

Cyberbezpieczeństwo w polskich firmach

RAPORT 2020



Spis treści

Wstęp	4
Życie w sieci	6
Granica bezpieczeństwa	7
Biznes kar się nie boi?	10
Cyfrowy świat, realne zagrożenia	12
Czy Twoja firma jest w grupie ryzyka?	17
Kto jest narażony najbardziej?	18
Podsumowanie	21
Metodologia	24



Wstęp

Polskie przedsiębiorstwa aktywnie uczestniczą w czwartej rewolucji przemysłowej. Rosnący udział nowych technologii w gospodarce buduje szereg nowych szans i przynosi wymierne korzyści. Według globalnych analiz, firmy, których strategia zakłada wdrażanie elementów transformacji cyfrowej są wyżej wyceniane przez rynek i osiągają średnio o 26 proc. większe zyski od konkurencji.

Jednak powszechne zastosowanie rozwiązań IT w biznesie wywołuje także poważne niebezpieczeństwa. Zjawiska, takie jak informatyzacja przedsiębiorstw, rosnący trend Internetu Rzeczy, wykorzystania sztucznej inteligencji w procesach produkcyjnych i analitycznych, rodzą znaczące zagrożenia dla bezpieczeństwa zasobów informatycznych i integralności firmowych danych. W badaniu Global Risks Report, opracowanym na zlecenie Światowego Forum Ekonomicznego wskazano, że cyberprzestępczość i kradzież danych, obok katastrof środowiskowych i zmian klimatycznych, będą stanowiły największe wyzwania dla światowego biznesu w 2020 i kolejnych latach.

Eksperci i obserwatorzy rynku przekonują, że nadchodzące lata przyniosą wyraźny wzrost aktywności zorganizowanych grup hakerów, które specjalizują się w sprzedaży innym przestępcom sieciowego dostępu do banków. Rośnie zagrożenie bezpieczeństwa transakcji online, wynikające między innymi z pojawiania się szkodliwego oprogramowania atakującego aplikacje mobilne. Możemy się również spodziewać intensyfi-

kacji ataków typu ransomware, poprzez które blokowany jest dostęp do zasobów informatycznych do czasu zapłacenia okupu przez poszkodowane firmy lub użytkowników.

Dla części polskich firm, powyższe scenariusze mogą się wydawać dość abstrakcyjne. Może się jednak zdarzyć, że niedaleka przyszłość przyniesie bolesne doświadczenia. Polska już znalazła się w gronie 20 państw, które są najbardziej narażone na cyberataki. Wynika to przede wszystkim ze specyfiki położenia geopolitycznego i dość niskim inwestycjom w zabezpieczanie infrastruktury informatycznej.

VECTO po raz trzeci postanowiło przeanalizować świadomość polskich firm odnośnie cyberzagrożeń oraz rozwiązań, które stosujemy w zakresie bezpieczeństwa IT. Gorąco Państwa zapraszam do zapoznania się z niniejszym Raportem, w którym podsumowaliśmy efekt ponad 200 firm, wyłącznie polskich, przedsiębiorstw. Wierzę, że zgromadzona wiedza pozwoli na refleksję oraz zweryfikowanie przydatności stosowanych narzędzi i procedur bezpieczeństwa w Państwa biznesie.

