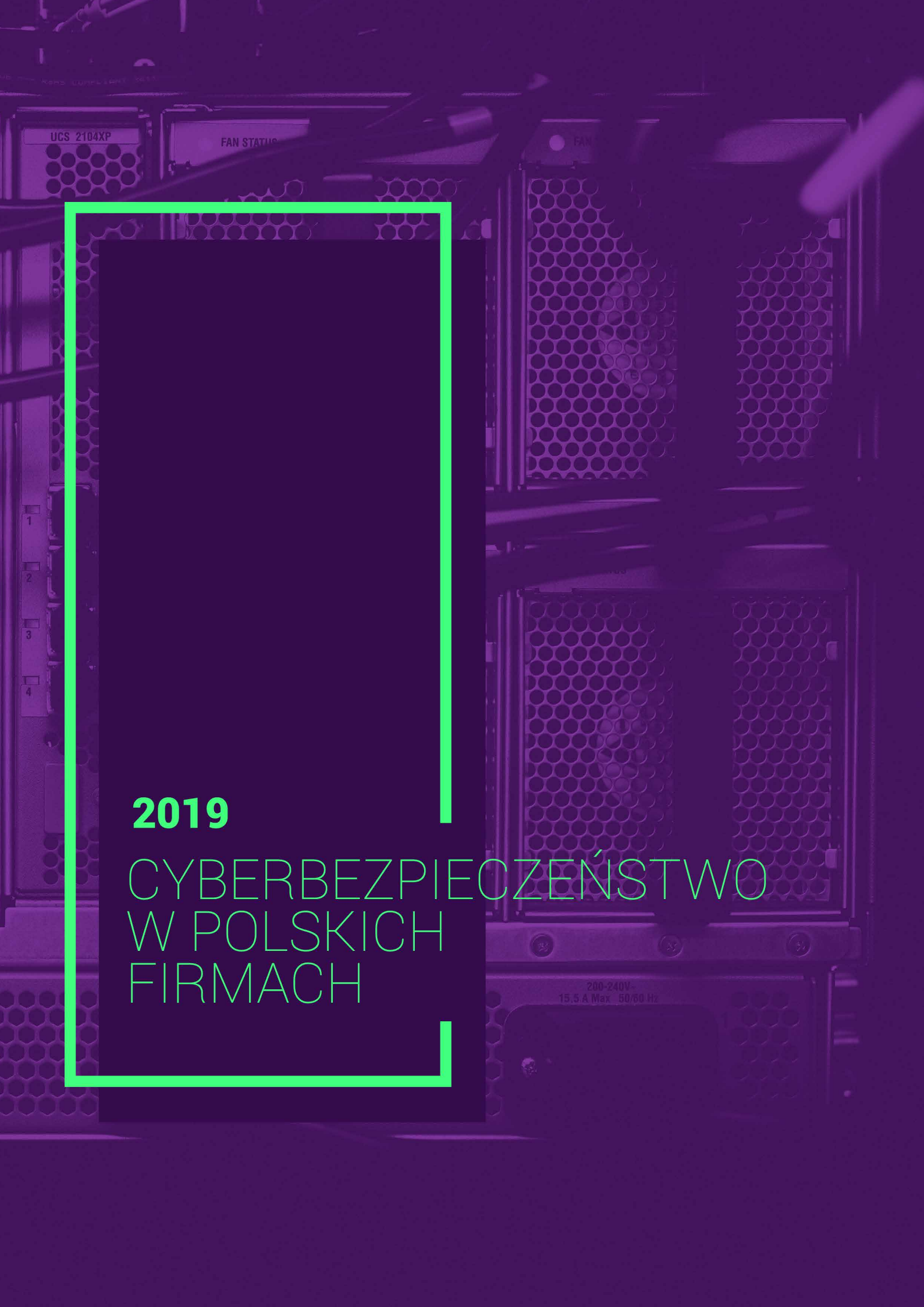


2019

CYBERBEZPIECZEŃSTWO W POLSKICH FIRMACH

WSTĘP

Po 12 miesiącach od publikacji pierwszej edycji raportu „Cyberbezpieczeństwo w polskich firmach", ponownie diagnozujemy świadomość polskich przedsiębiorstw w obszarze cyfrowego bezpieczeństwa.

Po raz pierwszy mamy możliwość porównania zebranych wyników na przestrzeni roku. Możemy zatem pokusić się o pierwsze wnioski, czy polski biznes uczy się na swoich błędach, czy w zabezpieczaniu naszych danych nadążamy za kreatywnością cyberprzestępców. Jak kształtuje się nasza świadomość i jakie działania podejmujemy, by minimalizować ryzyka płynące z obecności polskich przedsiębiorstw w globalnej sieci internetowej?

A ryzyka te nie słabną. Wręcz przeciwnie. W 2018 r. liczba ataków hakerskich drastycznie wzrosła. Już w pierwszej połowie ubiegłego roku mowa była o podwojeniu ich liczby w stosunku do analogicznego okresu w 2017 roku. W drugim kwartale skutki działań przestępczych online dotknęły 765 mln osób[1], co jasno pokazuje jak wielki jest to problem dla całego świata.

Postępująca digitalizacja wszystkich przestrzeni życiowych udostępnia zupełnie nowe perspektywy i pozwala na redefinicję metod osiągania celów i zaspokajania biznesowych ambicji. Czy jednak polskie firmy dostrzegają towarzyszące szansom zagrożenia? Czy potrafimy chronić się przed tymi, dla których Internet jest narzędziem nie tworzenia, a destrukcji?

Na te i inne pytania postaramy się odpowiedzieć w niniejszym raporcie, do którego lektury serdecznie Państwa zapraszam.

Jakub Wychowański
Sales manager
Członek zarządu VECTO Sp. z o.o.

14,3%

ankietowanych przyznało, że ich służbowy telefon lub tablet zostały zabezpieczone programem antywirusowym.

40%

ankietowanych nie potrafi jasno wskazać, co ich przedsiębiorstwa zrobiły w kontekście nowych regulacji prawnych.

95 tys.

skarg na brak stosownych działań ze strony firm.

29%

ankietowanych uważa, że w ich przedsiębiorstwach sieć jest prawidłowo zabezpieczona.

DELL EMC PARTNER PLATINUM

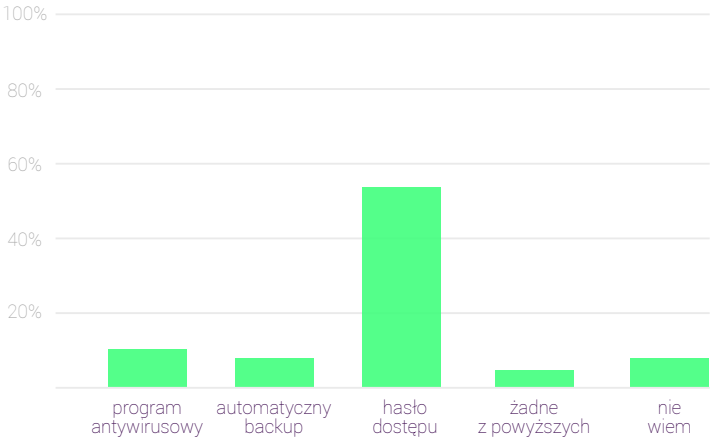
VECTO

RAPORT: BEZPIECZEŃSTWO W SIECI 2019

Zbieranie danych o aktywności cyberprzestępców w 2018 r. w naszym kraju trwa, jednak medialne doniesienia wskazują, że ubiegły rok był pod tym względem rekordowy.

W Polsce, według badania CBOS[2], z Internetu przynajmniej raz w tygodniu korzysta już niemal 70 proc. ankietowanych. Cykliczne badanie PBI/Gemius wskazuje, że w grudniu 2018 r. ich liczba wynosiła już 28 mln, z czego na komputerach osobistych i laptopach (komputery osobiste używane w domu oraz w pracy) – 23 mln, a na urządzeniach mobilnych (smartfony i tablety) 23,5 mln[3]. Niestety, wpływa to negatywnie na nasz poziom cyfrowego bezpieczeństwa. Nieświadomie wystawiamy się na cel ataków, chętnie korzystając z bezpłatnych, ale i niezabezpieczonych, sieci wi-fi na dworcach, lotniskach i w innych miejscach użyteczności publicznej. Zaskakujące jest również to, że o ile nasza świadomość konieczności instalowania oprogramowania antywirusowego na komputerze jest wysoka, o tyle telefon wciąż uważany jest za urządzenie innej kategorii. Okazuje się jednak, że to właśnie urządzenia mobilne, smartfony i tablety są coraz częściej celem ataków cyberprzestępców.

