VECTO

IV edycja

RAPORT 2021

Cyberbezpieczeństwo
w polskich firmach


VECTO
DELL TECHNOLOGIES • PLATINUM PARTNER

Spis treści

Wstęp

Gdy w zeszłym roku przygotowywaliśmy trzecią edycję raportu Cyberbezpieczeństwo w polskich firmach nikt nie spodziewał się, że 2020 rok upłynie pod znakiem dramatycznej walki z Covid-19. Dziś wiemy, jak bolesne piętno odcisnęła pandemia koronawirusa w systemie połączonych gospodarek i jak bezlitośnie obnażyła najsłabsze strony globalizacji. Wyłączenia z pracy całych sektorów gospodarki, narodowe kwarantanny paraliżujące przemysł, ograniczenie dostępności transportu i komunikacji, czy przerwane łańcuchy dostaw postawiły ludzkość w obliczu całkiem nowych wyzwań. Cyfryzacja, która w ostatnich latach tak dynamicznie zmieniała krajobraz światowego, ale i polskiego biznesu, została wyniesiona na zupełnie inny poziom. I to właśnie dzięki niej, a także rozwiązaniom IT, dziś udaje się ludzkości minimalizować pandemiczne straty.

Koronawirus stał się katalizatorem głębokich przemian na wielu płaszczyznach. Wymusił zmiany organizacyjne, które w połączeniu z rozwojem takich technologii, jak AI, IoT, Big Data czy rozwiązań chmurowych, zrewolucjonizował model prowadzenia biznesu i spopularyzował koncept pracy zdalnej. Efektem tych zmian jest drastyczne zwiększenie ruchu w sieci, przesyłanych informacji, a także i czasu, jaki użytkownicy spędzają przed ekranami komputerów i urządzeń mobilnych.

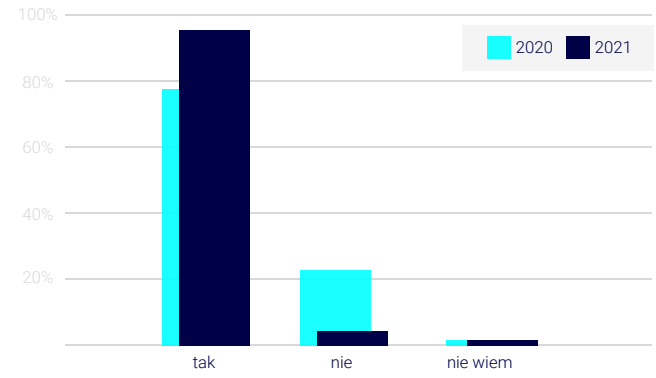
W cieniu szans, wynikających z digitalizacji i wzrostu udziału nowoczesnych technologii w biznesie, kryją się jednak zagrożenia. Cyberprzestępczość wkroczyła w swoją złotą erę, a jej skala rośnie w zastraszającym tempie. Według danych Bitdefender, analitycy odnotowują dziś średnio dwieście infekcji szkodliwym oprogramowaniem na sekundę. Można zatem przyjąć, że w ciągu doby notowanych jest ponad 17,5 mln cyberincydentów. Swoje żniwo zbiera wciąż oprogramowanie ransomware. Polskie firmy również muszą być przygotowane na czarne scenariusze, albowiem Polska już znalazła się w gronie 20 państw najbardziej narażonych na cyberataki.

Jak co roku, celem przeprowadzonego badania było określenie stopnia świadomości polskich firm odnośnie zagrożeń oraz podejmowanych działań w zakresie cyberbezpieczeństwa i ochrony danych. W niniejszym opracowaniu porównaliśmy również efekty naszych analiz z odpowiedziami, które respondenci udzielili w latach ubiegłych. Serdecznie zapraszam do lektury Raportu i naszej diagnozy gotowości polskich firm do stawienia czoła wyzwaniom w obszarze cyberbezpieczeństwa i cyfryzacji biznesu w post-covidowej rzeczywistości.

Jakub Wychowański, VECTO

Komputer
służbowy do celów prywatnych

Nie można analizować przygotowania polskich firm do współczesnych cyberzagrożeń bez nakreślenia obrazu, jak nasza biznesowa codzienność w ciągu ostatnich 12 miesięcy się zmieniła. Aż 95 proc. Polaków deklaruje, że z internetu korzysta codziennie. Z pewnością wynika to z coraz powszechniej stosowanego modelu pracy zdalnej, nauki przez internet, ale również wyraźnie obserwowanej zmiany zachowań konsumenckich. Pandemia zatrzymała nas w domach, jednak konieczność realizacji naszych potrzeb i codziennych przyzwyczajeń zainspirowała do śmielszego korzystania z dobrodziejstw internetu. Czas spędzony online w dobie koronawirusa, według 33 proc. Polaków, wydłużył się nawet o 2-4 godzin dziennie[1]. Zdecydowanie chętniej korzystamy z bankowości elektronicznej, zakupów przez internet, mediów społecznościowych i rozrywki. Według analiz WIB, podczas pierwszego okresu pandemii - pomiędzy marcem i majem 2020 - Polacy w formie elektronicznej korzystali najczęściej z bankowości i możliwości załatwienia spraw urzędowych (79 proc.), zakupów odzieży (32 proc.) oraz e-porad medycznych (26 proc.)[2]. Co ciekawe, w kolejnych miesiącach zainteresowanie zdalnymi formami usług rosło nawet w czasie luzowania obostrzeń, co wskazuje na to, że wielu Polaków przełamało dotychczasową niechęć lub obawy odnośnie bezpieczeństwa realizacji internetowych transakcji finansowych czy zakupu produktów lub usług przez internet.



Czy używasz firmowego komputera do celów prywatnych?

Dane te, choć w niniejszym raporcie zajmujemy się tematem cyberbezpieczeństwa polskich firm, a nie użytkowników prywatnych, przytaczamy nie bez przyczyny. Istnieje bowiem ścisła korelacja pomiędzy naszą aktywnością w sieci, a bezpieczeństwem firm, w których pracujemy. Dotyczy ona faktu, że aż 92 proc. naszych ankietowanych deklaruje, że ze sprzętu firmowego korzysta zarówno w celach służbowych, jak i prywatnych. To znaczny wzrost względem danych z 2019 roku, kiedy to podobną opinię wyraziło 78 proc. respondentów. Naturalnie trudno jest egzekwować od pracowników, że sumiennie będą korzystać z powierzonych im urządzeń wyłącznie do celów służbowych, ale ryzyko pojawienia się incydentów zagrażających bezpieczeństwu danych firmowych rośnie wraz z katalogiem naszej aktywności w sieci. Dostęp do mediów społecznościowych, prywatnej poczty e-mail, komunikatorów, bezrefleksyjne ściąganie plików, filmów czy gier zwiększa szanse na zainfekowanie systemu szkodliwym oprogramowaniem.

Czas spędzony online wydłużył się nawet o

2-4 godz.

dziennie

* Jak Polacy korzystają z telefonu i internetu w czasie pandemii, Krajowy Rejestr Długów, 2020 r.

Kluczowy

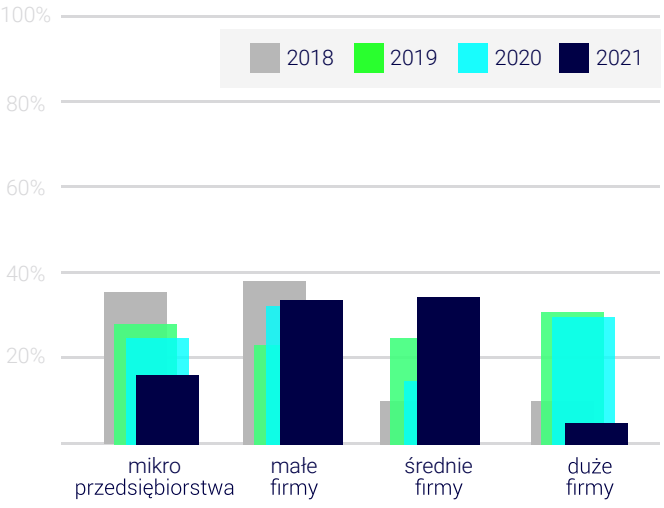
błąd ludzki

Błąd ludzki jest zresztą wciąż najczęstszym powodem infekowania firmowej infrastruktury IT różnymi wersjami oprogramowania typu ransomware.