Jakub Wychowański,
członek zarządu VECTO



DELL TECHNOLOGIES PLATINUM PARTNER

VECTO ponownie wśród
partnerów Platinum



Życie w sieci

Internet stał się już nieodłączną częścią naszego życia. To w sieci poznajemy nowych ludzi, robimy zakupy, przeglądamy wiadomości czy też przeprowadzamy operacje bankowe. Dostępność technologii mobilnych sprawiła, że wszystkie te czynności możemy wykonywać niezależnie od miejsca i czasu, w którym się znajdujemy. Niestety często zapominając o tym, jakie sieć niesie ze sobą zagrożenia. Dodatkowo na rynek pracy wkracza coraz śmielej pokolenie Z, osób urodzonych po 1995 roku. Grupa ta określa swoją tożsamość, język i zachowania poprzez stosunek do technologii. Niezwykle chętnie instalujemy różnego rodzaju aplikacje w teorii mające ułatwiać nam życie. Jednocześnie, jak donosi raport badaczy z Uniwersytetu Warszawskiego, coraz więcej polskich internautów boryka się z FOMO (lękiem przed odłączeniem od internetu) – 1 na 7 internautów. Według raportu „FOMO 2019. Polacy a lęk przed odłączeniem” na wysokie FOMO cierpi 23 proc. nastolatków (15 - 19 lat), 21 proc. osób w wieku 21-24 lata oraz 26 proc. z grupy wiekowej 25-34 lata. W przypadku osób w wieku 45-54 lat jest to już jedynie 7 proc., 38 proc. osób z wysokim FOMO sięga po social media w trakcie prowadzenia samochodu (8 proc. w grupie przeciętnych internautów). Wysoki phubbing* odczuwa 22 proc. użytkowników internetu, średni – 62proc. , niski – 15 proc. Wysoką nomofobię** przejawia natomiast 15 proc. respondentów.¹

W grudniu 2019 roku, według analiz PBI, z internetu w Polsce korzystało 27,7 mln Polaków, a przeciętny internauta spędzał w sieci blisko 1 godz. 37 min. dziennie.

23,4 mln wykorzystywało do tego celu urządzenia mobilne (23,1 mln internautów posługiwało się smartfonami, a 2,9 mln przeglądało zasoby sieci przy pomocy tabletów).² Niestety jak pokazują badania, mimo iż nasza świadomość dotycząca zagrożeń w sieci wydaje się być coraz większa, nadal czujemy się w niej wyjątkowo bezpiecznie i bagatelizujemy zagrożenia.



38 proc.

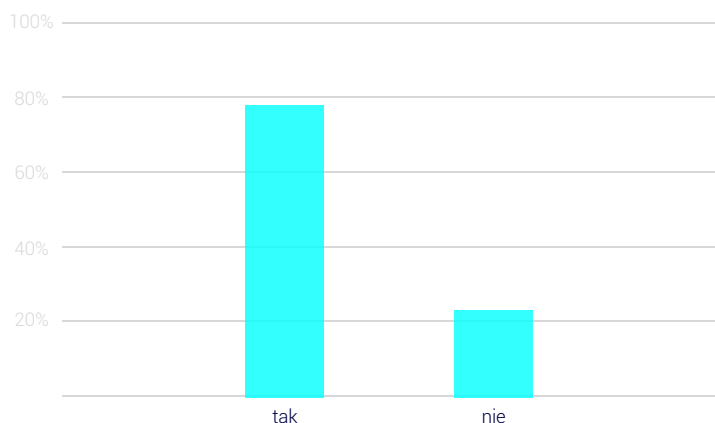
osób z wysokim FOMO sięga po social media w trakcie prowadzenia samochodu

* phubbing - ignorowanie i lekceważenie drugiej osoby poprzez intensywne korzystanie w jej obecności z urządzeń mobilnych (telefonów komórkowych, smartfonów, tabletów itp.) (<http://nowewyrazy.uw.edu.pl/>)

** nomofobia - chorobliwy lęk przed sytuacją, w której nie ma możliwości skorzystania z telefonu komórkowego (<http://nowewyrazy.uw.edu.pl/>)

Granica bezpieczeństwa

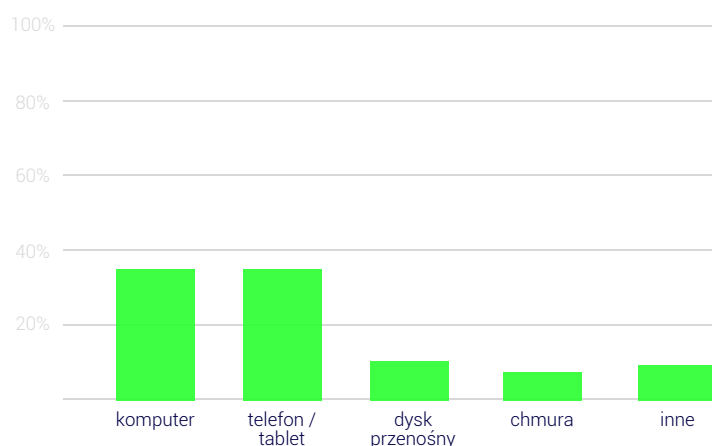
Trzecia już edycja badania firmy VECTO „Cyberbezpieczeństwo w polskich firmach 2020” jasno pokazuje, że nadal nie tylko nie dostrzegamy zagrożeń dla firmowej infrastruktury IT, ale też coraz częściej używamy służbowych telefonów i komputerów do celów prywatnych, do czego przyznało się aż 78 proc. ankietowanych.