Druga edycja badania firmy VECTO „Cyberprzestępczość w polskich firmach 2019", wyraźnie potwierdza, że nie dostrzegamy zagrożeń dla całej firmowej infrastruktury IT, gdy korzystamy z urządzeń mobilnych. Jedynie 14,3 proc. ankietowanych przyznało, że ich służbowy telefon lub tablet zostały zabezpieczone programem antywirusowym. Z kolei jeszcze mniej, bo tylko 11,3 proc., ma uruchomioną opcję automatycznego tworzenia kopii zapasowych danych z telefonu. Ponad 50 proc. wskazało, że stosuje zabezpieczenie w postaci hasła, ale w kontekście pozostałych wyników może to świadczyć o tym, że zakładając hasło, kierujemy się bardziej ochroną swojej prywatności, a nie bezpieczeństwem firmowych zasobów informatycznych. Pozostali nie byli w stanie wskazać żadnych zabezpieczeń.



W jaki sposób jest zabezpieczony twój firmowy telefon/tablet?

Sytuację nieco próbują ratować producenci urządzeń mobilnych. Trwa wyścig na implementację innowacyjnych metod zabezpieczenia sprzętu mobilnego, jednak obecnie stosowane rozwiązania rozpoznawania linii papilarnych, czy biometryki skanowania owalu twarzy, są wysoce nieskuteczne. Nabywcy droższych telefonów mogą być rozczarowani jak łatwo można obejść tego rodzaju systemy.

Holenderskie Stowarzyszenie Konsumentów, w podsumowaniu swoich badań, stwierdziło, że 42 ze 110 testowanych smartfonów wspierających zabezpieczenie dostępu do telefonu z wykorzystaniem biometrycznego skanu twarzy, mogą zostać odblokowane za pomocą zdjęcia użytkownika[4]. Sami badacze podkreślili, że zaskoczyło ich z jaką łatwością można obejść takie, wydawałoby się, bardzo zaawansowane rozwiązania.

Zbieranie danych o aktywności cyberprzestępców w 2018 r. w naszym kraju trwa, jednak medialne doniesienia wskazują, że ubiegły rok był pod tym względem rekordowy. To efekt postępującej cyfryzacji naszego społeczeństwa

XDATA by VECTO

dedykowany zespół specjalistów
od optymalizacji baz danych

JAK DZIAŁAMY?

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.

MASZ PYTANIA?

Skontaktuj się z nami i zamów bezpłatny audyt Twoich baz danych
lub skorzystaj z konsultacji z jednym z naszych inżynierów.

Agnieszka Zajączkowska tel.: **(22) 548 78 65**
e-mail: **agnieszka.zajaczkowska@vecto.pl**

www.vecto.pl/xdata

oraz powszechnego już dziś wykorzystania Internetu w codziennej komunikacji biznesowej. Niniejszy raport VECTO pokazuje, że większość polskich firm wciąż podchodzi do kwestii cyberzagrożeń z przeświadczeniem, że ryzyka te ich nie dotyczą. Tymczasem hakerzy w swojej działalności nie kierują się granicami państw, sympatią do poszczególnych narodowości, branżą czy wysokością PKB. Atakują te firmy, które mają słabe zabezpieczenia, szukają luk w systemach i bezlitośnie dowodzą prawdziwości powiedzenia „mądry Polak po szkodzie". Pewnym wyjątkiem jest tu jednak administracja rządowa, która dość regularnie zmaga się z efektami działalności przestępczej online. Od 28 sierpnia obowiązuje ustawa o krajowym systemie cyberbezpieczeństwa[5], co dowodzi, że na szczeblu rządowym problematyka cyberzagrożeń jest już objęta słuszną atencją.

Zgodnie ze wspomnianą ustawą, powstać ma Krajowy System Cyberbezpieczeństwa, składający się z m.in. administracji rządowej i samorządowej oraz największych firm ze strategicznych branż. Przy Ministrze Cyfryzacji uruchomiony zostanie Pojedynczy Punkt Kontaktowy (PPK), który umożliwi wymianę informacji o poważnych incydentach, jakie dotknęły co najmniej dwa państwa członkowskie UE. Na tym etapie oczywiście nie można jeszcze ocenić skutków nowej regulacji, niemniej samo jej powstanie pokazuje, że podejście do zagrożeń płynących z Internetu się zmienia. Oczywiście nie przesłania ono zalet świata online i możliwości z nim związanych, niemniej jego ciemną stronę trzeba też brać pod uwagę. Tym bardziej, że wycieki danych dotykają coraz większych grup użytkowników i nie chodzi tylko o ich adresy e-mail czy hasła dostępowe do popularnych serwisów.

Zaledwie pod koniec stycznia w sieci zaczęły krążyć 24 miliony stron dokumentów składanych przez Amerykanów w ramach starania się o kredyty hipoteczne, czy kredyty bankowe. Jak można sobie wyobrazić, zawierały one wszelkie dane osobowe i informacje o sytuacji finansowej, miejscu zatrudnienia, oszczędnościach[6]. Według ekspertów, dane pochodzące z baz firmy analitycznej Ascension prawdopodobnie zostały umieszczone na serwerze firmy Amazon, ale nie zostały zabezpieczone żadnym hasłem. Kwestią czasu było zatem uzyskanie do nich dostępu przez osoby niepowołane, a efekty ich wykorzystania są łatwe do przewidzenia. Tak szeroki zakres informacji o osobie prywatnej może doprowadzić do zjawiska tzw. kradzieży tożsamości, z którym niezwykle ciężko jest walczyć, a szkodliwe skutki takiego procederu poszkodowana osoba może odczuwa latami.

Z tego rodzaju zdarzeniami trudno jest walczyć w pojedynkę, nawet tak potężnym krajom jak USA. Tym bardziej, że hakerzy są bardzo często wykorzystywani do walki ideologicznej, mającej na celu osłabienie przeciwnika. Tajemnicą poliszynela jest fakt, że wiele z ataków na amerykańskie i europejskie strategiczne firmy i instytucje są inspirowane przez Chiny, Rosję czy Koreę Północną. Internet staje się kolejnym polem bitwy, na którym ideologia miesza się z prostą chęcią zarobku za wszelką cenę. Z jednej strony cyberprzestępcy paraliżują funkcjonowanie systemów bankowych, linii lotniczych czy firm energetycznych, z drugiej strony wymuszają okupy, za choćby częściowe, odzyskanie kontroli nad strukturami IT.

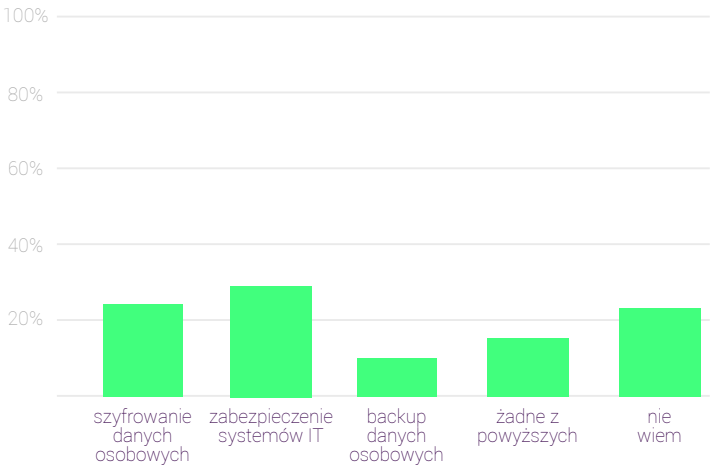
RODO

Zbieranie danych o aktywności cyberprzestępców w 2018 r. w naszym kraju trwa, jednak medialne doniesienia wskazują, że ubiegły rok był pod tym względem rekordowy.

