że sieć w twojej firmie jest prawidłowo zabezpieczona?



Jaki procent pracowników twojej firmy ma dostęp do firmowej infrastruktury IT?

JAK

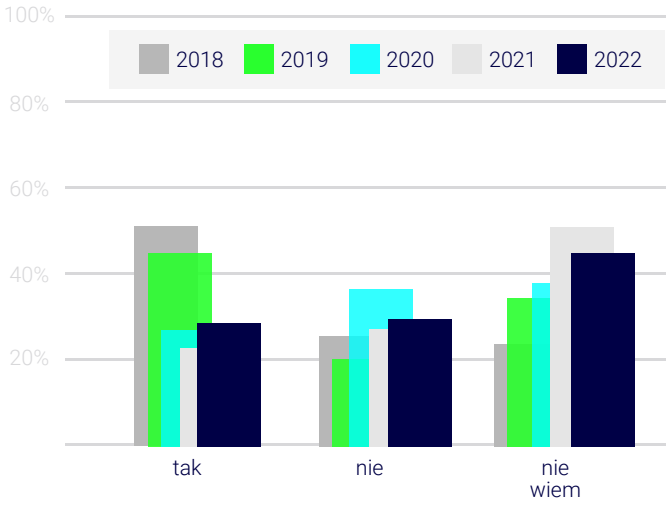
się zabezpieczamy?

Polskie firmy, według opinii 38 proc. respondentów, nie monitorują zagrożeń wynikających z cyberprzestępczości. Przeciwnego zdania jest co czwarty ankietowany, zaś 35 proc przyznało, że nie ma wiedzy na temat podejmowanych przez pracodawcę działań w tym zakresie. Zważywszy jednak na fakt, że tylko 14,68 proc. firm ma przygotowany scenariusz postępowania w przypadku wystąpienia incydentu naruszającego bezpieczeństwo danych, można wnioskować, że choć świadomość rośnie, to nie przekłada się ona na realne działania prewencyjne lub strategię minimalizacji kosztów skutecznie przeprowadzonych ataków. Odsetek firm przyznających, że takich procedur nie wdrożono wyniósł 39 proc., odpowiedź „nie wiem" wskazało aż 45,84 proc. ankietowanych. Nieznajomość procedur dotyczących postępowania po naruszeniu integralności danych skłania do wniosku, że w przytłaczającej większości firm takie procedury nie istnieją lub są źle komunikowane pracownikom.

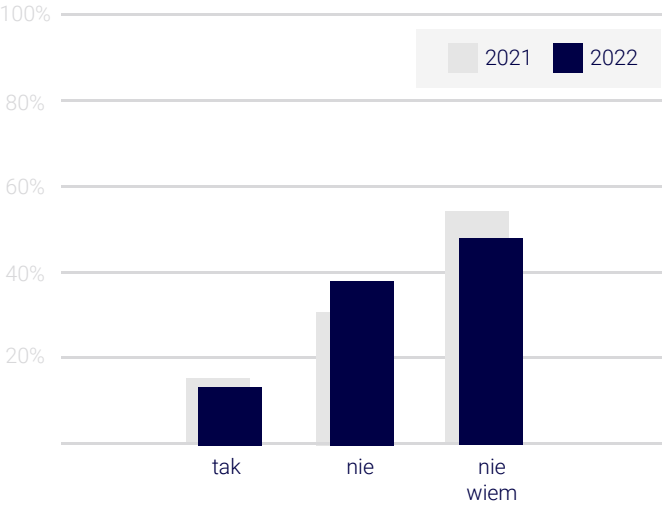
tylko

14,68 proc. firm

ma przygotowany scenariusz reagowania w przypadku wystąpienia cyberataku

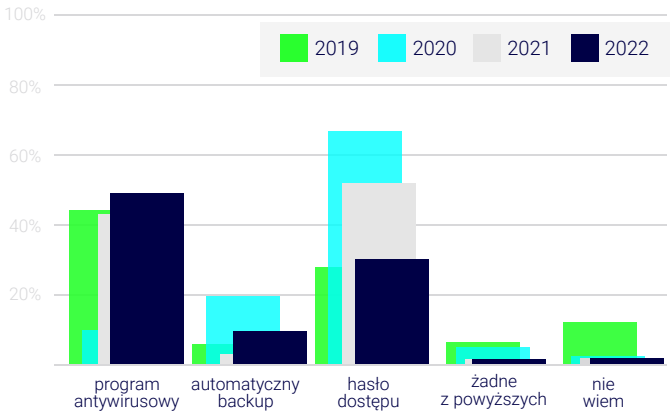


Czy twoja firma monitoruje zagrożenia wynikające z cyberprzestępczości?



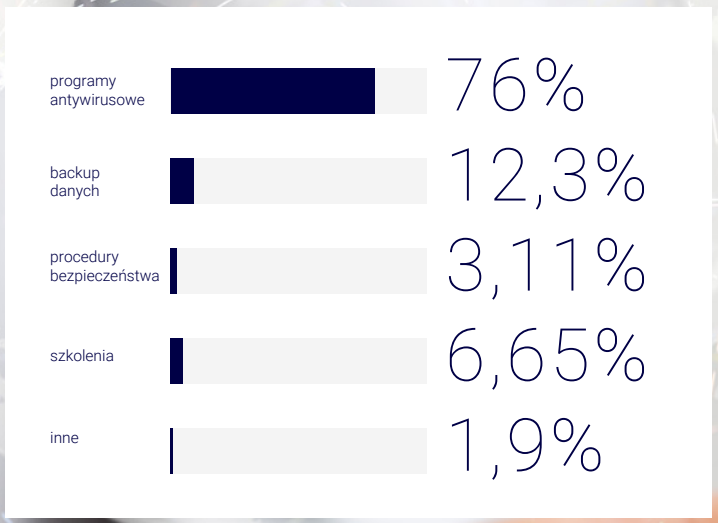
Czy twoja firma ma przygotowany scenariusz postępowania w przypadku wystąpienia incydentu naruszającego bezpieczeństwo danych?