Czy używasz firmowego komputera / telefonu do celów prywatnych?

Są to dość niepokojące dane. Pracodawcy coraz częściej przekazują pracownikom służbowy sprzęt. W przypadku wielu branż służbowy laptop, tablet i telefon są już swego rodzaju normą. Kodeks pracy nie normuje natomiast w żaden sposób korzystania ze służbowego sprzętu. Pozostają więc ustalenia między pracownikiem, a pracodawcą, czy też odpowiednie regulaminy i zapisy w umowach. W praktyce wygląda to jednak tak, że w prze-

ważającej liczbie przedsiębiorstw brak jest ustaleń dotyczących możliwości korzystania prywatnie ze sprzętu służbowego. W wielu pracowników traktuje taki sprzęt jako dodatkowy bonus do wynagrodzenia, nie zachowując przy tym odpowiedniej ostrożności. Na służbowych komputerach niejednokrotnie przechowujemy jednak poufne dokumenty firmy, których utrata lub wyciek mogą być dla przedsiębiorstw wyjątkowo bolesne. Warto w tym miejscu zauważyć, że niemal 37 proc. ankietowanych przyznało, że to właśnie na komputerze przechowuje najcenniejsze dla siebie dane. Tyle samo przechowuje je na telefonach i tabletach. Jedynie 10 proc. wskazało jako miejsce przechowania dysk przenośny lub chmurę (6,9 proc.).



Gdzie przechowujesz najcenniejsze dla siebie dane?

78,11 proc.

ankietowanych przyznało, że używa
służbowego komputera/telefonu
do celów prywatnych.

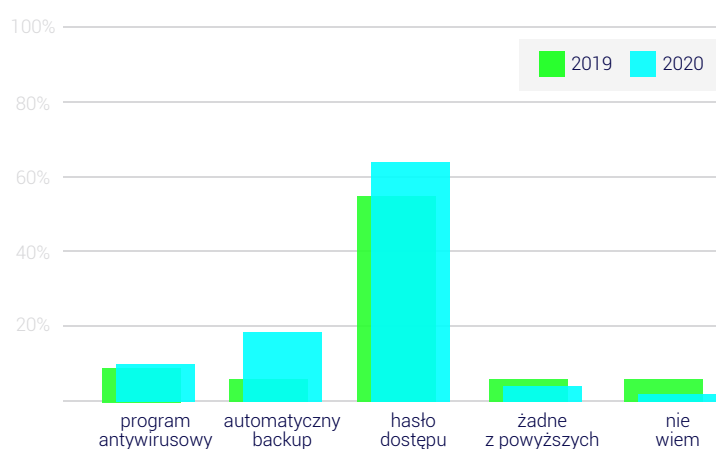
14,43 proc.

ankietowanych przyznało, że ich służbowy
telefon lub tablet zostały zabezpieczone
automatycznym backupem.

46,27 proc.

badanych twierdzi, że ich firma nie
zatrudnia specjalisty w zakresie
bezpieczeństwa danych.

Jednocześnie, również przedsiębiorstwa nie-dostatecznie dbają o powierzony pracownikom sprzęt. Jak wynika z przeprowadzonego przez VECTO badania, jedynie 7 proc. ankietowanych przyznało, że ich służbowy telefon lub laptop zabezpieczone są programem antywirusowym. Automatyczny backup stosowany jest natomiast w zaledwie 20 proc. przypadków. Zaledwie 64 proc. ankietowanych przyznało, że ich sprzęt chroniony jest hasłem.