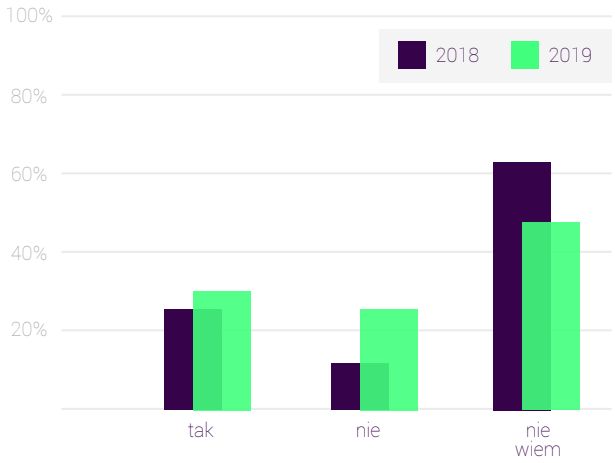
W ubiegłym roku polskie firmy stanęły w obliczu konieczności dostosowania się do RODO, czyli europejskiej dyrektywy o ochronie danych osobowych. W wielu aspektach rozporządzenie to było i jest krytykowane, ale jednak wymusiło na polskich firmach konieczność przeanalizowania obecnie funkcjonujących procedur bezpieczeństwa i zarządzania danymi. Dodatkową motywacją do wdrożenia nowych przepisów jest widmo wysokich kar, nawet do 2 proc. rocznych obrotów, które mogą być nakładane na firmy w przypadku stwierdzenia wycieku, czy naruszenia integralności danych osobowych. Oczywiście przymus implementacji

nowego prawa budzi sprzeciw wielu podmiotów, a wskutek rozbieżności interpretacyjnych dochodzi niekiedy do chaosu. Polskie firmy mają bez wątpienia świadomość ogólnych zasad RODO, ale istnieje problem ze wskazaniem konkretnych rozwiązań, które zostały w kontekście dyrektywy wdrożone. Potwierdza to badanie VECTO. Pracownicy niemal 40 proc. firm nie potrafią jasno wskazać, co ich przedsiębiorstwa zrobiły w kontekście nowych regulacji prawnych. 16 proc. ankietowanych twierdzi bowiem, że nie stosuje się żadnych procedur w zakresie ochrony danych osobowych, a kolejne 22 proc. nie umie ich wskazać. Z drugiej strony 23,7 proc. przyznało, że stosuje szyfrowanie danych osobowych, a 29 proc. zabezpiecza systemy IT na wypadek zewnętrznej ingerencji. Jednak jużż tylko mniej niż co dziesiąta firma stosuje zabezpieczania typu backup, czyli tworzenie kopii zapasowych, pozwalających na szybkie przywrócenie poprawnie działających systemów w razie ingerencji zewnętrznej, czy awarii technicznej.

Co prawda od czasu wejścia w życie RODO nie minęło dużo czasu, ale można było oczekiwać, że firmy skuteczniej zareagują na nowe regulacje, choćby z powodu potencjalnego ryzyka kar.



Czy twoja firma realizuje wytyczne wskazane dyrektywą RODO? Wskaż, które.



Czy twoja firma zatrudnia specjalistę od bezpieczeństwa danych w firmie?

Przed RODO mówiło się bardzo dużo na temat działań online, jak zbierane są dane klientów i w jaki sposób należy je przechowywać, aby nie wpadły w niepowołane ręce. Najwidoczniej wciąż za mało. Tymczasem, jak podaje Komisja Europejska, na brak stosownych działań ze strony firm wpłynęło już 95 tys. skarg[7]. Może dopiero pierwsze spektakularne kary dla polskich firm doprowadzą do oczekiwanych przez nas wszystkich zmian oraz zagwarantują dochowanie przez rodzimy biznes wszelkich starań w obszarze zabezpieczenia naszych danych osobowych. Tym bardziej, że społeczność międzynarodowa, pomimo pewnych biurokratycznych słabości, wiąże z RODO duże oczekiwania. Dała temu jasny wyraz po skandalu dotyczącym wykorzystywania danych przez serwisy społecznościowe, z Facebookiem na czele, który udostępniał prywatne dane użytkowników firmie Cambridge Analityca. Firma ta pracowała dla rożnych podmiotów, także polityków, by w oparciu o dane z Facebooka przygotowywać kampanie reklamowe i świadomościowe skierowane do konkretnych odbiorców i powoli, ale systematycznie, wpływać na ich zachowania i preferencje.

W 2018 r. liczba ataków hakerskich drastycznie wzrosła. W drugim kwartale skutki działań przestępczych online dotknęły 765 mln osób, co jasno pokazuje jak wielki jest to problem dla całego świata.

„ZAGROŻENIA? NAS NIE DOTYCZĄ!"

W zeszłym roku doszło do spektakularnego ataku na największą polską firmę hostingową Home.pl, z usług której korzysta ponad połowa polskich stron internetowych.

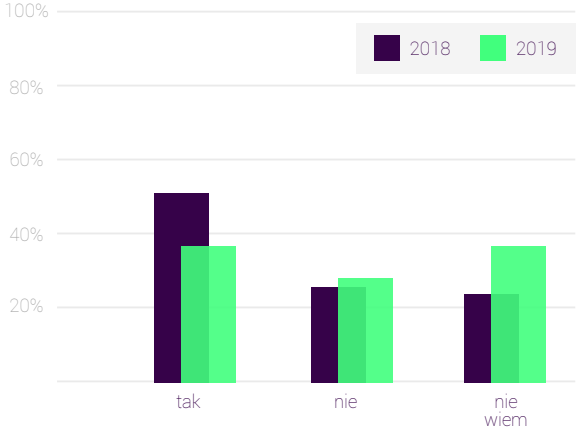
Budżety polskich firm przeznaczane na kwestie bezpieczeństwa stanowią średnio zaledwie 3 proc. całkowitych budżetów IT[8]. Badanie VECTO potwierdza, że zdają sobie sprawę z rosnącej skali aktywności cyberprzestępców i zagrożeń w sieci, ale wciąż uważają, że ich firmy dla hakerów nie są interesujące. Tymczasem, jak wspomniano we wstępie do niniejszego raportu, zakres działań cyfrowych przestępców coraz częściej dotyka rzesze użytkowników sieci internetowej. W zeszłym roku doszło do spektakularnego ataku na największą polską firmę hostingową Home.pl, z usług której korzysta ponad połowa polskich stron internetowych. W jego efekcie, na początku października, nie działało nie tylko wiele stron www czy serwerów pocztowych, ale również systemy kart miejskich w wielu aglomeracjach[9]. Firma podała, że był to największy w ciągu 20 lat atak na jej infrastrukturę. Złożono zawiadomienie o popełnieniu przestępstwa, a sprawcom ataku grozi nawet do 8 lat więzienia. Zważywszy na fakt, że skala tego zjawiska rośnie z roku na rok, ochrona przeciwko zagrożeniom związanym z atakami typu DDoS stała się dla firm niezwykle ważna. Nazwa.pl, kolejny z polskich graczy na rynku hostingowym, w obliczu problemów swojego konkurenta, wdrożył plan znacznych inwestycji zabezpieczających infrastrukturę przed podobnymi zagrożeniami. Czy działanie to okaże się skuteczne, zapewne okaże się w kolejnych latach. Przypadek ataku na Home.pl nie jest oczywiście jednostkowy. Rok 2018 pamiętać będą użytkownicy sklepu Morele.net, jednego z czołowych sprzedawców sprzętu elektronicznego w sieci. Wskutek braku odpowiednich zabezpieczeń, doszło do masowego wycieku danych osobowych 2 mln klientów, w tym takich informacji, jak numery dowodów osobistych. Doniesienia o kolejnych, mniejszych, czy większych atakach i wyciekach danych w polskich firmach, pojawiają się w mediach niemal codziennie.

INTERNET RZECZY

Inteligentne urządzenia domowe, które dzięki połączeniu z internetem mogą być ogromnym ułatwieniem w gospodarowaniu czasem, mogą również stać się obiektem cyberataku.