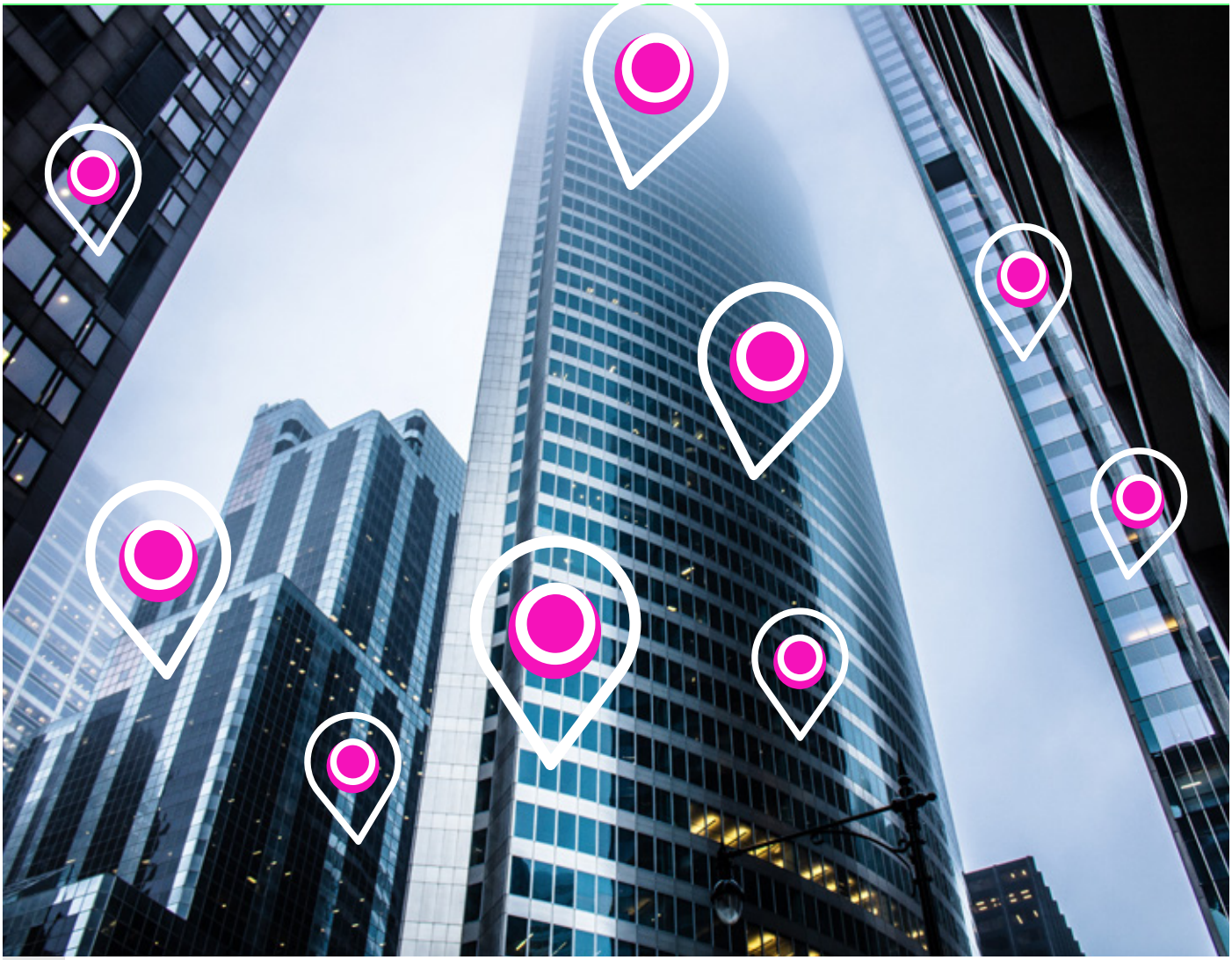
W zeszłym roku nie brakowało na tym froncie spektakularnych zwycięstw cyberprzestępców. Przykłady? Można je mnożyć. W historycznych annałach rok 2020 zapisał się bolesnymi głoskami dla kilku europejskich i amerykańskich uniwersytetów, wśród których największy okup zapłacił University of California SF. Odzyskanie zaszyfrowanych danych dotyczących badań nad Covid-19 kosztowało uczelnię niemal 1,2 mln dolarów. Na celowniku hakerów znalazły się również takie firmy jak Canon, LG, Xerox, Garmin, Ubisoft, czy brazylijski producent samolotów Embraer. Jeśli cyberatak można określić mianem zuchwałego, to z pewnością zasługuje na nie skok na systemy IT firmy FireEye, jednego z największych producentów rozwiązań w zakresie cyberbezpieczeństwa. Przestępcy wykradli szczegóły opracowanej tarczy Red Team, która miała być skutecznym narzędziem do walki z... hakerami. Na wieść o ataku natychmiast zareagowała giełda, a wartość szacowanych na 3,4 mld dolarów akcji spadła aż o 7 proc.

Jednak z analiz ekspertów wynika, że ataki na wielkie brandy to jedynie czubek góry lodowej. Wśród pokrzywdzonych przez cyberprzestępców dominują małe i średnie przedsiębiorstwa, które nie przywiązywały wcześniej większej wagi do kwestii bezpieczeństwa IT. Hakerzy - często do momentu zaszyfrowania danych - nie wiedzą nawet, jakie

firmy obrali za cel. Doświadczenia wielkich marek dzielą więc również i mniejsze firmy, a skala działalności atakowanych podmiotów czy instytucji nie ma większego znaczenia. Na naszym, polskim podwórku przekonał się o tym zarówno Narodowy Bank Polski (atak grupy hakerów z Wietnamu, luty 2020 r.), Orange Polska (lipiec 2020 r.), znana Klinika Budzik, gminy Kościerzyna i Lututów, jak i małe, działające lokalnie przedsiębiorstwa. Ofiary łączy zatem nie potencjał czy obszar działalności, tylko spektrum żądań cyberprzestępców i - ostatecznie - konieczność zapłacenia okupu za przywrócenie dostępu do zasobów IT lub pogodzenie się z ich bezpowrotną stratą. Dostrzegają to również respondenci naszego badania. Poproszeni o wskazanie potencjalnie najbardziej zagrożonych firm (pod względem wielkości), niemal równo rozdzielili ryzyko niebezpieczeństw na małe 35,83 proc. i średnie przedsiębiorstwa 36,67 proc. Mikroprzedsiębiorstwa wskazał niemal co 5 badany, duże firmy zaś co 10.



Jakie firmy są Twoim zdaniem szczególnie narażone na utratę danych?