W ocenie respondentów badania, najskuteczniejszą metodą ochrony przed cyberzagrożeniami są programy antywirusowe. Taką odpowiedź wskazało 76,21 proc. ankietowanych. Względem ubiegłorocznego badania wzrósł również odsetek wskazujących rozwiązania z zakresu backup'u danych – 12,13 proc. Szkolenia wskazało 6,65 proc, procedury bezpieczeństwa zaś 3,11 proc. Połowa wszystkich użytkowników komputerów służbowych przyznała, że sprzęt jest zabezpieczony programem antywirusowym (49,59 proc.), a na 10,84 proc. urządzeń jest zainstalowane również rozwiązanie zapewniające automatyczny backup. Z haseł dostępu korzysta 29 proc. respondentów. Brak jakichkolwiek zabezpieczeń deklaruje tylko 1,73 proc. pytanych.

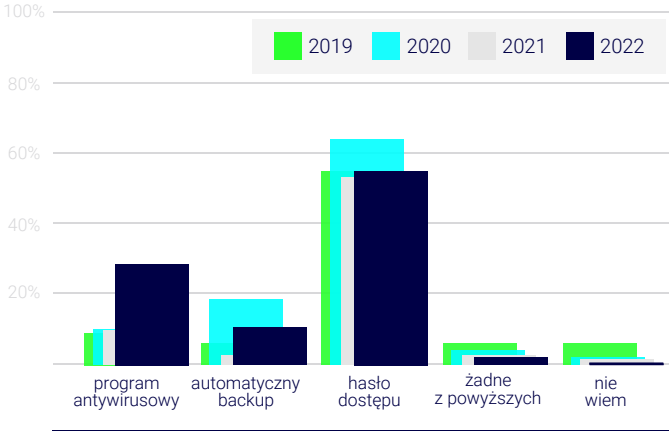


W jaki sposób zabezpieczone są komputery w twojej firmie?

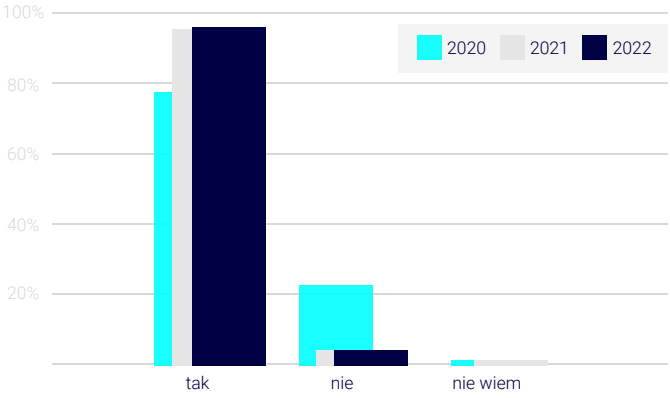
Wybierz metodę, która twoim zdaniem jest najskuteczniejszą w ochronie przed cyberzagrożeniami.



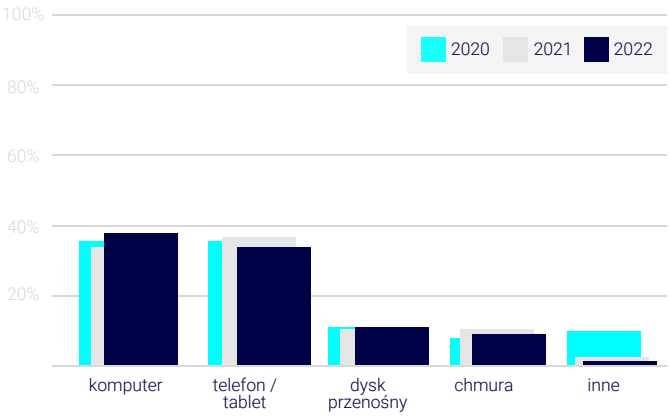
W zakresie urządzeń mobilnych, firmy do zabezpieczenia danych najczęściej stosują hasła dostępu (55,47 proc.), oprogramowanie antywirusowe (28,11 proc.) i backup (12,04 proc.). Większość wymienionych narzędzi zanotowała wzrost poziomu ich wykorzystania względem ubiegłorocznego badania. To dobry trend zważywszy na fakt, że aż 96 proc. badanych potwierdziło, że sprzęt firmowy wykorzystuje również do celów prywatnych, wymiany korespondencji, przeglądania Internetu, rozrywki i aktywności w mediach społecznościowych. Zabezpieczenie komputerów i urządzeń mobilnych jest tym bardziej istotne, że to właśnie na nich najczęściej przechowujemy najcenniejsze dane – te odpowiedzi respondentów zyskały odpowiednio niemal 40 proc. i 34 proc.