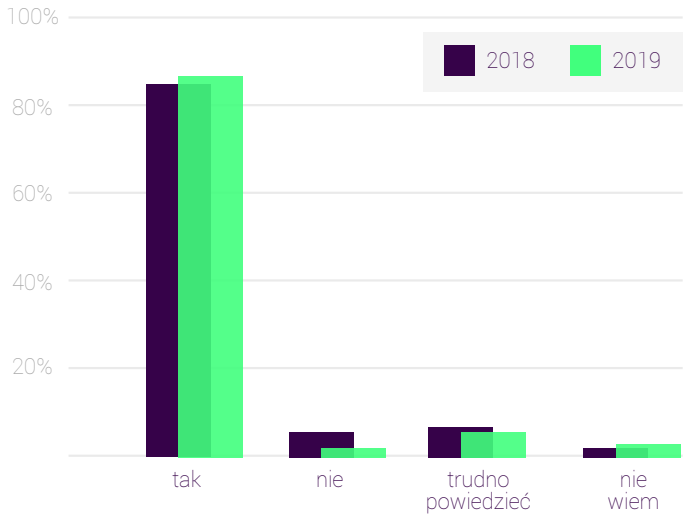
Internet Rzeczy na dobre zadomawia się w naszym codziennym życiu. Inteligentne urządzenia domowe, które dzięki połączeniu z internetem mogą być ogromnym ułatwieniem w gospodarowaniu czasem, mogą również stać się… obiektem cyberataku. Już od lat zdarzają się przypadki wykorzystywania przez hakerów np. lodówek do masowego wysyłania wiadomości w ramach ataków typu DDoS, co w efekcie prowadzi do zablokowania zaatakowanej strony. Mało kto myśli o zabezpieczaniu przed ingerencją z zewnątrz sprzętów typu lodówka czy piekarnik, ale jest już dostatecznie wiele przykładów na potwierdzenie tezy, że innego zdania są cyberprzestępcy. Może się okazać, że słabym ogniwem w naszym korporacyjnym systemie informatycznym może okazać się automat do kawy, podłączony do firmowej sieci. Świetnie zabezpieczone komputery i urządzenia mobilne pokonane przez ekspres do kawy? Całkiem realny scenariusz.

Powyższe przykłady wyraźnie wskazują, że choć postępująca cyfryzacja otwiera przed nami zupełnie nowe, nieosiągalne wcześniej możliwości, to jednak niesie ze sobą mnóstwo zagrożeń. Na co dzień nie zwracamy na nie specjalnej uwagi, ale faktycznie funkcjonujemy w realiach ciągłego zagrożenia. Dla hakerów nie ma też żadnych granic ani świętości, coraz częściej blokują serwery nie tylko z chęci zarobienia, ale aby po prostu pokazać swoją siłę. Zabezpieczanie się przed szkodliwym działaniem cyberprzestępców, za którymi stać będzie również pozafinansowa motywacja, może być paradoksalnie jeszcze trudniejsze do zrealizowania.



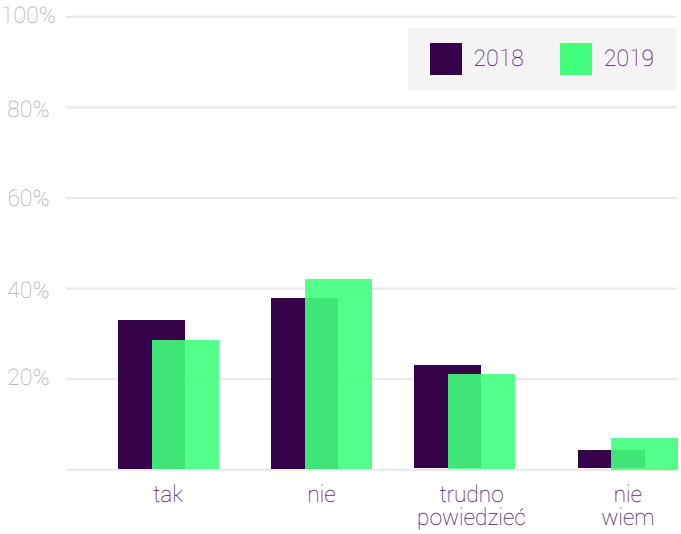
Czy kiedykolwiek twoja firma zetknęła się z cyberatakiem?

Polskie firmy, z nielicznymi wyjątkami, wciąż niechętnie przyznają się do tego, że zostały dotknięte cyberatakiem. Chronią swój wizerunek, informując o przejściowych problemach technicznych w dostępie do serwerów, w tym samym czasie próbując odzyskać kontrolę nad zasobami informatycznymi lub negocjując z hakerami. Uspokajając klientów, często zapominamy o tym, że realizujemy wygodną dla cyberprzestępców strategię niedostrzegania problemu, usypiania naszej czujności. Co za tym idzie, nie podnosimy świadomości tych zagrożeń, a tylko poprzez świadomość, możemy skutecznie przeciwdziałać. W tegorocznej edycji badania VECTO, 38 proc. badanych firm przyznało, że zetknęło się z cyberatakiem. Rok temu odpowiedziało tak ponad 54 proc. ankietowanych, ale chyba nikt nie wierzy w to, że skala problemu zmalała. Przeciwnego zdania było z kolei tylko niemal co czwarte przedsiębiorstwo, czyli tyle samo co rok temu. Tę dysproporcję można łączyć z problemem jednoznacznego zinterpretowania, czym tak naprawdę jest cyberatak. W powszechnej świadomości jest to działanie, wskutek którego tracimy kontrolę nad danymi informatycznymi. Tymczasem incydentem naruszającym bezpieczeństwo może być już samo otrzymanie wiadomości mailowej zawierającej załącznik z oprogramowaniem typu ransomware, spyware, itp.



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

Jesteśmy świadomi cyberryzyk, ale czy z tej świadomości wynika coś więcej? Zdaniem 86 proc. badanych przez VECTO, kwestia zabezpieczania firmowych danych jest istotna, co oznacza niewielki, ale jednak wzrost tego typu wskazań w porównaniu do poprzedniej edycji. Jedynie co trzydziesty badany stwierdził, iż tego zagadnienia nie rozpatruje jako priorytet, rok temu podobnie odpowiedziało 5,6 proc. ankietowanych. Pozostali nie wiedzieli jak daną kwestię ocenić, bądź nie byli w stanie wskazać żadnej odpowiedzi.



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

Zatem w teorii świadomość ryzyka widać, ale czy przekłada się to na realne działania, to już zupełnie inna opowieść. Sami ankietowani są bowiem przekonani, że poziom firmowych zabezpieczeń w ich miejscach pracy nie wygląda zbyt imponująco. Tylko 29 proc. uważa, że w ich przedsiębiorstwach sieć jest prawidłowo zabezpieczona. To nawet mniej, niż w ubiegłorocznej edycji badania, kiedy taką opinię wyraziło 33,6 proc. Wzrósł za to odsetek udzielonych odpowiedzi „nie" – z 38 proc. w 2018 roku do 41,3 proc w najnowszym badaniu. Dużo, bo około co piąty badany, nie jest w stanie wyrazić swojej opinii na ten temat. W opinii VECTO potwierdza to tezę, że świadomość polskich użytkowników internetu wzrasta, ale firmy zbyt opieszale podchodzą do modernizacji i zabezpieczania swoich zasobów informatycznych. Rozkład odpowiedzi na te pytania sugeruje, że być może muszą one zmierzyć się z efektami ataku, by ostatecznie zrozumieć absolutną konieczność przeznaczenia większych nakładów inwestycyjnych w obszarze bezpieczeństwa IT.

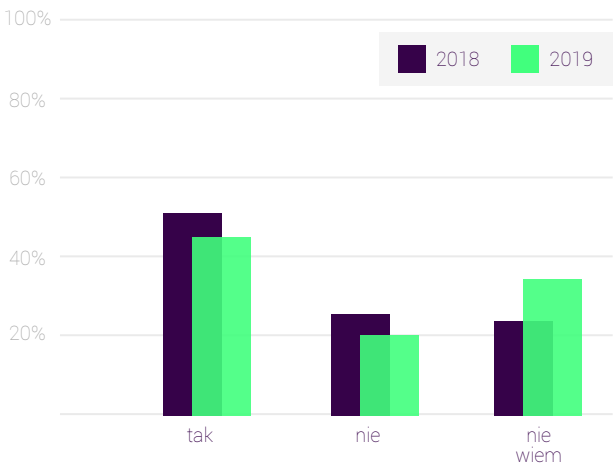
Potwierdzają to odpowiedzi na kolejne pytania zadane respondentom. Rok temu tylko co czwarta firma przyznała, że zatrudnia specjalistę w zakresie bezpieczeństwa danych, obecnie odsetek wzrósł do 31 proc. Część firm korzysta z zewnętrznej obsługi IT obejmującej kwestie bezpieczeństwa informatycznego (24 proc), ale aż 44 proc. twierdzi, że takiego wsparcia w ogóle nie potrzebuje. Może w przypadku mikroprzedsiębiorstw trudno oczekiwać pędu do tego rodzaju wydatków, niemniej większe

firmy powinny być bardziej świadome wynikających z tego korzyści.