ATAKI HAKERSKIE W 2020 ROKU W POLSCE

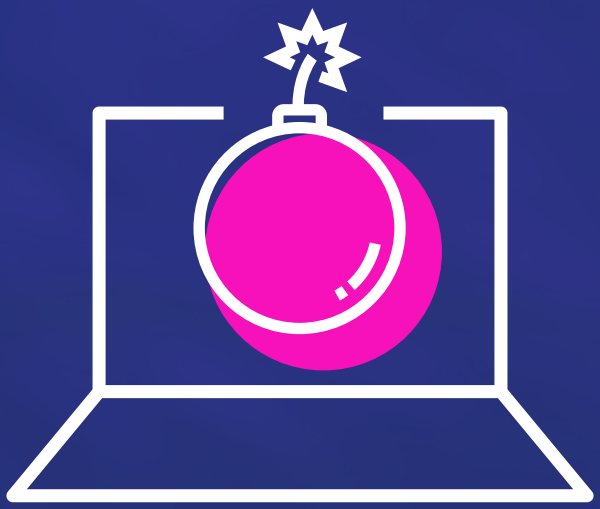
Narodowy Bank Polski

Klinika Budzik

Orange Polska

gmina Kościerzyna

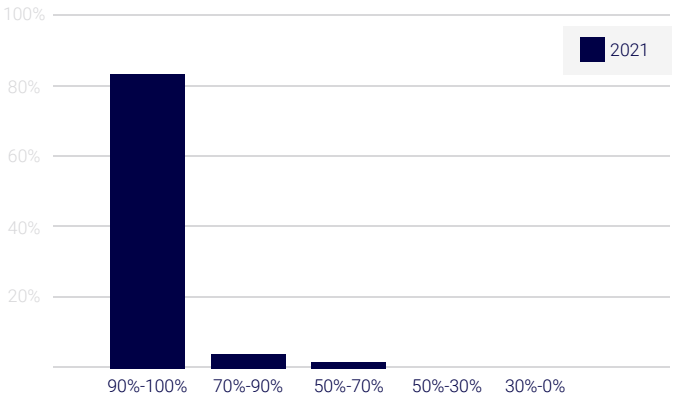
gmina Lututów



Praca zdalna

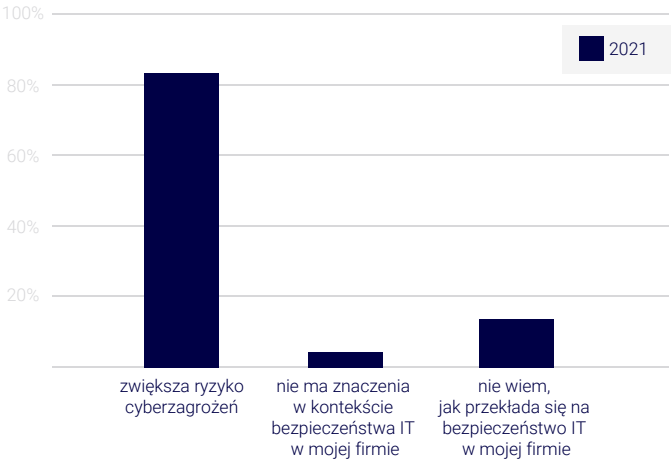
– dodatkowe zabezpieczenia w co 10 firmie

Skalę potencjalnych niebezpieczeństw obrazują kolejne dane. Aż 91,67 proc. naszych ankietowanych stwierdziło, że dostęp do firmowej infrastruktury IT, w tym komputerów, smartfonów, tabletów ma od 90 do 100 proc. wszystkich pracowników. Choć ogromna część zatrudnionych pracuje do dziś zdalnie, to w aż 88 proc. badanych firm nie wprowadzono żadnych dodatkowych zabezpieczeń dla pracowników w trybie home office. Jedynie 12 proc. ankietowanych przedsiębiorstw podjęło takie działania. Dane są zaskakujące, gdy skonfrontujemy je z analizą odpowiedzi na pytanie, czy wspomniana praca zdalna w dobie koronawirusa zwiększa ryzyko wystąpienia cyberzagrożeń. Twierdząco



Jaki procent pracowników Twojej firmy ma dostęp do firmowej infrastruktury IT, w tym komputerów, smartfonów, tabletów, itp.?

Zmiana modelu pracy w dobie koronawirusa i coraz powszechniejsza tzw. zdalna praca, Twoim zdaniem:



odpowiedziało aż 82 proc. badanych firm. Odmiennego zdania było tylko 6 proc., 12 proc. nie wie, jak zmiana modelu pracy wpływa na omawiane aspekty.

Zapytaliśmy również naszych respondentów, czy tegoroczna pandemia bezpośrednio wpływa na konieczność inwestowania w firmowe rozwiązania IT. Na to pytanie twierdząco odpowiedziało aż 85 proc. ankietowanych. Jednak konfrontacja tych danych z faktem, że tylko 12 proc. realnie wdrożyła rozwiązania prewencyjne dla osób pracujących zdalnie wskazuje, że oczywiście dostrzegamy niebezpieczeństwa wynikające z fundamentalnej zmiany modelu pracy w wielu polskich firmach,

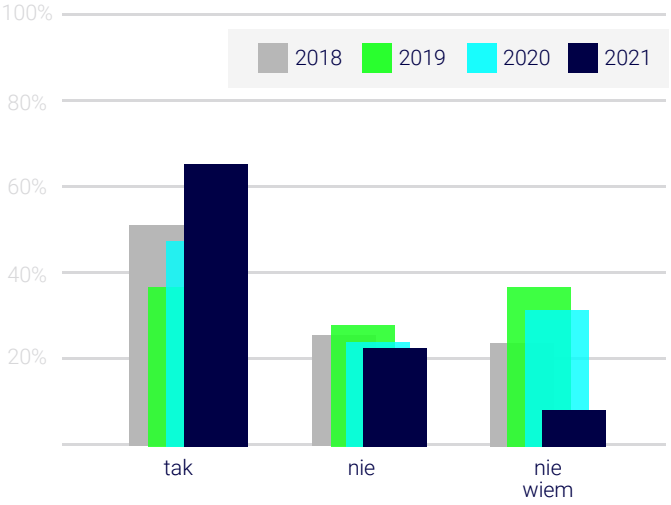
Czy tegoroczna pandemia bezpośrednio wpłynęła na konieczność inwestowania w rozwiązania IT w Twojej firmie?

ale na tej świadomości poprzestajemy. Podobne wnioski płyną z szerszej perspektywy. Wydłużenie czasu spędzanego online, korzystanie z urządzeń służbowych do celów prywatnych, niekiedy przez inne osoby, a nawet dzieci, zwiększenie liczby przesyłanych zdalnie danych, korzystanie z domowych, niezabezpieczonych sieci i wiele innych aspektów pracy zdalnej musi prowadzić do drastycznego zmniejszenia poziomu bezpieczeństwa. Dane płynące z raportu Bitdefender (Mid-Year Threat Landscape) potwierdzają istnienie korelacji pomiędzy pandemiczną transformacją naszych zachowań, a zwiększeniem liczby cyberzagrożeń. Jak wynika z przedstawionych w dokumencie statystyk, w pierwszej połowie 2020 roku (w porównaniu z tym samym okresem z roku poprzedniego) liczba ataków związanych z żądaniami okupu wzrosła aż o 715 procent.

Cyberincydent

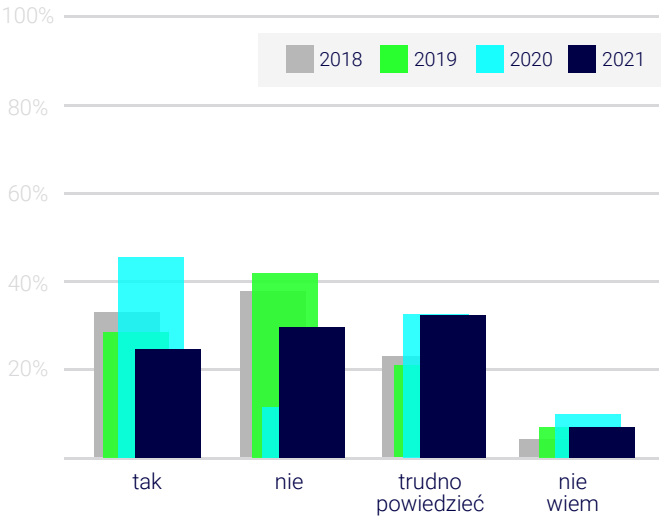
już w 64 proc. polskich firm

Szokująco względem danych z lat ubiegłych wzrósł odsetek firm, które stały się celem cyberataku lub odnotowały incydenty zagrażające bezpieczeństwu systemów IT i integralności danych. W kolejnych edycjach naszego badania obserwowaliśmy w tym wymiarze trend wznoszący, ale różnice rok do roku wynosiły zaledwie kilka procent. Dane za 2020 rok przyniosły jednak znaczący skok, albowiem aż 64,17 proc. firm potwierdziło odnotowanie zdarzenia, które stanowiło zagrożenie lub wprost doprowadziło do utraty lub zaszyfrowania danych firmowych. Oznacza to wzrost o 19 proc. względem