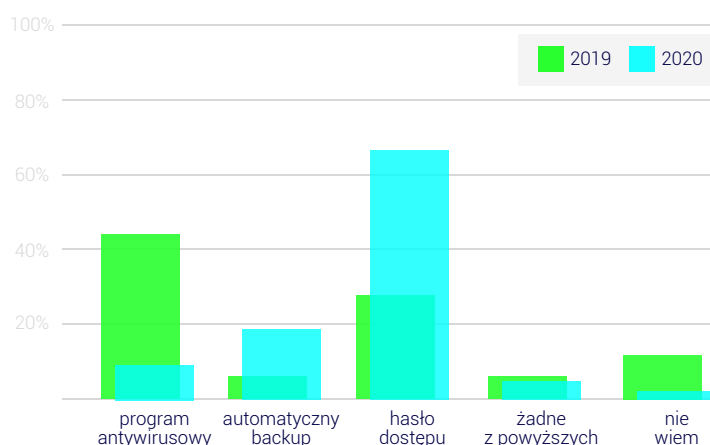


W jaki sposób jest zabezpieczony
Twój firmowy telefon/tablet?

Porównując wyniki z poprzednim rokiem ponownie możemy odnieść wrażenie, że nie jest to dbałość o bezpieczeństwo firmowych zasobów, a jedynie ochrona własnej prywatności. Ponadto możemy domniemywać, że również pracodawcy nie dbają dostatecznie o bezpieczeństwo, nie dostarczając pracownikom odpowiednio zabezpieczonych narzędzi i traktując smartfony jak zwykłe telefony - na co wskazuje wyraźnie ewidentny brak dodatkowego oprogramowania antywirusowego na telefonach i laptopach służbowych.

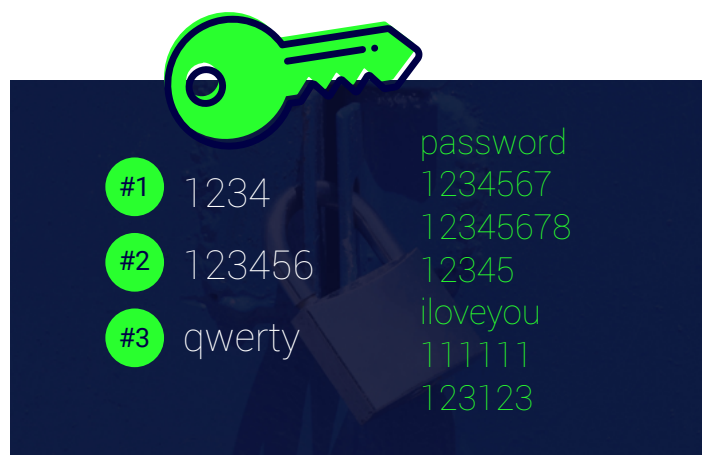
Niewiele lepiej jest w przypadku firmowych komputerów. Niestety zaledwie 27 proc. ankietowanych potwierdziło, że ich komputery chronione są programem antywirusowym. Automatyczny backup stosuje natomiast 14 proc. ankietowanych. Ponad 54 proc. ankietowanych przyznało, że stosuje hasła dostępu, pozostali natomiast nie potrafili zdefiniować zabezpieczeń. Ponadto, jak wynika z badania,

aż 46 proc. ankietowanych wskazało, że w ich przedsiębiorstwach nie zatrudnia się specjalistów od bezpieczeństwa danych. Wynik ten jest zbliżony do ubiegłorocznego - 44 proc.



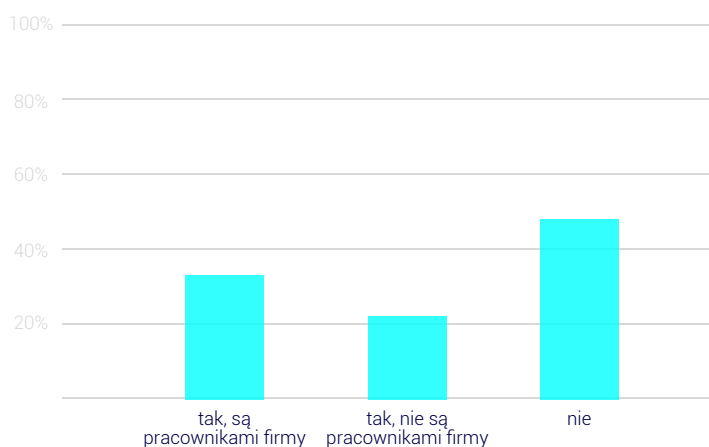
W jaki sposób jest zabezpieczony
Twój firmowy komputer?