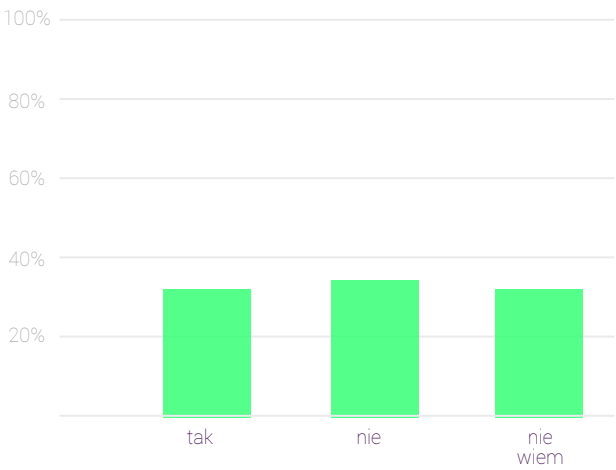
Tymczasem firmy rezygnują ze wsparcia wewnętrznych lub zewnętrznych pracowników odpowiedzialnych za bezpieczeństwo informatyczne nie dlatego, że takiego wsparcia nie potrzebują, tylko zazwyczaj chcą na tym zaoszczędzić. W ocenie VECTO jest to błędna strategia, albowiem konieczność inwestowania w obszar IT wymusza postęp cywilizacyjny oraz wciąż rosnący udział rozwiązań internetowych w dosłownie każdej działalności biznesowej. Coraz więcej firm również generuje swoją wartość w oparciu o zasoby niematerialne, jak programy czy bazy danych, zatem wizja ich utraty powinna być wystarczającym motywatorem do skutecznych metod ich zabezpieczenia.

Ten kierunek potwierdzają trendy globalne. Zaczyna dominować podejście, iż lepiej inwestować w ochronę, niż później zmagać się ze skutkami wycieku danych, czy wadliwie pracującymi systemami wstrzymującymi procesy. Zgodnie z raportem Global Market Insights poziom wydatków na bezpieczeństwo IT wzrośnie ze 120 mld dol. w roku 2017 do 300 mld dol. w 2024 r.[10]

Analizując tegoroczny i poprzedni raport VECTO, nie brakuje kolejnych zaskoczeń, bowiem w wielu aspektach polskie firmy wypadły gorzej, niż rok temu. To bardzo niebezpieczny trend, wskazujący, że nie nadążamy za postępem cyfrowym. O ile rok temu ponad 50 proc. ankietowanych przyznawało się do tego, iż monitoruje zagrożenia związane z cyberprzestępczością, to tegoroczny wynik jest niższy i wynosi 42,7 proc. Tak znaczący spadek w kwestii fundamentalnej dla bezpieczeństwa IT, powinien być asumptem do zastanowienia się polscy menadżerowie nie popełniają, kosztownego zapewne w skutkach, błędu zaniechania stałej analizy zagrożeń płynących z cyberprzestrzeni. Generalnie, choć wciąż zdecydowana większość firm rozumie, że atak cyberprzestępców na system informatyczny może wpłynąć na funkcjonowanie przedsiębiorstwa, to wiedza ta nie przeradza się w realne działania. Przyjrzyjmy się odpowiedziom respondentów na pytanie, czy ich firma ma przygotowany scenariusz postępowania w przypadku wystąpienia incydentu naruszającego bezpieczeństwo danych w firmie. 31 proc. potwierdziło istnienie takich procedur, ale 37 proc. jest przekonanych o ich braku. Kolejne 32 proc. nie umiało na to pytanie odpowiedzieć. W sumie niemal 70 proc. respondentów nie wie, jak zareagować w chwili stwierdzenia cyberzagrożenia. Wynik zdecydowanie niepokojący, zważywszy na fakt, że w przypadku ataku na infrastrukturę IT szybkość reagowania jest kluczowa – szczególnie w kontekście minimalizacji strat finansowych i wizerunkowych.



Czy twoja firma monitoruje zagrożenia wynikające z cyberprzestępczości?

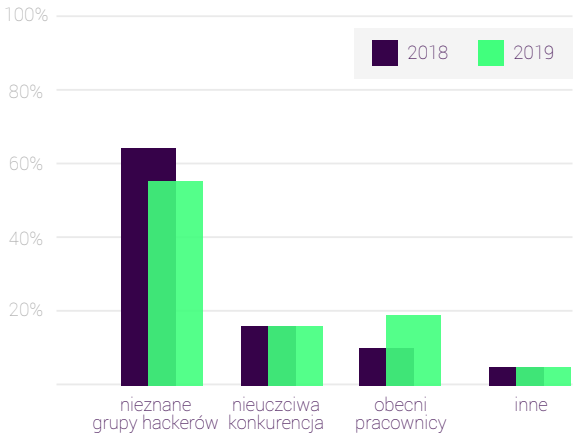


Czy twoja firma ma przygotowany scenariusz postępowania w przypadku wystąpienia incydentu naruszającego bezpieczeństwo danych w firmie?

KTO WEDŁUG NAS STOI ZA ATAKAMI

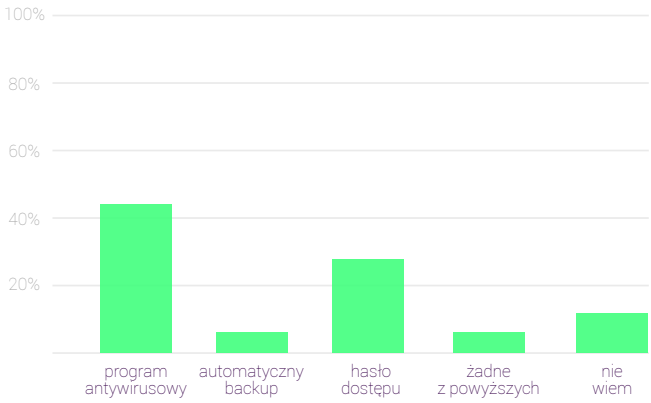
Nieznane grupy hakerów – to właśnie w nich polscy menedżerowie upatrują największe zagrożenie związanego z cyberbezpieczeństwem.

Odpowiedziało tak 55,7 proc. ankietowanych. Niemal co piąty uważa jednak, że niebezpieczeństwem dla integralności systemów IT są sami pracownicy. 17 proc. uważa, że czynnikiem ryzyka może być sabotaż nieuczciwej konkurencji.



Wskaż główne, twoim zdaniem, źródło cyberzagrożeń dla twojej firmy

Prawie co 10 respondent uznał, że zagrożenia płyną z innych, niż wskazane wcześniej, źródeł. Analitycy VECTO potwierdzają, że w zabezpieczenie obszarów IT najchętniej inwestują duże firmy, w skali globalnej odpowiadające za 60 proc. światowego rynku. Choć taki trend dostrzegamy również w Polsce, to jednak podejście mniejszych podmiotów musi się zmienić. Tym bardziej, że rynek oferuje aktualne rozwiązania skrojone na obecne oraz przyszłe potrzeby każdego rodzaju przedsiębiorstwa, w dowolnych branżach. Nie trzeba nawet jednorazowo ponosić wydatków związanych z zakupem systemów IT, można z nich korzystać np. w ramach systemu miesięcznego abonamentu, leasingu, czy innych, wygodnych form finansowania. Zasłanianie się kwestią braku budżetów pozwalających na inwestowanie w bezpieczeństwo IT to zatem słaba wymówka. Szczególnie, gdy mówimy o tak fundamentalnych kwestiach, jak na przykład korzystanie z programu antywirusowego zainstalowanego na komputerze służbowym. Może się wydać nieco zaskakującym fakt, że z tej formy zabezpieczenia korzysta tylko 43 proc. ankietowanych.



W jaki sposób jest zabezpieczony twój firmowy komputer?