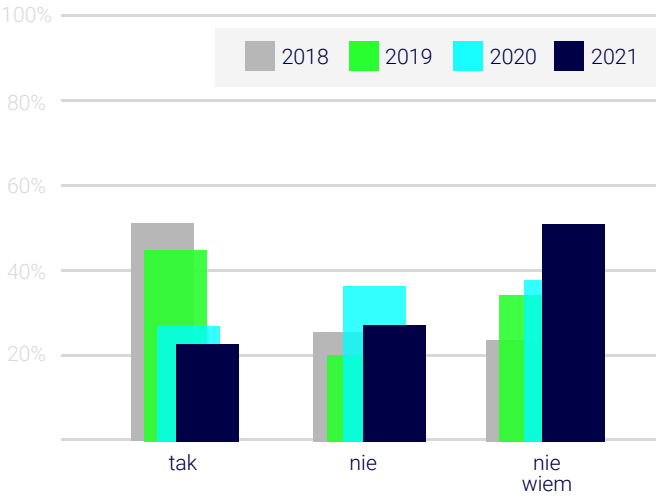
Czy Twoja firma zetknęła się kiedykolwiek z cyberatakiem?

roku 2019. Trend ten, połączony z niewątpliwie rosnącą świadomością cyberzagrożeń wśród Polaków, znajduje odzwierciedlenie w odpowiedziach na pytanie: „Czy uważasz, że sieć w Twojej firmie jest prawidłowo zabezpieczona?". O ile w poprzednich edycjach odpowiedź „tak" uzyskała 44 proc., o tyle w raporcie za 2020 rok odsetek ten wyraźnie spadł do poziomu 23,75 proc. Wzrosła za to liczba odpowiedzi „nie" oraz „trudno powiedzieć", notując kolejno 32,5 proc. i 35,42 proc.



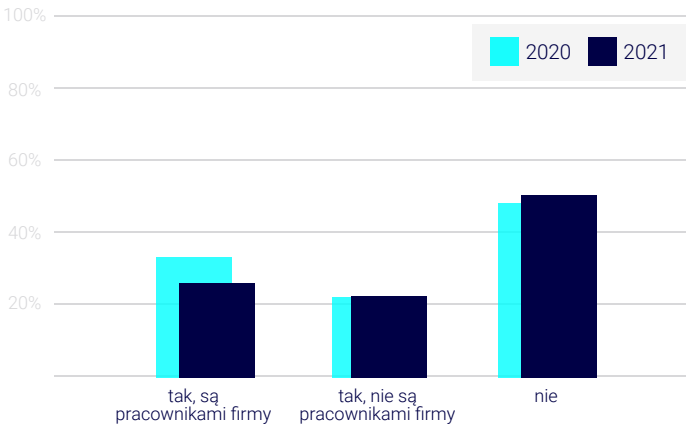
Czy uważasz, że sieć w Twojej firmie jest prawidłowo zabezpieczona?

Dowodem rosnącej świadomości jest również analiza opinii odnośnie do roli zabezpieczeń firmowych danych informatycznych. Aż 74,17 proc. badanych firm uważa, że bezpieczeństwo danych IT jest ważne – w tym aspekcie, w ciągu roku zanotowaliśmy wzrost o niemal 9 proc. Jednocześnie zaledwie 22 proc. firm monitoruje na bieżąco



Czy Twoja firma monitoruje zagrożenia wynikające z cyberprzestępczości?

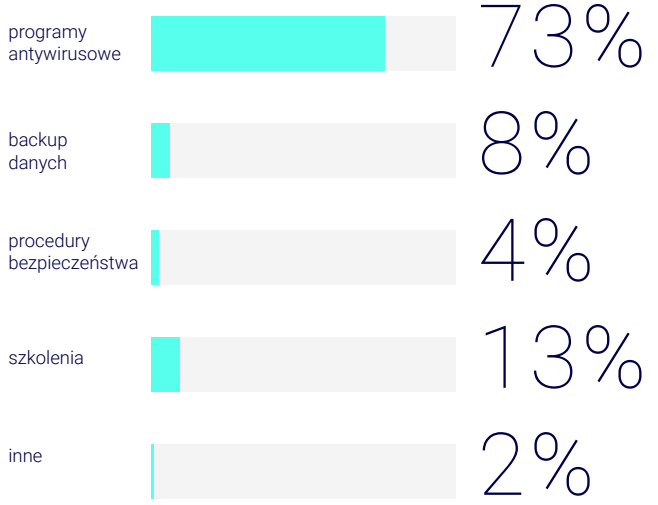
zagrożenia wynikające z cyberprzestępczości. Być może jest to spowodowane również tym, że wzrósł odsetek przedsiębiorstw, które nie korzystają z usług specjalistów w dziedzinie bezpieczeństwa danych – z 46 proc. w 2019 roku do niemal 52 proc. w 2020 roku. Deklarację korzystania ze specjalistów od cyberbezpieczeństwa złożyło łącznie 48,33 proc. badanych firm, z tego 26,25 proc. dysponuje tego typu kompetencjami inhouse, a 22,08 firm zleca obsługę obszaru ochrony systemów i danych IT na zewnątrz.



Czy Twoja firma zatrudnia specjalistę od bezpieczeństwa danych?

Podobnie jak w poprzednich latach w tegorocznej edycji Raportu przyjrzeliśmy się również kwestii najczęściej stosowanych rozwiązań prewencyjnych, których zadaniem jest, w ocenie respondentów, ochrona ich infrastruktury informatycznej. Nasi ankietowani otrzymali zadanie wskazania najskuteczniejszych metod ochrony przed cyberprzestępcami. Prym wśród odpowiedzi wiodło oprogramowanie antywirusowe (72,92 proc), szkolenia (12,50 proc), a także rozwiązania backupowe (8,33 proc). Warto tu jednak podkreślić, że większość polskich firm wciąż nie dostrzega korzyści wynikających z backupu. Szczególnie gdy weźmiemy pod uwagę fakt, że obecnie dostępne rozwiązania backupowe są ważnym i relatywnie niedrogim orężem w walce z oprogramowaniem typu ransomware, które od lat spędza sen z powiek menedżerom IT na całym świecie.

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



o 19%

wzrósł odsetek firm, które stały się celem cyberataku

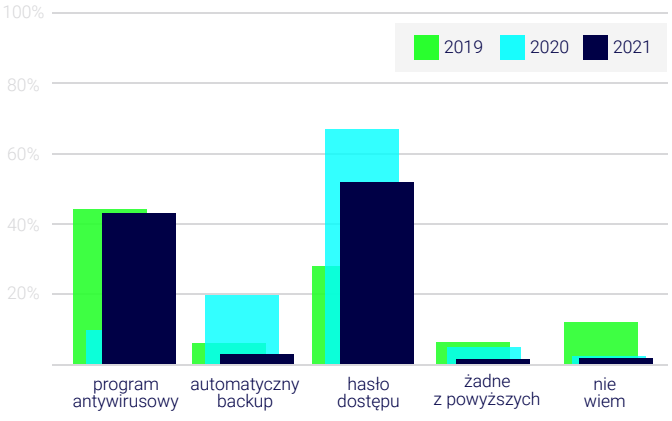
* w porównaniu do roku 2019

VECTO

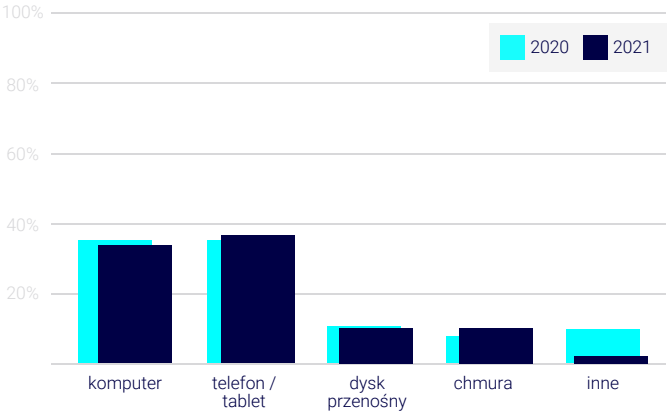
laureatem Diamentów
miesięcznika Forbes 2020