Nieco zmalał natomiast odsetek przedsiębiorstw korzystających z zewnętrznej obsługi IT obejmującej kwestie bezpieczeństwa informatycznego - obecnie z usług takich korzysta ok. 21 proc. firm, podczas gdy rok wcześniej było to 24 proc. Możemy śmiało powiedzieć, że dane te są wręcz zatrważające. Wygląda bowiem na to, że nadal traktujemy hasła jako skuteczne zabezpieczenie sprzętu. Jednocześnie, jak wynika z listy stu najgorszych, używanych w sieci haseł, przygotowanej przez SplashData, wciąż królują „1234”, „123456” czy też „qwerty”. Poza podium znaleźć możemy:



Najpopularniejsze hasła wg. SplashData

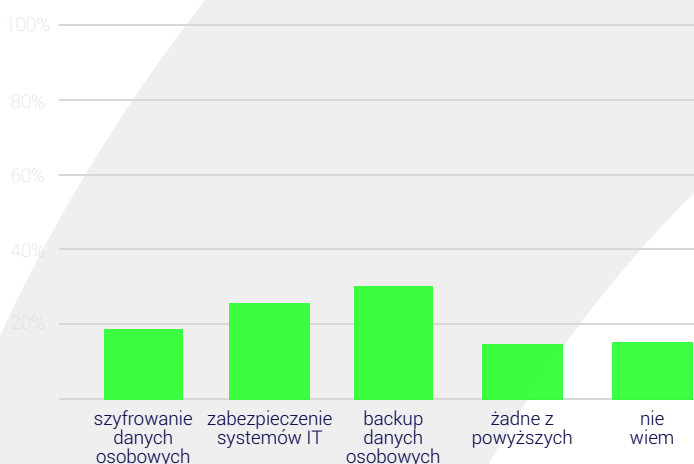
Miejsce 14 zajmuje natomiast znane zapewne nam wszystkim „admin”.³ I choć lista opublikowana przez amerykańską firmę może się nam wydawać daleka od polskiej rzeczywistości, to z doświadczenia możemy powiedzieć, że wiele z tych haseł wciąż króluje w naszych rodzimych przedsiębiorstwach.



Czy Twoja firma zatrudnia specjalistę od bezpieczeństwa danych?

Biznes kar się nie boi?

Niebawem mijają dwa lata od wprowadzenia w życie RODO, a jak wynika z raportu kancelarii DLA Piper, łączna suma kar w państwach Unii Europejskiej za naruszenia związane z RODO wyniosła ponad 114 mln euro.⁴ Mimo to nadal niemal 15 proc. ankietowanych przyznaje, że w ich przedsiębiorstwach nie stosuje się wytycznych wskazanych w dyrektywie. Ponad 26 proc. ankietowanych twierdzi, że w ich firmach stosowany jest Backup i zdolność do szybkiego przywrócenia dostępności danych osobowych i dostępu do nich w razie incydentu fizycznego lub technicznego. 23 proc. ankietowanych dowodzi natomiast, że w ich przedsiębiorstwach stosuje się zabezpieczenie systemów IT na wypadek zewnętrznej, nieuprawnionej ingerencji w ich integralność. W przypadku 19 proc. ankietowanych stosowane jest natomiast szyfrowanie danych osobowych. Aż 30 proc. ankietowanych nie potrafi natomiast wskazać czy i jakie wytyczne są stosowane w ich przedsiębiorstwach.



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



Vecto Cloud Backup

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

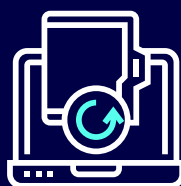
Co otrzymasz?