W jaki sposób zabezpieczone są urządzenia mobilne w twojej firmie?



Czy używasz firmowego komputera/telefonu do celów prywatnych?



Gdzie przechowujesz najcenniejsze dla siebie dane?

Czy Twoja firma realizuje wytyczne wskazane dyrektywą RODO?

16 proc.

szyfruje dane osobowe

36 proc.

zabezpiecza systemy IT na wypadek zewnętrznej, nieuprawnionej ingerencji w ich integralność

15 proc.

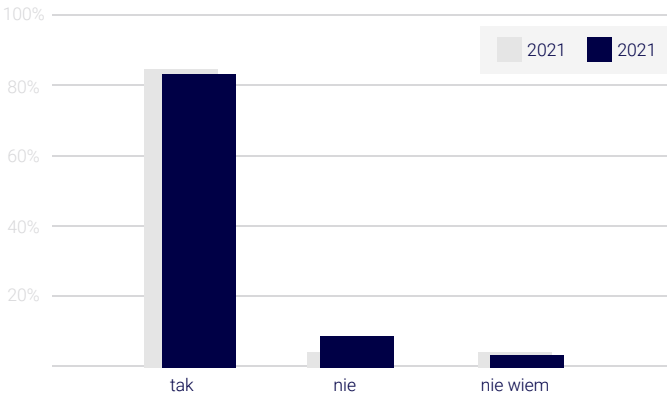
przeprowadza backup i zdolność do szybkiego przywrócenia dostępności danych osobowych i dostępu do nich w razie incydentu fizycznego lub technicznego

9 proc. ankietowanych odpowiedziało, że ich firma nie wprowadza żadnych z powyższych wtycznych, a 23 proc. nie wie jakie zabezpieczenia w zakresie RODO wprowadziła ich firma.

PANDEMIA

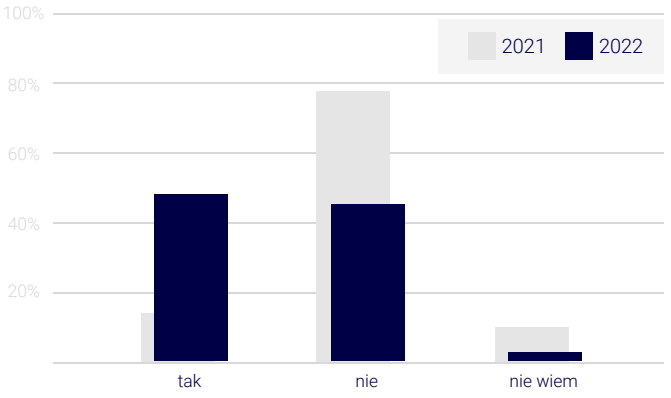
i praca zdalna wymusza inwestycje w IT

Częstsze wykorzystanie hybrydowych modeli pracy i pracy zdalnej przekłada się bezpośrednio na wzrost deklarowanych inwestycji w infrastrukturę IT. Trend ten obserwujemy od początku pandemii i w ostatnim roku został on utrzymany. 83 proc. ankietowanych potwierdza, że ich firmy inwestują w rozwiązania zapewniające zachowanie ciągłości pracy i procesów. Czterokrotnie wzrósł również (względem danych z poprzedniego raportu) odsetek ankietowanych (48,51 proc.), którzy przyznali, że ich firma wdrożyła dodatkowe zabezpieczenia dla pracujących zdalnie. Dynamika ta koresponduje również ze świadomością ankietowanych, że pandemia i wynikająca z niej weryfikacja dotychczasowych systemów pracy zwiększa ryzyko wystąpienia cyberataku. Tego zdania jest 88 proc. respondentów. Z tezą tą nie zgadza się 4,51 proc. uczestników badania.

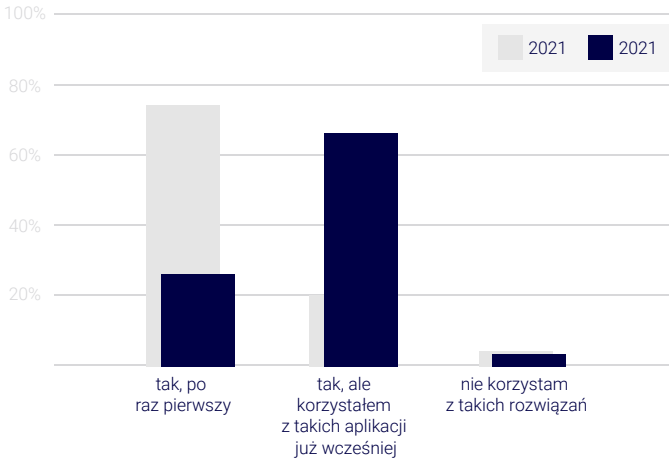


Czy pandemia bezpośrednio wpłynęła na konieczność inwestowania w rozwiązania IT w twojej firmie?

Czy twoja firma wprowadziła dodatkowe zabezpieczenia dla pracowników pracujących zdalnie?



Na to, że praca zdalna dla wielu firm jest już codziennością wskazuje również analiza odpowiedzi na pytanie o wykorzystanie w ostatnim roku komunikatorów video. O ile w poprzedniej edycji Raportu, odpowiedź „tak, po raz pierwszy" wskazało 72 proc. ankietowanych, to w tym roku swój debiut w spotkaniach online potwierdziło już tylko 26,73 proc. respondentów, zaś odpowiedź: „tak, ale korzystałem z takich aplikacji już wcześniej" uzyskała 65 proc., co wyraźnie wskazuje, że spotkania online na stałe zadomowiły się wśród metod komunikacji w zespole i budowania relacji z otoczeniem biznesowym.