Powyższe odpowiedzi korespondują z danymi, które zebraliśmy w ramach pytań o sposoby zabezpieczenia urządzeń IT, z których korzystają pracownicy w ramach firmowej infrastruktury. Okazuje się, że komputery firmowe najczęściej zabezpieczamy hasłem – czyni tak 47 proc. respondentów. Zdecydowanie wyższy odsetek notujemy dla urządzeń mobilnych – z tej metody zabezpieczenia dostępu do danych korzysta 59 proc. badanych. Według badań WIB ponad połowa Polaków (57 proc.) deklaruje stosowanie długich i skomplikowanych ciągów literowo-liczbowych w procesie tworzenia haseł. I byłaby to informacja bardzo optymistyczna, gdyby nie fakt, że 67 proc. tych samych respondentów przyznaje się do stosowania jednego hasła do logowania do różnych kont. Rozwiązaniem tego problemu może być procedura cyklicznej zmiany kodów dostępu, stosowana w wielu firmach. Kwestia ta jest jednak od lat dyskusyjna. Koncepcja wymuszania częstych zmian haseł lub kodów PIN, czy odpowiedniej ich złożoności ma swoich zwolenników, jak i zagorzałych przeciwników. Ci drudzy podnoszą przede wszystkim argument, że użytkownicy mają problem z ich zapamiętywaniem i najczęściej zapisują nowe hasła na innych nośnikach lub karteczkach, często przechowywanych w pobliżu komputera.

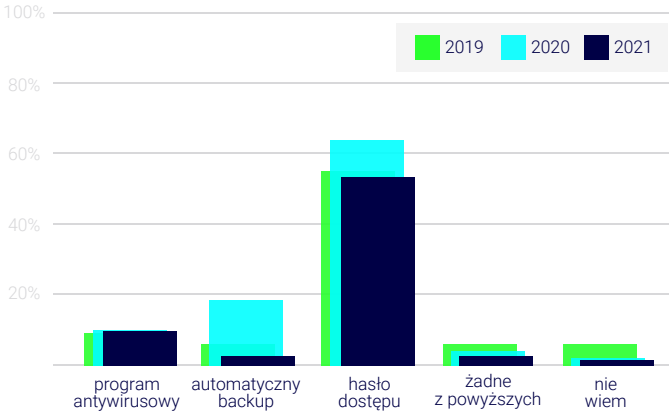
Jednocześnie warto wspomnieć, że swoje najcenniejsze dane przechowujemy właśnie na komputerach (35,42 proc.) oraz telefonie/tablecie (38,42 proc.).



W jaki sposób jest zabezpieczony Twój firmowy komputer?



Gdzie przechowujesz najcenniejsze dla siebie dane?



W jaki sposób jest zabezpieczony Twój firmowy telefon/tablet?

67% respondentów przyznaje się do stosowania **jednego hasła** do logowania do różnych kont.

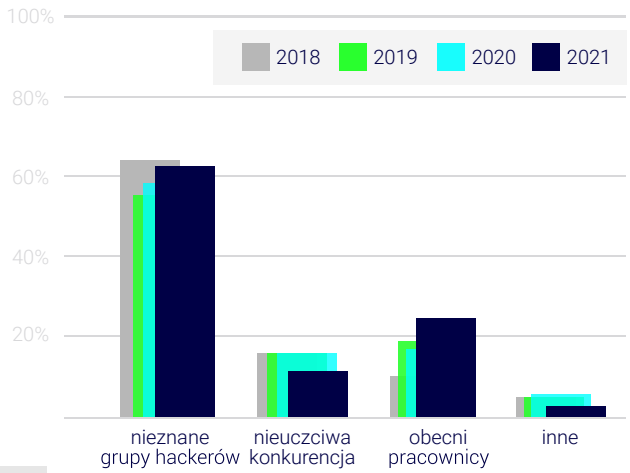
Zagrożenia?

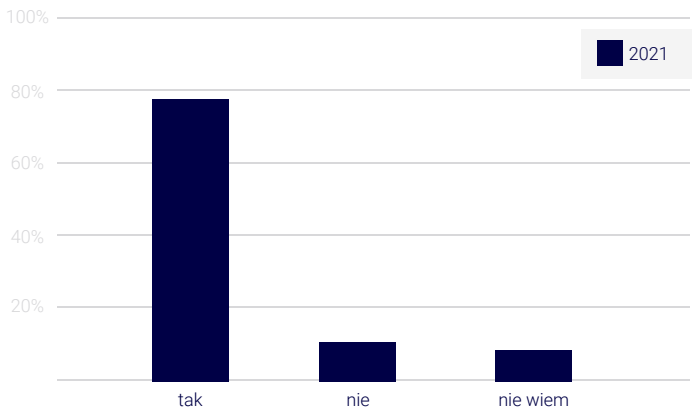
Hakerzy i my sami!

Za cyberincydenty winimy przede wszystkim nieznane grupy hakerów (62 proc.). Podobnie jak w latach poprzednich ta odpowiedź była wskazywana najczęściej w kontekście pytania o źródła zagrożeń bezpieczeństwa IT. Na drugim miejscu uplasowaliśmy samych siebie – obecni pracownicy, w ocenie 24,58 proc. respondentów, odpowiadają za naruszenie integralności systemów informatycznych. 11,25 proc. wskazało nieuczciwą konkurencję.

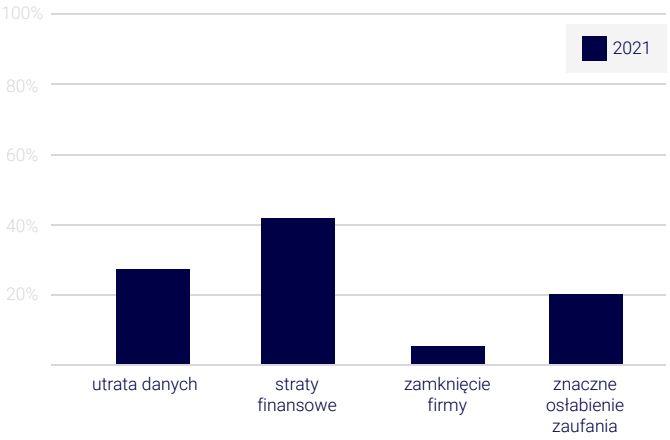
Bezsprzecznie mamy świadomość, że cyberprzestępczość może wpłynąć na funkcjonowanie firmy. Wie o tym aż 79,58 proc. ankietowanych. Wśród najpoważniejszych skutków ataku na systemy IT, 41,67 proc. badanych wymieniło doprowadzenie do strat finansowych. Dla 28,75 proc. respondentów najgorszym efektem takich zdarzeń jest widmo utraty klientów lub znacznego osłabienia wizerunku i zaufania (20 proc). Wśród obszarów, w których utrata danych byłaby dla firmy najbardziej dotkliwa, respondenci najczęściej wskazywali bazę klientów i kontaktów (33,33 proc.), utratę unikalnego know-how i własności intelektualnej (28,33 proc.). Zablokowanie strony internetowej, jako najbardziej dojmującą konsekwencję cyberataku wskazała niemal co czwarta ankietowana osoba, co zresztą wpisuje się w dynamicznie rosnący w 2020 roku udział internetowych kanałów w ogólnej sprzedaży polskich firm.