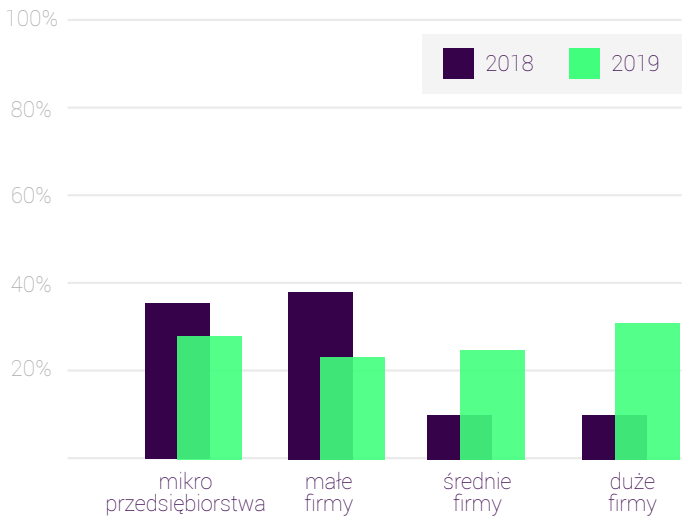
Jeszcze gorzej jest z urządzeniami mobilnymi, na których „antywirusa" ma zainstalowanych zaledwie 14 proc. respondentów. Zupełnie zapominamy o tym, że najczęściej ofiarą ataku pada komputer niezabezpieczony, bez względu na to, czy korzysta z niego prezes wielkiego banku, czy właścicielka kwiaciarni. Programy infekujące nasz sprzęt lub umożliwiające przejęcie nad nim kontroli przez niepowołane osoby, nie wiedzą przecież do kogo dane urządzenie należy. Narzędzia backupu, które umożliwiają błyskawiczne przywrócenie sprawności i integralności systemu po ataku hakerskim, nawet typu ransomware, to jeszcze większa rzadkość w arsenale obronnym polskich firm. Opcja backupu na komputerze to rozwiązanie, z którego korzysta 7,3 proc. firm. Niewiele więcej respondentów deklaruje posiadanie systemu tworzenia kopii zapasowych na urządzeniu mobilnym, bo tylko 11 proc. Natomiast niezwykle zaskakujące jest to, że z bezkosztowego ustalenia hasła dostępu do komputera korzysta zaledwie 28,7 proc. respondentów! Niemal 50 proc. ankietowanych zabezpiecza hasłem swoje urządzenia mobilne. Zważywszy na fakt, że obecnie coraz częściej furtką dla cyberprzestępców są niezabezpieczone urządzenia mobilne z dostępem do sieci firmowej, tak niski odsetek uczestników badania korzystających z tej najprostszej formy zabezpieczenia urządzeń przed nieuprawnionym dostępem, graniczy ze skrajną nieodpowiedzialnością. Ocenę wskazań dla pozostałych dwóch odpowiedzi: „żadne z powyższych" – 7 proc. i „nie wiem" – 13 proc., nie wymaga komentarza.

VECTO zapytała również respondentów o te rozwiązania, które oceniają jako najskuteczniejsze formy radzenia sobie z cyberzagrożeniami. Najwyższe oceny otrzymały: programy antywirusowe oraz backup danych. Mają w sumie wynik ponad 4 pkt. w hierarchii ważności w 5-punktowej skali. Inne rozwiązania spotkały się już z dużo mniejszym uznaniem badanych. Odpowiednie procedury bezpieczeństwa oraz szkolenia dla pracowników oceniono w sumie na nieco ponad 2,6 pkt., co jest wynikiem zaskakująco niskim, ale korespondującym z odpowiedziami na pytanie dotyczące procedur stosowanych w razie pojawienia się incydentu zagrażającego bezpieczeństwu danych firmowych. Zaskakiwać może również niski wynik dla szkoleń, jako dobrych form minimalizacji ryzyk. Z pewnością wiele kłopotów i zagrożeń dałoby się uniknąć, gdyby pracownicy mieli świadomość, że to właśnie ich nieodpowiedzialne zachowania najczęściej prowadzą do naruszenia integralności systemów, czy wycieku danych.

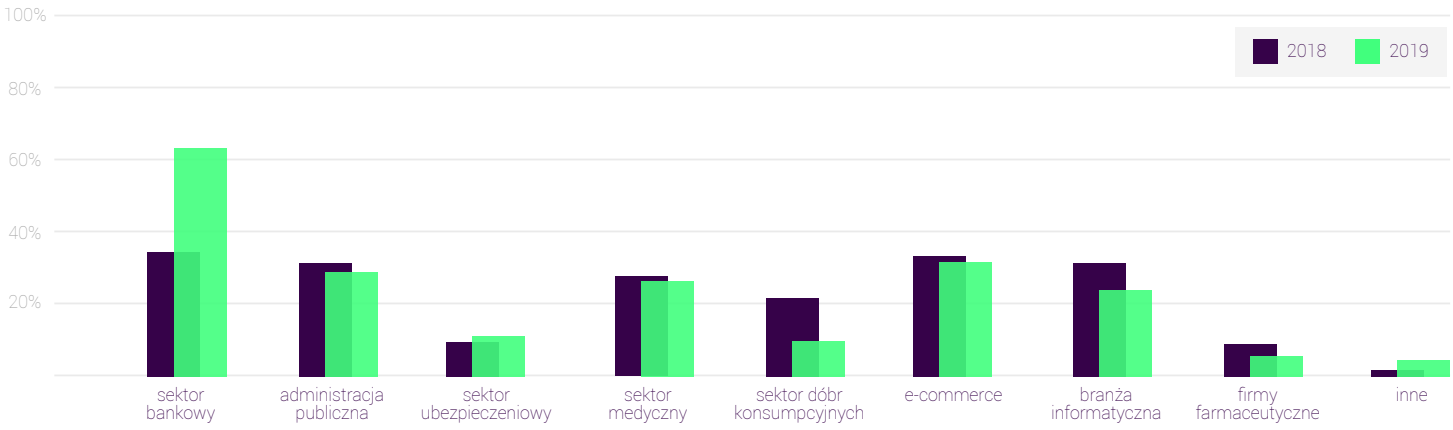
KTO JEST NARAŻONY NAJBARDZIEJ?

Zgodnie z badaniami najbardziej narażony na cyberatak jest sektor bankowy.

30 proc. badanych stwierdziło, że szkodliwa działalność cyberprzestępców dotyczy przede wszystkim dużych firm, choć trzeba oddać, że małe czy średnie przedsiębiorstwa zebrały po ponad 20 proc. wskazań. Ankietowani są w stanie dość dokładnie wskazać sektory, które ich zdaniem są szczególnie narażone na działalność przestępczą w Internecie. Największa grupa respondentów w tym kontekście wskazuje na sektor bankowy – 30,5 proc. Taki wynik jest zgodny z badaniami przeprowadzanymi w innych krajach. Firma FireEye podała w raporcie, że w ciągu kilku ostatnich lat, tylko hakerzy z Korei Północnej narazili ten sektor na straty rzędu 1,1 mld dol.[11] Z kolei jak podało brytyjskie Financial Conduct Authority, nadzorujące londyńskie City, liczba ataków hakerskich na zlokalizowane tam instytucje finansowe wzrosła w ciągu roku (na koniec października 2018 r.) aż o 138 proc.[12] Jednocześnie regulator zaznaczył, iż choć to imponująca skala wzrostu, to jednak nie pokazuje całego obrazu sytuacji. Instytucje skrupulatnie bowiem starają się za wszelką



Jakie firmy są twoim zdaniem szczególnie narażone na utratę danych?