Czy w 2021 roku korzystałeś z komunikatorów video?

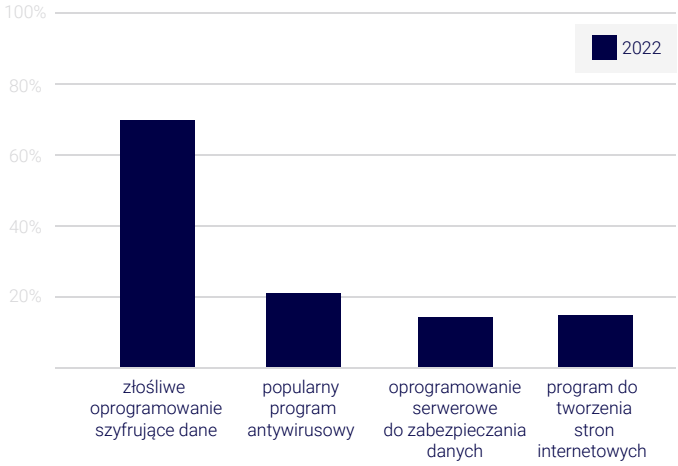
83 proc. ankietowanych

potwierdza, że ich firmy inwestują w rozwiązania IT, aby usprawnić pracę zdalną

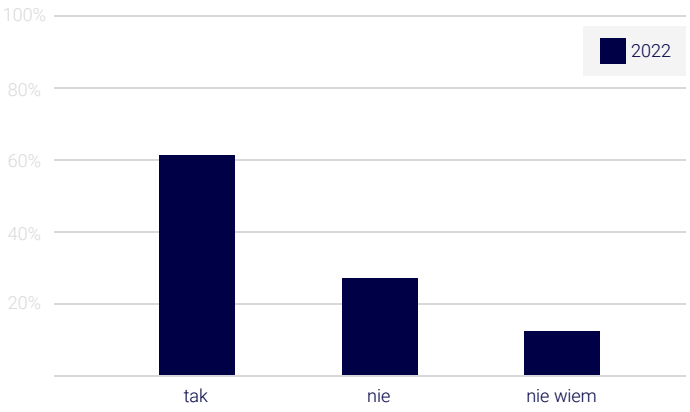
RANSOMWARE

oznacza kłopoty

Ransomware w Polsce zbiera swoje żniwo. Według doświadczeń VECTO, firmy dotknięte tego typu atakami najczęściej wolą zachować to w tajemnicy. Nie brakuje jednak i takich podmiotów, które choćby z tytułu obrotu akcjami na rynku publicznym są zobowiązane do informowania akcjonariuszy o ważnych wydarzeniach, które mogą mieć wpływ na kurs giełdowy. Wiemy zatem, że w ubiegłym roku celem skutecznego ataku hakerskiego stała się między innymi spółka restauracyjna Sfinks, zarządzająca m.in. sieciami Sphinx, Piwiarnia czy Chłopskie Jadło. System IT i dane firmowe zostały zaszyfrowane, wskutek czego o prawie miesiąc opóźniła się publikacja raportów rocznych za 2020 rok. Nie wiadomo jednak, czy spółka zapłaciła okup hakerom za odzyskanie dostępu do zasobów informatycznych.



Ransomware to?



Czy twoja firma byłaby gotowa zapłacić okup za odszyfrowanie przejętych przez hakerów danych?

Ofiarą najbardziej spektakularnego ataku na polskim rynku, który zresztą odbił się echem na całym świecie, stał się CD Projekt RED, producent gier wideo. W lutym 2021 firma utraciła cześć swoich danych, a incydent zakłócił przygotowania do premiery Cyberpunk 2077. Jak informowała spółka, cyberprzestępcy przechwycili kody źródłowe różnych gier. Zagrozili również opublikowaniem dokumentacji firmowej. Firma nie zapłaciła jednak okupu, a zgłoszenie dotyczące ataku hakerskiego przekazała organom ścigania, w tym Interpolowi i Europolowi. W ciągu kilku kolejnych dni, notowania giełdowe CD Projekt RED poszybowały w dół, notując jeden z najmocniejszych spadków wśród największych spółek na warszawskiej giełdzie należących do indeksu WIG20.

Wśród ubiegłorocznych incydentów warto również odnotować atak na Totolotek, jednego z najważniejszych w Polsce organizatorów zakładów bukmacherskich. Nieznani dotąd sprawcy najprawdopodobniej uzyskali dostęp do archiwalnych danych oraz danych osobowych klientów. Incydent został zgłoszony organom ścigania oraz Urzędowi Ochrony Danych Osobowych oraz CERT.