Wskaż główne, Twoim zdaniem,
źródła cyberzagrożeń dla Twojej firmy:





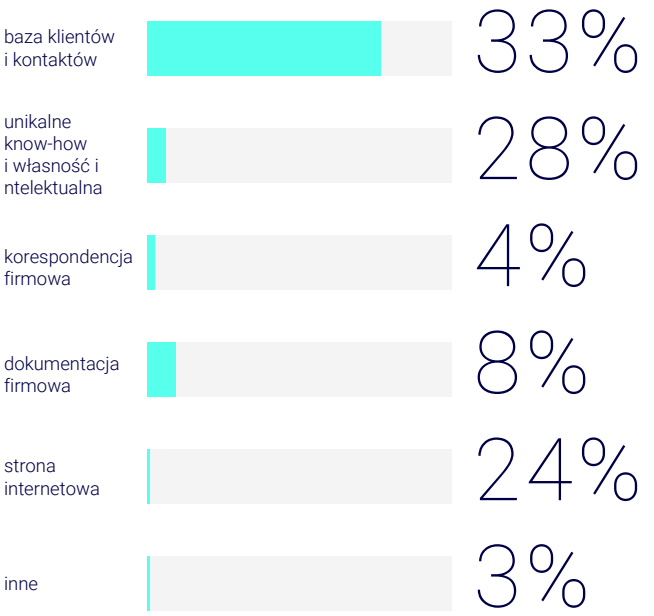
Czy Twoim zdaniem atak cyberprzestępców
na system informatyczny może wpłynąć
na funkcjonowanie firmy?



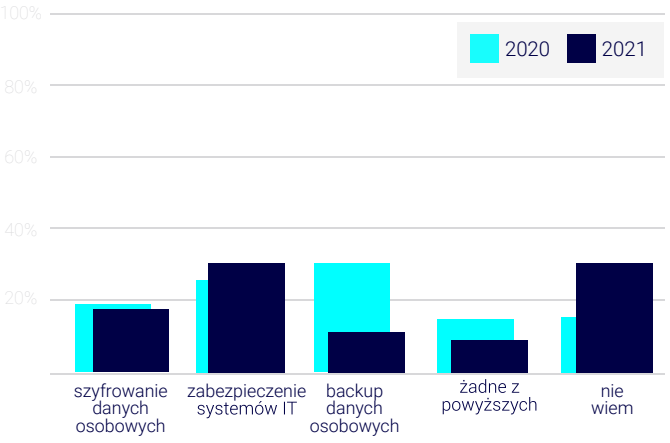
Potencjalnie najpoważniejsze skutki ewentualnego ataku cyberprzestępców.

W kontekście powyższych danych warto zwrócić uwagę, że o ile najczęstszym skutkiem ataków cyberprzestępców są straty finansowe, to jednak nie ograniczają się one wyłącznie do opłaty okupu. Według raportu Marsh, The Changing Face of Cyber Claims, w ponad 70 proc. przypadków, koszty skutecznie przeprowadzonego ataku potęgują wydatki związane z identyfikacją, oceną, a także pomocą prawną i zarządzaniem kryzysowym. Autorzy opracowania wskazują nadto, że przywrócenie infrastruktury do stanu pierwotnego (sprzed cyberataku) może trwać od 3 do 4 tygodni. Firmy, których działalność determinuje system informatyczny, muszą się zatem liczyć z dodatkowymi kosztami operacyjnymi i spadkiem obrotów z tytułu przestoju. Rachunki firmowe dodatkowo uszczuplić mogą kary za wyciek danych, nakładane przez krajowych regulatorów, odpowiedzialnych za nadzór nad ochroną danych osobowych. Również polski Urząd Ochrony Danych Osobowych takich decyzji ma za sobą już kilka. Przekonał się o tym choćby sklep internetowy morele.net (2,8 mln pln), Virgin Mobile Polska (2 mln pln) czy właściciel portalu pożyczkowego moneyman.pl (1 mln pln). Kary nie dotykają wyłącznie dużych graczy, w rejestrze prezesa UODO znajdziemy szkoły podstawowe, Głównego Geodetę Kraju czy osoby prowadzące działalność gospodarczą. Tymczasem respondenci niniejszego badania, poproszeni o wskazanie rozwiązań, które zostały wdrożone w kontekście dyrektywy RODO, nie potrafili udzielić jednoznacznej odpowiedzi – „nie wiem" zaznaczyło aż 30 proc. ankietowanych. Szyfrowanie danych osobowych uzyskało 18,75 proc., zabezpieczenie

Oceń obszary, w których utrata danych byłaby najbardziej dotkliwa:

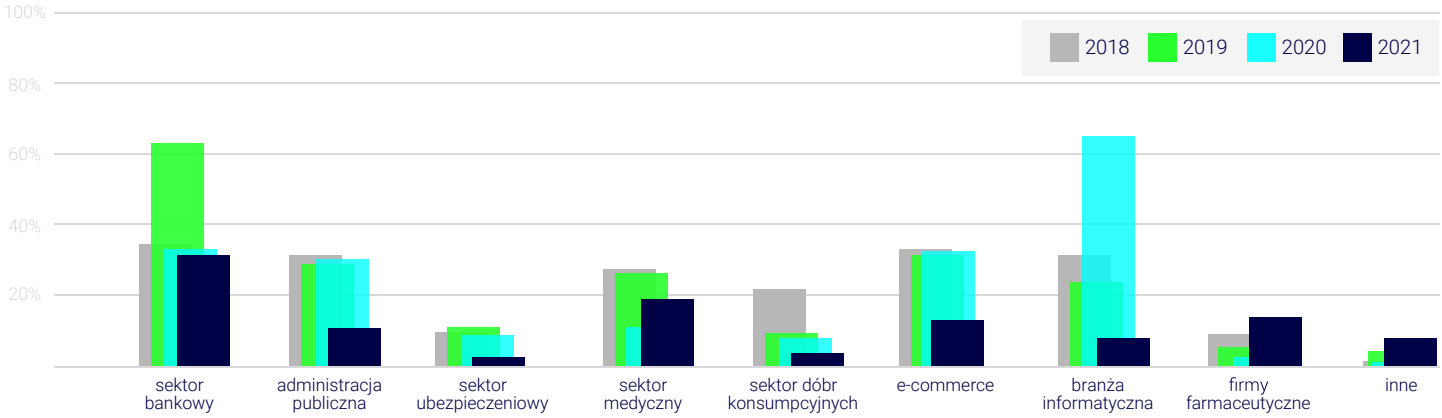


systemów IT na wypadek zewnętrznej ingerencji – 29,58 proc., zaś rozwiązania backupowe tylko 11,25 proc. „Żadne z powyższych rozwiązań" nie zostały wdrożone w co 10 z badanych firm. Wśród branż, które respondenci badania uważają za szczególnie narażone na działania cyberprzestępców, w porównaniu z 2019 rokiem, obserwujemy ciekawe przetasowania. Sektor bankowy niezmiennie wskazało najwięcej ankietowanych – 27,92 proc. Jednak na drugie miejsce w tym zestawieniu awansował sektor medyczny, uzyskując 19,58 proc. Kolejne lokaty zajęły: e-commerce (11,25 proc.),



Czy Twoja firma realizuje wytyczne wskazane dyrektywą RODO? Wskaż które.

firmy farmaceutyczne (10 proc.) i administracja publiczna (7,92 proc.) W zeszłorocznym badaniu, firmy medyczne i farmaceutyczne znalazły się na kolejno na 5 i ostatnim miejscu zestawienia. Co ciekawe, w raportach z lat poprzednich, za branże najbardziej narażone cyberatakiem uznawaliśmy te, w których sami pracujemy. Tymczasem w tym roku, choć reprezentanci branży medycznej stanowi zaledwie 12 proc. ogółu respondentów, to sektor ten zajął wysokie, drugie miejsce. Zdajemy sobie zatem sprawę z niebezpieczeństw, do których mogłyby doprowadzić ataki na dane informatyczne podmiotów służby zdrowia oraz firm farmaceutycznych. To również dowód na to, jak ogromne nadzieje pokładamy w obu branżach w kontekście wyjścia z dzisiejszego kryzysu epidemicznego i konieczności stawiania czoła widmu nadchodzącej, globalnej recesji.