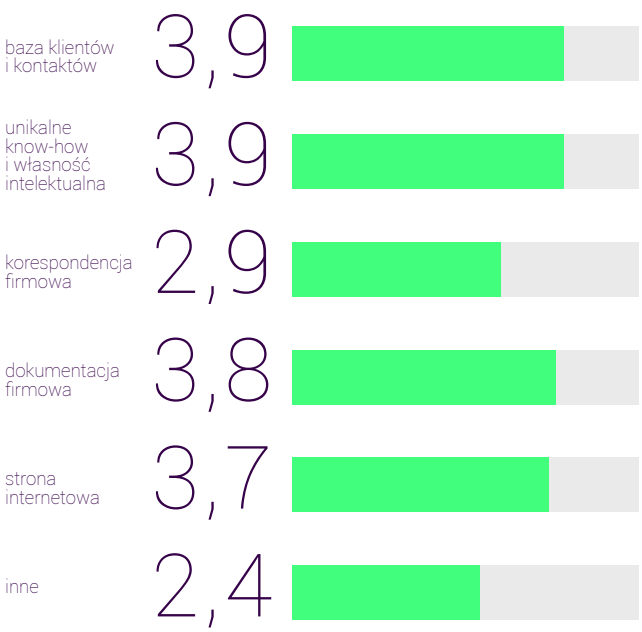


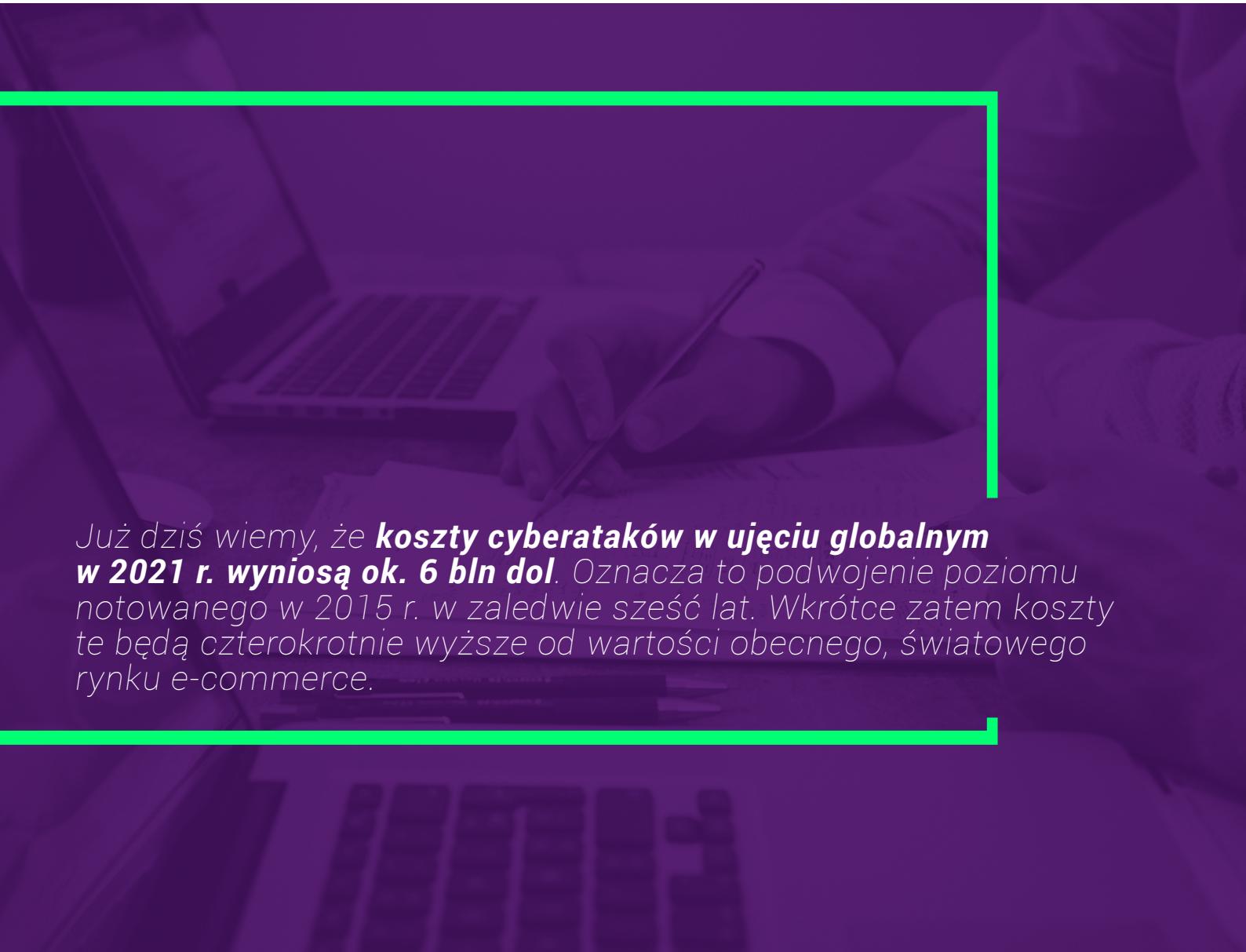
Branże szczególnie narażone na atak hakerów według ankietowanych

cenę unikać rozgłosu, który mógłby powodować odpływ zaniepokojonych klientów, czy nadszarpnąć ich dobre imię. Pozostałe branże, mogące stanowić obiekty zainteresowania cyberprzestępców, odnotowały zdecydowanie niższe wskazania. Sklepy internetowe w tym kontekście wymieniło nieco ponad 15 proc. badanych, a ponad 10 proc. wskazań zebrał z kolei sektor medyczny, firmy informatyczne czy administracja publiczna.

VECTO sprawdziło również, które obszary prowadzenia działalności biznesowej firmy chciałyby szczególnie chronić przed atakami cyberprzestępców. Ankietowani przyznali, że bardzo bolesna dla nich byłaby utrata bazy klientów i kontaktów. Ta odpowiedź uzyskała 4 punkty w 5-punktowej skali. Niewiele mniej, bo 3,9 pkt. przyznano ewentualnej stracie unikalnego know-how i naruszenia własności intelektualnej. Obawiamy się również skutków ataków. Najczęściej wskazaną odpowiedzią była wizja utraty klientów (3,82 pkt./5 pkt.) oraz wizerunku i zaufania całego otoczenia biznesowego (3,38 pkt./5 pkt.). Na niewiele mniej punktów respondenci ocenili możliwość doprowadzenia do strat finansowych (3,24 pkt./5 pkt.) i ostatecznie zamknięcia firmy (2,90 pkt./5 pkt.).

Oceń obszary, w których utrata danych byłaby dla twojej firmy najbardziej dotkliwa (1– mało dotkliwa, 5 – bardzo dotkliwa)





*Już dziś wiemy, że **koszty cyberataków w ujęciu globalnym w 2021 r. wyniosą ok. 6 bln dol**. Oznacza to podwojenie poziomu notowanego w 2015 r. w zaledwie sześć lat. Wkrótce zatem koszty te będą czterokrotnie wyższe od wartości obecnego, światowego rynku e-commerce.*

44%

ankietowanych twierdzi, że nie potrzebuje wsparcia w zakresie bezpieczeństwa IT.

70%

respondentów nie wie, jak zareagować w chwili stwierdzenia cyberzagrożenia.

180 mld $

o tyle do 2024 r. wzrośnie poziom wydatków na bezpieczeństwo IT według Global Market Insights.

14%

ankietowanych chroni swoje urządzenia mobilne programem antywirusowym.

DELL EMC PARTNER PLATINUM

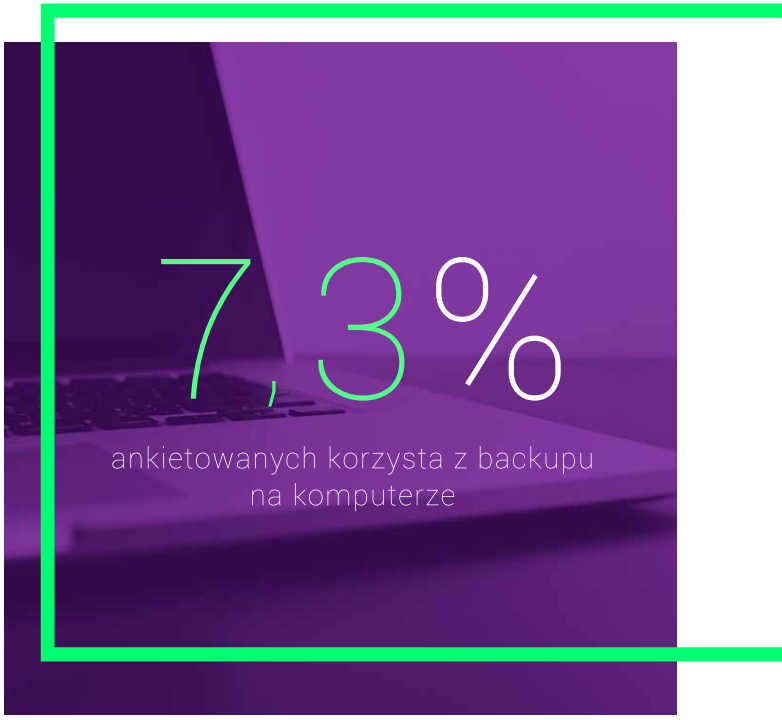
VECTO

PODSUMOWANIE

Cyfryzacja społeczeństwa, jaka stała się udziałem polskich firm i instytucji, tworzy nieograniczone możliwości rozwoju. Otwierają się przed nami wszystkimi perspektywy nowych obszarów aktywności. Skraca się dystans pomiędzy sprzedającym, a kupującym, dostawcą, a odbiorcą towarów i usług. Kwitnie rynek pracownika, który to pracując zdalnie widzi się z przełożonym tylko kilka razy w roku. Dziś możemy zarządzać biznesem z dowolnego miejsca na świecie, definiować cele dla zespołów, projektować procesy, rozliczać projekty. Operujemy coraz większymi plikami danych, streamujemy efekty swojej pracy i wiele obszarów życia codziennego. Nie wolno nam jednak zapominać, że nowe szanse przynoszą również nowe zagrożenia. Przecieramy szlaki do realizacji biznesowych marzeń i ambicji, ale gdzieś w cybernetycznym cieniu kryją się ci, którzy te same cele chcą osiągać drogami na skróty.