Spółka poinformowała o możliwości przechwycenia przez hakerów loginów, adresów e-mail, numerów telefonów oraz istotnych danych wrażliwych, jak numery PESEL, numery i serie dowodów osobistych, adresy zamieszkania i numery kont bankowych.

najgłośniejsze

CYBERATAKI

2021 roku

TOTOLOTEK

CD PROJECT

RED

sieć

T-MOBILE

spółka restauracyjna

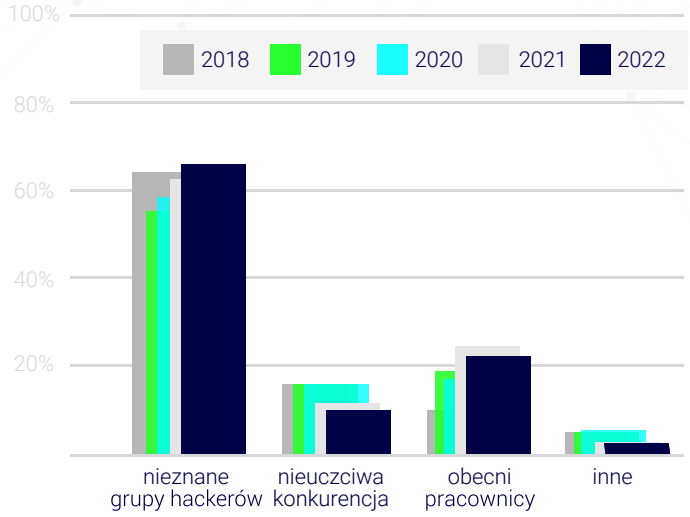
SFINX

KTO

odpowiada za cyberataki?

Niezmiennie, bowiem w poprzednich edycjach Raportu było podobnie, zdecydowana większość respondentów jest zdania, że głównym źródłem cyberzagrożeń są nieznane grupy hakerów (63,89 proc.). Zagrożenia widzimy również w działaniach obecnych pracowników (22,03 proc.) oraz nieuczciwej konkurencji (10,30 proc.).

Wskaż główne, twoim zdaniem, źródła cyberzagrożeń dla twojej firmy.



ponad

75 proc.

ankietowanych uważa, że atak cyberprzestępców na system informatyczny wpływa na funkcjonowanie firmy.

ponad

88 proc.

respondentów uważa, że praca zdalna bezpośrednio wpływa na zwiększenie ryzyka cyberzagrożeń.

prawie

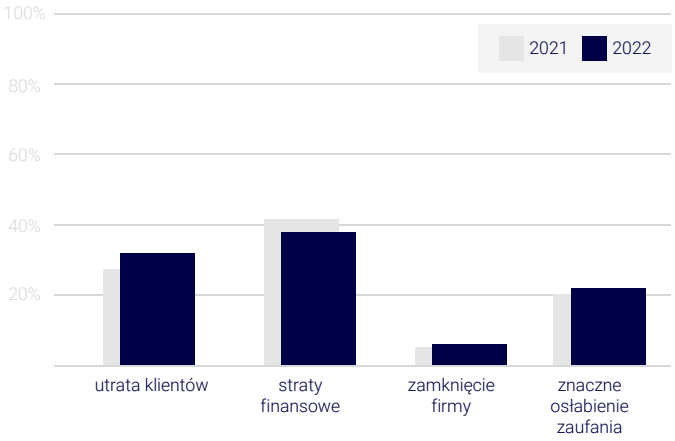
92 proc.