Branże szczególnie narażone na działania cyberprzestępców według ankietowanych

8 razy

częściej winny człowiek

Rosnąca skala cyberincydentów w Polsce i na świecie skłania coraz częściej do refleksji, że konieczne jest zweryfikowanie dotychczasowego podejścia do kwestii bezpieczeństwa IT. Dysponujemy dziś innowacyjnymi rozwiązaniami technologicznymi, które skutecznie potrafią chronić nas przed hakerami i szkodliwym oprogramowaniem. Jednak trudno o optymalną ochronę, jeśli równocześnie nie uwzględniamy błędów czynnika ludzkiego. Z raportu ZFODO wynika, że 8 razy częściej powodem wycieku danych

KARY
ZA WYCIEK DANYCH

2,8 mln pln
morele.net

2 mln pln
Virgin Mobile Polska

1 mln pln
portal pożyczkowy
moneyman.pl

Vecto Cloud Backup

kompleksowe rozwiązania zabezpieczania danych w oparciu o produkty renomowanej firmy DELL Technologies

Co otrzymasz?

Wykonanie do dwóch kopii zapasowych dziennie

Brak przerw w dostępności usług - backup serwera i baz danych wykonuje się w tle

W przypadku utracenia danych, możliwość przywrócenia pliku ze wskazanego backupu, bezpośrednio do komputera w ciągu kilku minut

Codzienny raport backupów

Sprawdź ofertę

www.vecto.pl/vecto-cloud-backup

jest błąd człowieka, niż luki w rozwiązaniach technologicznych[3]. W tym kontekście rośnie znaczenie idei kultury bezpieczeństwa, rozumianej jako tworzenie środowiska, w którym każdy pracownik dysponuje szerszą wiedzą o cyberbezpieczeństwie i potrafi reagować w obliczu zagrożeń. Poprzez umiejętność dzielenia się swoimi doświadczeniami, a także świadomość ryzyka wynikającego z codziennej aktywności w sieci, człowiek staje się ważnym elementem firmowej cybertarczy. Warto zatem, obok dbałości o technologiczne aspekty bezpieczeństwa systemu IT, inwestować w kompetencje pracowników, tworzyć procedury i uczyć odpowiedzialności. Tym bardziej, że narzędzia, z których korzystamy w pracy zdalnej pozostaną z nami na dłużej – jak choćby komunikatory video. Aż 72,08 proc. respondentów naszego badania przyznało, że w 2020 roku po raz pierwszy skorzystali z takiej formuły spotkań biznesowych. Nie każdy jednak wie, że i tu czyhają niebezpieczeństwa. To, co pokazujemy innym w obiektywie kamerki internetowej, czy na zdjęciach publikowanych w mediach społecznościowych, może stanowić dla cyberprzestępców źródło cennych informacji. Pod koniec listopada 2020 roku boleśnie przekonała się o tym minister obrony Holandii, która niefortunnie opublikowała na Twitterze fotografię z częścią kodu PIN i adresem logowania na spotkanie ministrów obrony narodowej państw UE. Brak roztropności pani minister wykorzystał dziennikarz holenderskiej stacji RTL Nieuws, zupełnie niezauważony dołączając do grona uczestników dyskusji o kwestiach obronności UE.

Podsumowanie

Pandemiczny rok 2020 z pewnością przejdzie do historii jako czas zmian społecznych na wielu płaszczyznach, reorganizacji dotychczasowych modeli pracy i funkcjonowania przedsiębiorstw, a także zupełnie nowych trendów technologicznych. Ewolucja, której wszyscy jesteśmy uczestnikami, niesie wiele szans dla ludzkości, ale niewątpliwie tworzy zupełnie nowe przestrzenie dla cyberprzestępców. Drastyczny wzrost naszej aktywności w sieci, wynikający między innymi z powszechnego modelu pracy i nauki zdalnej, przy jednoczesnym braku implementacji rozwiązań zwiększających bezpieczeństwo danych, to wymarzone pole działań dla hakerów. Już 64 proc. polskich firm deklaruje odnotowanie incydentu zagrażającego integralności danych i wszystko wskazuje na to, że w kolejnych miesiącach i latach owe statystyki będą rosły. Świat dostrzega te ryzyka i już dziś definiuje je jako największe wyzwania dla działalności biznesowej na całym świecie. Podmioty gospodarcze, służba zdrowia, urzędy i instytucje publiczne muszą mieć świadomość, że uczestniczą w permanentnej konfrontacji ze światem świetnie zorganizowanej cyberprzestępczości. Tylko konsekwentne inwestowanie w rozwiązania technologiczne i kompetencje pracowników pozwoli na minimalizację ryzyk, a także kosztów finansowych i wizerunkowych skutecznie przeprowadzonych ataków.

O ile koszty wizerunkowe trudno estymować, o tyle według prognoz RiskIQ w 2021 roku cyberprzestęp-

czość wygeneruje straty rzędu 11,4 mln dolarów na minutę[4]. Walnie przyczynią się do tego użytkownicy sieci domowych pracujący zdalnie. W opinii naszych respondentów, najbardziej narażone na ataki będą małe i średnie przedsiębiorstwa, w których wciąż notujemy wiele luk w zabezpieczeniach. Problemem jest również wiedza samych użytkowników, których firmy nie zdążyły odpowiednio przeszkolić w zakresie umiejętności definiowania cyberzagrożeń. Aż 92 proc. respondentów naszego badania przyznało się, że korzystają oni z urządzeń służbowych do celów prywatnych. Na firmowym komputerze i smartfonie otwieramy prywatną pocztę, ściągamy oprogramowanie, udostępniamy niekiedy dzieciom do zabawy. Tymczasem warto przypomnieć, że do ataków ransomware dochodzi przede wszystkim w wyniku błędu ludzkiego. To sam użytkownik, ulegając nieświadomie zabiegom socjotechnicznym czy pułapkom phishingu, infekuje system szkodliwym oprogramowaniem narażając swoją firmę na gigantyczne straty. Ransomware ma szansę zdominować katalog zagrożeń w 2021 roku. Tym bardziej, że w ocenie obserwatorów kolejne miesiące będą czasem zażartej walki gangów specjalizujących się w tej właśnie metodzie ataku, a ich ostra konkurencja o „cyberłupy" wpływa na konsekwentne doskonalenie stosowanych narzędzi szyfrujących i eksfiltracyjnych. Sprzyjać będzie temu również rozwój i popularyzacja technologii 5G, zapewniająca łatwiejszy dostęp do ogromnej mocy obliczeniowej i urządzeń brze-

gowych sieci. To zła wiadomość dla pracujących zdalnie użytkowników komputerów osobistych i podłączonych do firmowej infrastruktury IT urządzeń mobilnych.

W polskich przedsiębiorstwach wciąż pokutuje przeświadczenie, że nie są one interesującym celem ataków. Jednakże w katalogu firm i instytucji, którym przyszło się zmierzyć w ubiegłym roku z konsekwencjami cyberataków, nie znajdujemy wyłącznie podmiotów z pierwszych stron gazet. Znane marki wśród ofiar cyberprzestępców to jedynie czubek góry lodowej. Na jej fundament, niewidoczny pod powierzchnią oceanu szkodliwego oprogramowania, ransomware, szpiegostwa gospodarczego, phishingu i wielu innych narzędzi cyberprzestępców, składa się dramat małych i średnich firm. Setki polskich przedsiębiorstw i tysiące użytkowników codziennie zdaje sobie sprawę, że nie dostrzegli w porę zagrożeń dzisiejszego cyberświata.