Badanie, któremu poddaliśmy polskie firmy w 2018 roku, nie przynosi optymistycznych wniosków. Tym bardziej, że mieliśmy po raz pierwszy okazję do zestawienia odpowiedzi respondentów i dokonania porównania trendów. Zamiast oczekiwanych wzrostów i potwierdzenia, że polskie firmy przekuwają świadomość cyberzagrożeń w realne działania zapobiegawcze, otrzymujemy przygnębiający obraz konsekwentnej wiary w to, że cyberprzestępcy nie mają powodów, by interesować się właśnie nami, naszą firmą, naszym komputerem, czy telefonem. Zapewniam jednak, że nie trzeba być na liście 100 NAJWIĘKSZYCH FIRM W POLSCE „Forbesa", by zetknąć się z konsekwencjami swojej nieostrożności. Najpopularniejsze formy ataków hakerskich nie są motywowane wcześniejszą analizą dynamiki wzrostu przychodów, rankingów popularności firm, czy marek. Hakerzy poszukują urządzeń niezabezpieczonych, łatwych do unieszkodliwienia i zazwyczaj dopiero, gdy atak jest skuteczny, dochodzi do pierwszego kontaktu z ofiarą. Tak funkcjonują ataki typu ransomware, które prowadzą do pełnego zablokowania dostępu do danych. Pozostaje nam zapłacić okup za ich odblokowanie lub pogodzenie się z ich utratą na zawsze.

Z punktu widzenia osoby, która zajmuje się kwestiami bezpieczeństwa informatycznego polskich firm, wyniki raportu wskazują, że przed nami wciąż daleka droga do cyfrowego bezpieczeństwa. Jej meta oczywiście bezustannie oddala się, napędzana kreatywnością cyberprzestępców. W tym wyścigu jednak cały świat nam ucieka, jeśli tylko 43 proc. firm zabezpiecza komputery programem antywirusowym, a jeszcze mniej, bo zaledwie 14 proc., chroni w ten sposób urządzenia mobilne. Zadziwiający jest fakt, że tak usilnie staramy się chronić nasze hasła do portali społecznościowych, PIN-y do kart czy numery PESEL, a jednocześnie logujemy się na konta bankowe za pośrednictwem dworcowego wi-fi. Za tego typu nieostrożność przyjdzie nam słono zapłacić. Już dziś



wiemy, że koszty cyberataków w ujęciu globalnym w 2021 r. wyniosą ok. 6 bln dol. Oznacza to podwojenie poziomu notowanego w 2015 r. W zaledwie sześć lat. To właśnie na nas, branży IT, w instytucjach państwowych, a także mediach i wszystkich świadomych zagrożeń indywidualnych użytkownikach Internetu spoczywa odpowiedzialność za cyfrowe bezpieczeństwo wszystkich polskich zasobów informatycznych. Edukujmy i dzielmy się zatem wiedzą, aby przyszłoroczne badanie pozwoliło na nieco bardziej optymistyczną wizję cyfrowej przyszłości.

METODOLOGIA

Badanie zostało przeprowadzone od kwietnia do końca grudnia 2018 r. na próbie 300 przedsiębiorstw. Największą liczbę badań przeprowadzono w formie kwestionariusza internetowego, stosowane były też ankiety w formie papierowej oraz e-mailowej.

Największa grupę stanowili przedstawiciele sektora bankowego oraz usług finansowych (ponad 6,3 proc. udziału w ogólnej liczbie) i usługowego (ponad 15,3 proc.). Odpowiednio po ponad 12 proc. stanowiły też przedsiębiorstwa zajmujące się medycyną i ochroną zdrowia oraz administracją rządową i samorządową. Dominowali przedstawiciele firm średnich i dużych. Przedsiębiorstwa zatrudniające 6-10 osób stanowiły 22 proc., te z zatrudnieniem 11-50 osób – 24 proc. Co czwarta ankietowana firma była reprezentantem firm małych, z zatrudnieniem do 5 osób, a firmy największe z ponad 50-oobowymi zespołami stanowiły 31,3 proc. badanych przedsiębiorstw.

Wielkość firmy

1-5 osób	23%
6-10 osób	22%
11-50 osób	24%
powyżej 50 osób	31%

Reprezentowana branża

budownictwo / architektura / wykończenie wnętrz	0,7%
edukacja / badania naukowe	1,3%
finanse / bankowość	16%
hotelarstwo / turystyka / rekreacja / sport	2,7%
handel hurtowy i detaliczny	7,7%
instytucje rządowe i samorządowe	12,7%
łączność / telekomunikacja	1,7%
media / kultura i sztuka / rozrywka	9,7%
medycyna / ochrona zdrowia	12,3%
produkcja / dystrybucja / logistyka	4,3%
przemysł komputerowy / oprogramowanie	5,3%
przemysł komputerowy / sprzęt	3%
usługi dla firm / usługi dla klientów indywidualnych	15,3%
usługi internetowe	1,3%
inna	5,7%

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 EMC. 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

PRZYPISY

1. www.eu.usatoday.com/story/money/2018/12/28/data-breaches-2018-billions-hit-growing-number-cyberattacks/2413411002
2. www.cbos.pl/SPISKOM.POL/2018/K_062_18.PDF
3. www. pbi.org.pl/badanie-gemius-pbi/polski-internet-w-grudniu-2018
4. www.biometricupdate.com/201901/more-than-a-third-of-smartphone-facial-biometric-systems-defeated-with-photo
5. www.rp.pl/Bezpieczenstwo/308319957-Ustawa-o-krajowym-systemie-cyberbezpieczenstwa-weszla-w-zycie.html
6. www.techcrunch.com/2019/01/24/mortgage-loan-leak-gets-worse/?utm_medium=TCnewsletter
7. www.europa.eu/rapid/press-release_STATEMENT-19-662_en.htm
8. www.pwc.pl/pl/publikacje/2018/cyber-ruletka-po-polsku-5-edycja-badania-stanu-bezpieczenstwa-informacji-pwc.html
9. www.pomoc.home.pl/komunikaty/chwilowa-niedostepnosc-uslug-wynikajaca-z-ataku-ddos
10. www.prnewswire.com/news-releases/cybersecurity-market-worth-over-300bn-by-2024-global-market-insights-inc--863930577.html?utm_campaign=CybersecurityDiligence&utm_source=hs_email&utm_medium=email&utm_content=69125141&_hsenc=p2ANqtz-_4nxCmnU79Cqu9tGb4eAvpFT3XQPUsSB_IuN1R-E293XFVgpLIveTi9j0MM20INW9aykZoUIfMCsH7hr_MNjKYYhp350kTUMHJ_SsnTiid8dKZDOM&_hsmi=69125141
11. www.bloomberg.com/news/articles/2018-10-08/north-korea-hackers-broke-into-banks-tried-to-take-1-1-billion
12. www.independent.co.uk/news/business/news/banks-tech-failures-tsb-it-outage-cyber-attacks-fca-finance-report-a8654631.html

BACKUP DANYCH

Skorzystaj z naszej oferty backupu danych i zabezpiecz się przed ich utratą. VECTO zapewnia opiekę informatyczną w oparciu o umowy serwisowe, które znacząco redukują koszty utrzymania firmowych działów i usług IT, przy jednoczesnej gwarancji wysokiej jakości tych usług oraz ich systematycznego wykonywania.

Oferta cenowa:

39 zł

ZA STANOWISKO
(laptop, stacja robocza do 50 GB)

79 zł

ZA BACKUP 1 SERWERA
(do 200 GB)

OUTSOURCING IT

Wycena obsługi w 48h

Dzięki strategi #outIT zyskasz:

20 min

maksymalny czas reakcji obsługi zdalnej

24h

wsparcie techniczne

nawet

40%

oszczędności vs. własny dział IT

Odwiedź naszą stronę i dowiedz się więcej **www.vecto.pl**

VECTO

al. Lotników 32/46, blok XV
02-668 Warszawa
www.vecto.pl