ankietowanych w tym roku korzystało z komunikatorów video

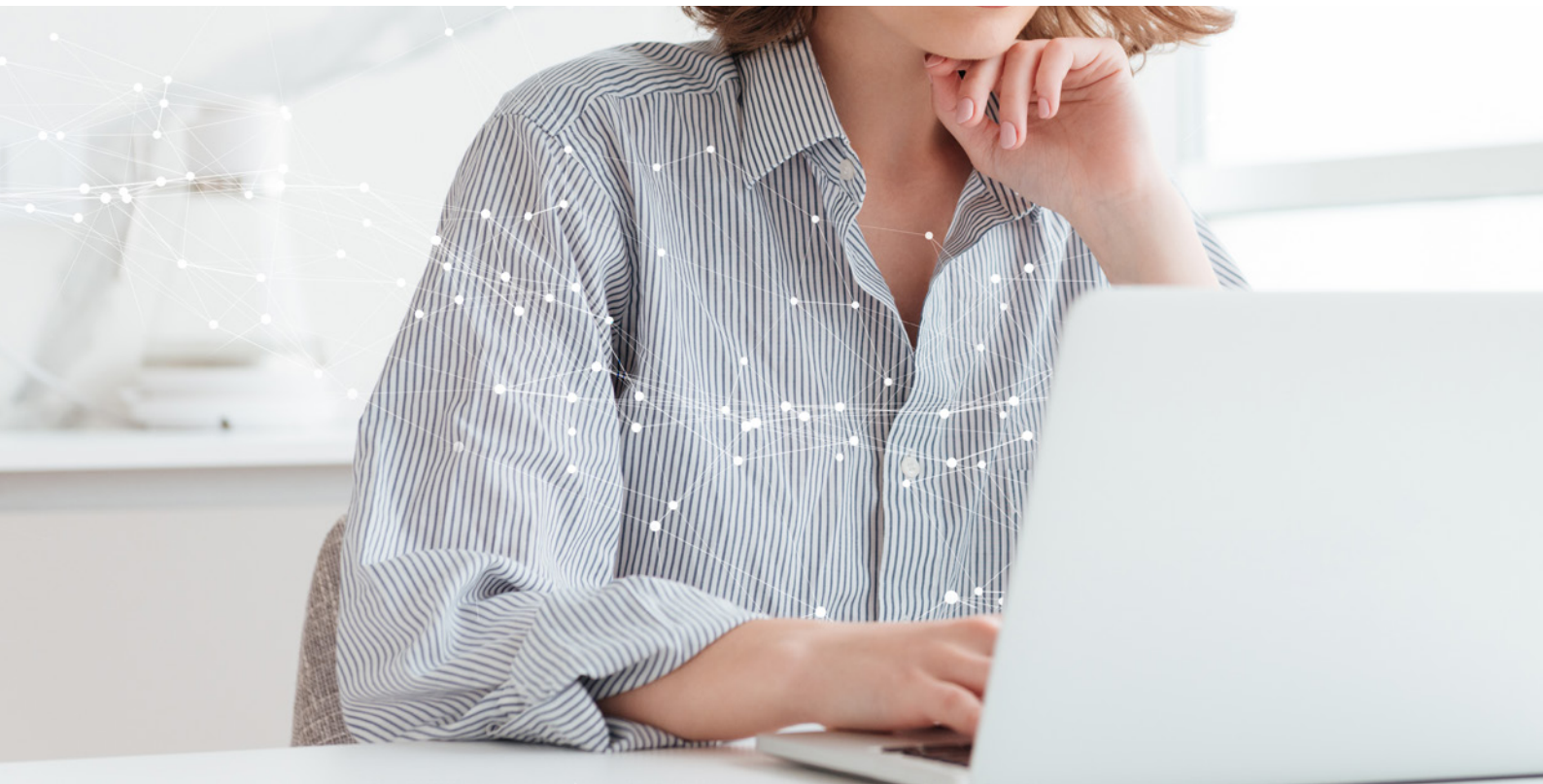
DOTKLIWE

skutki cyberataku

Zapytaliśmy naszych respondentów, w jakich obszarach upatrują najbardziej dotkliwych skutków ataku. Choć, podobnie jak w roku ubiegłym, najwięcej osób wskazało uszczerbek w bazie i relacjach z kontrahentami (29,89 proc.) i niebezpieczeństwie utraty unikalnego know-how i własności intelektualnej (24,78 proc.), to zanotowaliśmy znaczący wzrost udziału odpowiedzi „korespondencja firmowa" – z 3,75 proc. w 2021 roku do 17,44 proc. obecnie. Respondenci mogą zatem być obserwatorami kłopotów z wyciekiem maili urzędników państwowych i doceniają niebezpieczeństwa, w tym wizerunkowe, wynikające z tego typu zdarzeń. Badani obawiają się również utraty dokumentacji przedsiębiorstwa (8,91 proc.) i przejęcia kontroli nad stroną internetową (17,10 proc.).

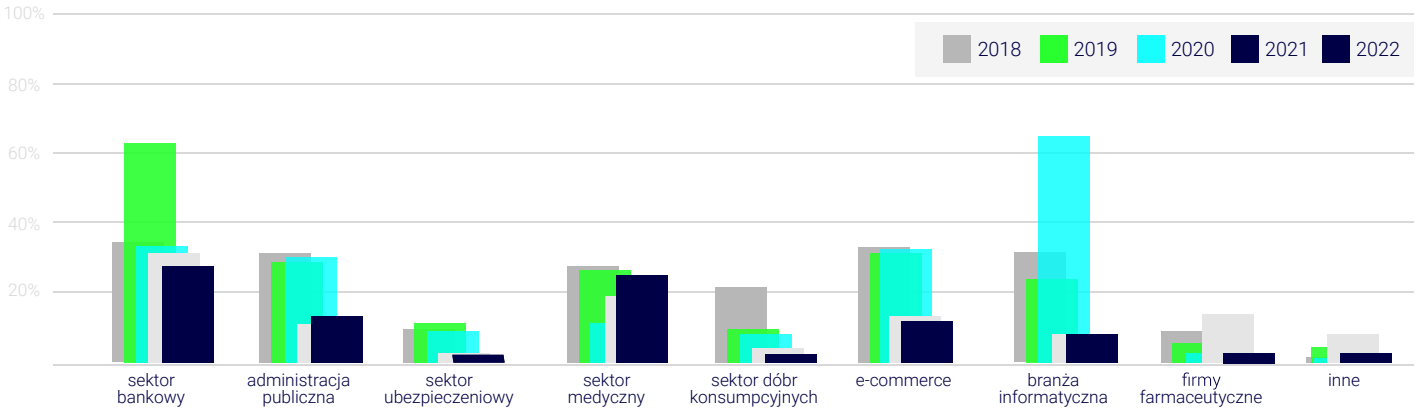


Wskaż obszar, w którym utrata danych byłaby dla twojej firmy szczególnie dotkliwa.



ZAGROŻONE

branże



Wskaż branżę, która twoim zdaniem jest szczególnie narażona na działania cyberprzestępców

W opinii uczestników badania, szczególnie zagrożona zainteresowaniem hakerów jest branża bankowa i finansowa, sektor medyczny, e-commerce oraz administracja publiczna. Choć w tej kategorii na podium nastąpiła roszada, to czołowa czwórka względem poprzedniej edycji badania pozostała bez zmian. Na piątym miejscu wskazano sektor telekomunikacyjny, co może być związane z szumem medialnym dotyczącym ubiegłorocznych ataków na dużych operatorów, w tym przede wszystkim na T-Mobile.