Tymczasem rynek jest pełen interesujących rozwiązań, które pozwalają skutecznie przygotować się na ewentualność naruszenia integralności danych. Nie zawsze są to narzędzia kosztowne, choć i te, oferowane dziś w modelu subskrypcyjnym, nie są nieosiągalne dla podmiotów o mniejszych możliwościach finansowych. Doświadczenia na polskim rynku, a także wyraźne trendy globalne powinny być wystarczającą rekomendacją dla każdego odpowiedzialnego przedsiębiorcy i zachętą do weryfikacji dotychczasowej strategii zabezpieczenia danych i infrastruktury IT. Tylko dbając o bezpieczeństwo firmowych danych i zasobów informatycznych, możemy skutecznie zadbać o przyszłość naszego biznesu.

Przypisy

1. Jak Polacy korzystają z telefonu i internetu w czasie pandemii, Krajowy Rejestr Długów, 2020 r.
2. „Postawy Polaków wobec cyberbezpieczeństwa", Warszawski Instytut Bankowości, 2020 r.
3. Incydenty ochrony danych osobowych, ZFODO 2020
4. The Evil Internet Minute, RiskIQ, 2020 r.

XDATA by VECTO

dedykowany zespół specjalistów
od optymalizacji baz danych

ANALIZA

Przeprowadzamy wielopłaszczyznowe audyty całej struktury IT, a ich wyniki są skrupulatnie analizowane przez wyspecjalizowany zespół inżynierów VECTO.

GWARANCJA

Proponujemy naszym Klientom współpracę w modelu pay-as-you-grow, uzależniającą poniesienie kosztów optymalizacji od skuteczności wdrożonych rozwiązań.

OPTYMALIZACJA

Wielowątkowe audyty, zgromadzony know-how oraz dostęp do najnowocześniejszych technologii IT, pozwalają nam tworzyć rozwiązania szyte na miarę.

Sprawdź ofertę

www.vecto.pl/xdata

Meto-dolo-gia

Badanie zostało przeprowadzone w formie ankiety internetowej i papierowej od kwietnia do grudnia 2020 r. na próbie 240 przedsiębiorstw.

Największą grupę respondentów stanowili przedstawiciele branży komputerowej - łącznie 24,6 proc. badanych. 21,25 proc. badanych reprezentuje sektor finansów i bankowości, a 12,08 medycyny i ochrony zdrowia. Wśród respondentów dominowali przedstawiciele przedsiębiorstw zatrudniających 11-50 osób - 29,17 proc. Na drugim miejscu znalazły się przedsiębiorstwa zatrudniające powyżej 50 osób (25 proc.). Pracownicy firm zatrudniających 1-5 osób stanowili 24,58 proc. ogółu badanych, zaś co 5 respondent to pracownik firm zatrudniających 6-10 osób (21,25 proc.).

Reprezentowana branża	
budownictwo / architektura / wykończenie wnętrz	4,17 proc.
edukacja / badania naukowe	2,5 proc.
finanse / bankowość	21,25 proc.
hotelarstwo / turystyka / rekreacja / sport	4,58 proc.
handel hurtowy i detaliczny	3,75 proc.
instytucje rządowe i samorządowe	9,17 proc.
łączność / telekomunikacja	1,67 proc.
media / kultura i sztuka / rozrywka	1,25 proc.
medycyna / ochrona zdrowia	12,08 proc.
produkcja / dystrybucja / logistyka	2,92 proc.
przemysł komputerowy / oprogramowanie	12,08 proc.
przemysł komputerowy / sprzęt	12,5 proc.
usługi dla firm / usługi dla klientów indywidualnych	4,58 proc.
usługi internetowe	5 proc.
inna	2,5 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:

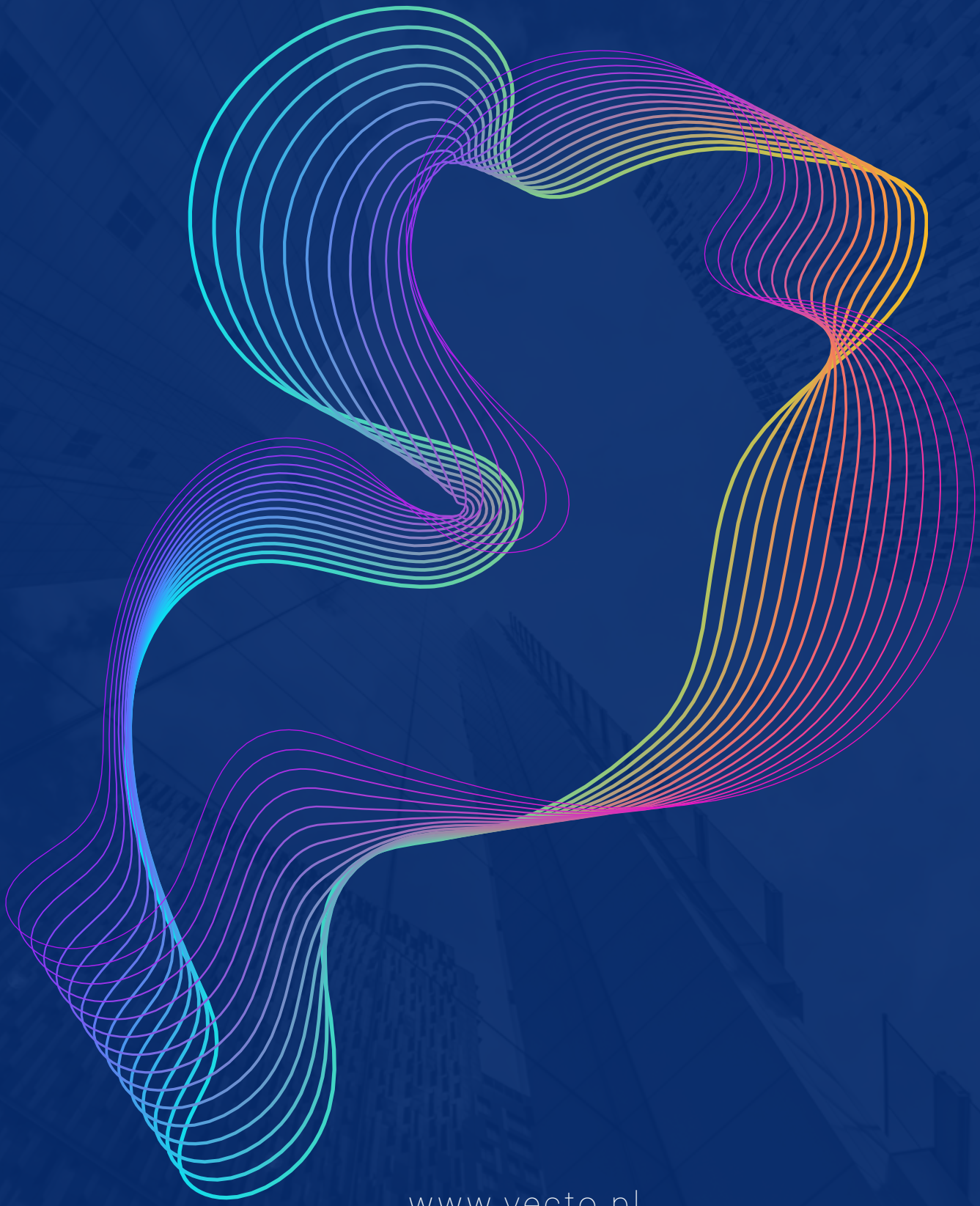
Jakub Wychowański

jakub.wychowanski@vecto.pl

Tel. +48 22 548 78 65

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

www.vecto.pl



www.vecto.pl