Na uwagę zasługuje również wzrost wskazań dla sektora medycznego. Pandemia znacząco paraliżuje działalność jednostek służby zdrowia. Utrata lub zaszyfrowanie danych dotyczących zdrowia pacjentów i wykonywanych zabiegów może pogrążyć cały system opieki medycznej w kompletnym chaosie. A warto przypomnieć, że w 2021 roku globalnie segment ten zanotował wzrost liczby ataków aż o 55 proc. Co tydzień przestępcy próbują włamać się do podmiotów medycznych średnio 752 razy. Do najbardziej dotkliwych ataków doszło w lipcu 2021 r., kiedy to hakerzy zablokowali dostęp do danych klinicznych jednego ze szpitali w Bukareszcie. Miesiąc później cyberprzestępcy doprowadzili do dezorganizacji procesu szczepień przeciw Covid-19 we włoskim regionie Lacjum. Potwierdzono również, że atak na centrum kliniczne w Düsseldorfie w 2020 r., bezpośrednio przyczynił się do śmierci pacjentki – wskutek blokady systemów i tego, że nie otrzymała na czas pomocy.
Prawdziwy armagedon przeszła jednak w grudniu ubiegłego roku brazylijska służba zdrowia. Hakerzy

z Lapsus$ group przeprowadzili skuteczny atak na tamtejszą bazę szczepień. Cyberprzestępcy przejęli wszystkie wewnętrzne dane państwowe, a następnie je skasowali. Odzyskanie skradzionych informacji prawdopodobnie uzależnione było od opłacenia okupu. Co ciekawe, atak nastąpił tuż przed realizacją planu wprowadzenia obowiązkowej pięciodniowej kwarantanny dla niezaszczepionych podróżnych, ale utrata danych mocno skomplikowała te zamiary. Tymczasem Brazylia należy do grona państw najbardziej dotkniętych koronawirusem. Na covid-19 zmarło w tym kraju niemal 650 tys. osób (dane na 9 stycznia 2022 r.).

W naszym kraju również odnotowano ataki hakerskie na placówki służby zdrowia. Wśród celów cyberprzestępców znalazł się na przykład szpital miejski w Elblągu, American Heart of Poland (sieć szpitali kardiologicznych), Szpital Pirogowa w Łodzi i wiele innych.

Znaczący wzrost potwierdzonych ataków notują również urzędy i instytucje publiczne. W ubiegłym roku potwierdzono zaszyfrowanie danych poprzez ransomware między innymi w Urzędzie Miasta Otwocka. Dane na miejskich serwerach zostały zablokowane, a odzyskanie dostępu do nich uwarunkowane było zapłaceniem okupu. Praca urzędu została sparaliżowana, przestępcy najprawdopodobniej uzyskali dostęp do danych wrażliwych osób, które były przechowywane w systemie IT urzędu, w tym numerów PESEL mieszkańców. Podobne incydenty odnotował również Małopolski Urząd Marszałkowski, gmina w Kościerzynie, gmina Nowiny i wiele innych podmiotów administracji w różnych częściach Polski.

Problemy dotknęły również podwarszawską gminę Konstancin-Jeziorna, choć w jej przypadku najprawdopodobniej doszło do ataku typu business e-mail compromise. Metoda ta jest dobrze znana od wielu lat i polega na podszyciu się pod kontrahenta i podaniu fałszywych danych do przelewu. Niewykluczone, że wcześniej przestępcy infiltrowali system IT w poszukiwaniu informacji o realizowanych przez gminę inwestycjach i osobach, które w samorządzie są odpowiedzialne za ich przebieg. Atak był na tyle skuteczny, że pracownicy gminy nie zauważyli braku 5 mln złotych na kontach, a o potencjalnej kradzieży dowiedzieli się od policji.

PODSUMOWANIE

Postępująca cyfryzacja polskich firm skutecznie realizuje ideę Rewolucji Przemysłowej 4.0. Jesteśmy obserwatorami dynamicznych zmian, które pozwalają pokonać stawiane przez pandemię Covid-19 ograniczenia w prowadzeniu biznesu. To w dużej mierze technologia decyduje dziś o wzroście konkurencyjności polskich firm. To technologia, której wpływu na kolejne gałęzie przemysłu i gospodarki obecnie doświadczamy, pozwala firmom korygować dotychczasowe kierunki rozwoju, dostrzegać i wykorzystywać nowe szanse i możliwości. Rozwój IoT (Internet of Things), upowszechnienie usług w chmurze, efektywne zarządzanie danymi i implementacja narzędzi precyzyjnej wymiany informacji i przepływu kompetencji istotnie zmienia krajobraz polskiej przedsiębiorczości. Dynamiczne zmiany dotyczą jednak nie tylko biznesu. Warto odnotować, że według SpeedTest.pl, w ubiegłym roku znacząco zwiększyły się możliwości przesyłowe polskiego Internetu – w obszarze gospodarstw domowych o niemal 20 proc., Internetu mobilnego aż o 25, 2 proc. (dane za: pierwsze półrocze 2021 vs ostatnie półrocze 2022). Ulepszenie infrastruktury dostawców Internetu z pewnością związane jest ze zwiększonymi potrzebami użytkowników końcowych, którzy coraz częściej realizują swoje służbowe obowiązki w trybie zdalnym. Według szacunków, do 2025 roku globalne skutki cyberincydentów kosztować będą poszkodowane firmy i instytucje ok. 10,5 bln dolarów rocznie. Przekonanie, że udział w tej zawrotnej kwocie

ominie polskie firmy jest irracjonalne. Jak wynika z niniejszego raportu już prawie 70 proc. rodzimych przedsiębiorstw musiało zmierzyć się z różnymi formami ataków. Z pewnością, część firm, które stanęły w obliczu konieczności poniesienia kosztów utraty dostępu do zasobów IT zdecydowała o konieczności zakończenia działalności. Straty wynikające z opóźnienia procesów, czy odbudowy infrastruktury i baz danych często przewyższają wartość oczekiwanego przez cyberprzestępców okupu. Ten z kolei, według Webroot Brightcloud Threat, w 2021 roku wyniósł średnio w skali globalnej 233 817 USD – i był o 30 proc. wyższy, niż w 2020 r. Nie istnieją obecnie rzetelne dane, które wskazywałyby średnią wartość okupu płaconego przez polskie firmy. Warto jednak podkreślić, że inwestycja w zabezpieczenie danych nie tylko jest mniej kosztowna niż wartość oczekiwanego przez hakerów okupu, ale przede wszystkim radykalnie zmniejsza ryzyko wystąpienia cyberincydentu i innych zagrożeń dla prawidłowego funkcjonowania firmowej infrastruktury IT. Na szczęście przedsiębiorstw, które odpowiedzialnie podchodzą do kwestii bezpieczeństwa informatycznego jest coraz więcej, o czym może świadczyć również fakt, że w 2021 roku rynek ochrony przed cyfrowymi zagrożeniami wzrósł o 10 proc. a prognozy na 2022 przewidują dalsze wzmocnienie tego trendu.

W kontekście polskich firm, wyniki niniejszego Raportu wskazują wyraźnie, że postęp technologiczny wyprzedza świadomość zagrożeń. Bez wątpienia należy docenić rodzimy biznes za zmiany, które dokonały się na przestrzeni ostatnich pięciu lat, od kiedy opublikowaliśmy pierwszą edycję naszego Raportu. Pamiętajmy jednak, że wyścig trwa, a cyberprzestępcy w ostatnich latach nie odpoczywali. Przeciwnie, wciąż powiększają i urozmaicają arsenał swoich możliwości, a rosnąca liczba ataków dowodzi, że są w swojej działalności niezwykle skuteczni. To, w jakim stopniu ich aktywność dotknie polskie firmy w głównej mierze zależy od naszej gotowości i podjętych działań prewencyjnych. Parafrazując znane powiedzenie, chcąc prowadzić satysfakcjonującą działalność biznesową, musimy szykować się na cyberwojnę.

METODOLOGIA

Badanie zostało przeprowadzone w formie ankiety internetowej, telefonicznej i papierowej od czerwca do grudnia 2021 roku na próbie 220 przedsiębiorstw i instytucji, działających w ubiegłym roku na polskim rynku.

Największą grupę respondentów stanowili przedstawiciele branży finansów i bankowości (15,45 proc), instytucji rządowych i samorządowych (10,45 proc.) oraz usług dla firm i ludności (9,55 proc.). Wśród uczestników ankiety dominowali przedstawiciele podmiotów zatrudniających do 5 osób – 30,45 proc. Na drugim miejscu znalazły się przedsiębiorstwa i instytucje zatrudniające od 6-10 osób (26,82 proc.). Co czwarty respondent (25 proc.) zatrudniony jest w firmie lub instytucji, której poziom zatrudnienia wynosi od 11-50 osób. Przedstawiciele największych podmiotów (zatrudnienie pow. 50 osób) stanowili 17,73 proc. ogółu badanych.

Reprezentowana branża	
budownictwo / architektura / wykończenie wnętrz	4,09 proc.
edukacja / badania naukowe	3,18 proc.
finanse / bankowość	15,45 proc.
hotelarstwo / turystyka / rekreacja / sport	5,91 proc.
handel hurtowy i detaliczny	5,00 proc.
instytucje rządowe i samorządowe	10,45 proc.
łączność / telekomunikacja	5,45 proc.
media / kultura i sztuka / rozrywka	5,45 proc.
medycyna / ochrona zdrowia	8,18 proc.
produkcja / dystrybucja / logistyka	4,55 proc.
przemysł komputerowy / oprogramowanie	6,82 proc.
przemysł komputerowy / sprzęt	2,73 proc.
usługi dla firm / usługi dla klientów indywidualnych	9,55 proc.
usługi internetowe	5,45 proc.
inna	7,73 proc.

ORGANIZATOR

badania

VECTO sp. z o.o.

Spółka działa od 2008 roku. Firma łączy kilkudziesięcioletnie doświadczenie kadry kierowniczej z potencjałem młodego zespołu, który rozumie realia rynku IT i wyzwania stojące przed firmami i instytucjami wobec dynamicznie zmieniającej się technologii. Spółka dostarcza i wdraża systemy informatyczne oraz świadczy usługi outsourcingu IT dla firm. Oferuje kompleksowe rozwiązania zabezpieczania danych oraz backupu w oparciu o produkty renomowanej firmy DELL Technologies. Wszystkie prace wdrożeniowe wykonuje zespół certyfikowanych, doświadczonych inżynierów.

Kontakt:

Jakub Wychowański

jakub.wychowanski@vecto.pl
Tel. +48 22 548 78 65

al. Lotników 32/46, blok X V
02-668 Warszawa

www.vecto.pl


VECTO.PL