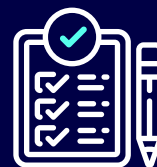
Wykonanie do dwóch kopii
zapasowych dziennie



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



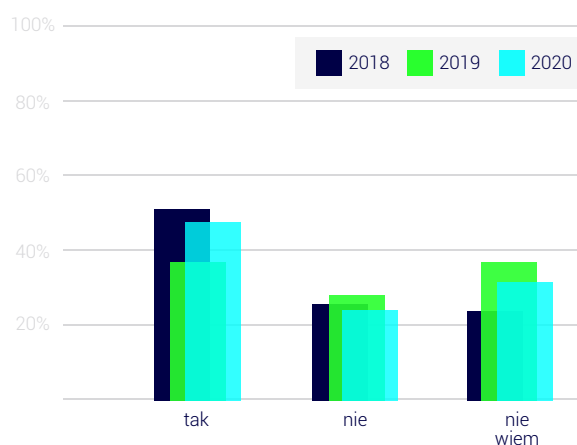
Codzienny raport
backupów

Sprawdź ofertę
www.vecto.pl/vecto-cloud-backup

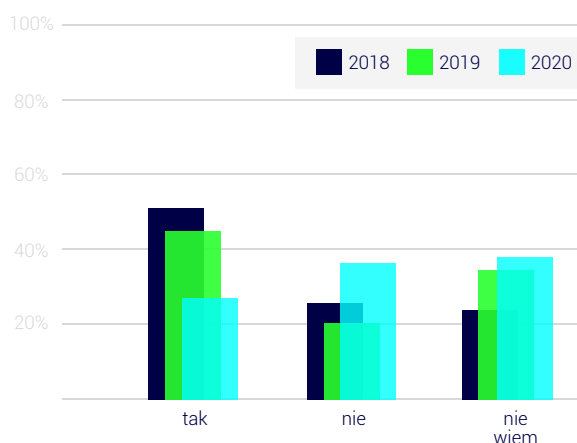
Cyfrowy świat, realne zagrożenia

Granice pomiędzy tym, co wirtualne, a tym co rzeczywiste znacznie się zacierają. Dotyczy to zarówno naszej indywidualnej aktywności w sieci, jak i działań, planów i strategii biznesowych. Jeszcze nie tak dawno, sceptycznie odnosiliśmy się do zawierania wirtualnych znajomości, płatności on-line i zakupów. Dziś e-commerce jest jedną z najdynamiczniej rozwijających się kategorii handlu na świecie. Chętnie korzystamy z usług bankowości internetowej, w sklepach płacimy telefonami, zegarkami i BLIK'iem. Media społecznościowe zaś, stają się główną platformą budowania i utrzymywania relacji społecznych.

Wzajemne przenikanie się obu światów rodzi ogromne niebezpieczeństwa. Korzystając z sieci w celach prywatnych, nie zastanawiamy się nad kwestiami cyberzagrożeń. Czujemy się zwykle anonimowo i nie analizujemy ryzyk, związanych z naszą aktywnością. Tymczasem to właśnie my, użytkownicy sieci, generujemy najczęściej największe zagrożenia. Bezrefleksyjne logowanie się do niezabezpieczonych sieci, otwieranie podejrzanych załączników w mailach, przekazywanie danych wrażliwych poprzez komunikatory rodzą konkretne skutki. W tegorocznym badaniu niemal 45 proc. ankietowanych przyznało, że zetknęło się z cyberatakiem, podczas gdy w ubiegłym roku potwierdziło to 38 proc. badanych firm. Aż 30 proc. badanych przedsiębiorstw nie wie natomiast czy do takiego ataku doszło. Jednocześnie ponad 36 proc. ankietowanych przyznaje, że ich firmy nie monitorują zagrożeń związanych z cyberatakami, a niemal 32 proc. nie ma na ten temat wiedzy. Niespełna 26 proc. ankietowanych przedsiębiorstw monitoruje zagrożenia.



Czy Twoja firma kiedykolwiek zetknęła się z cyberatakiem?



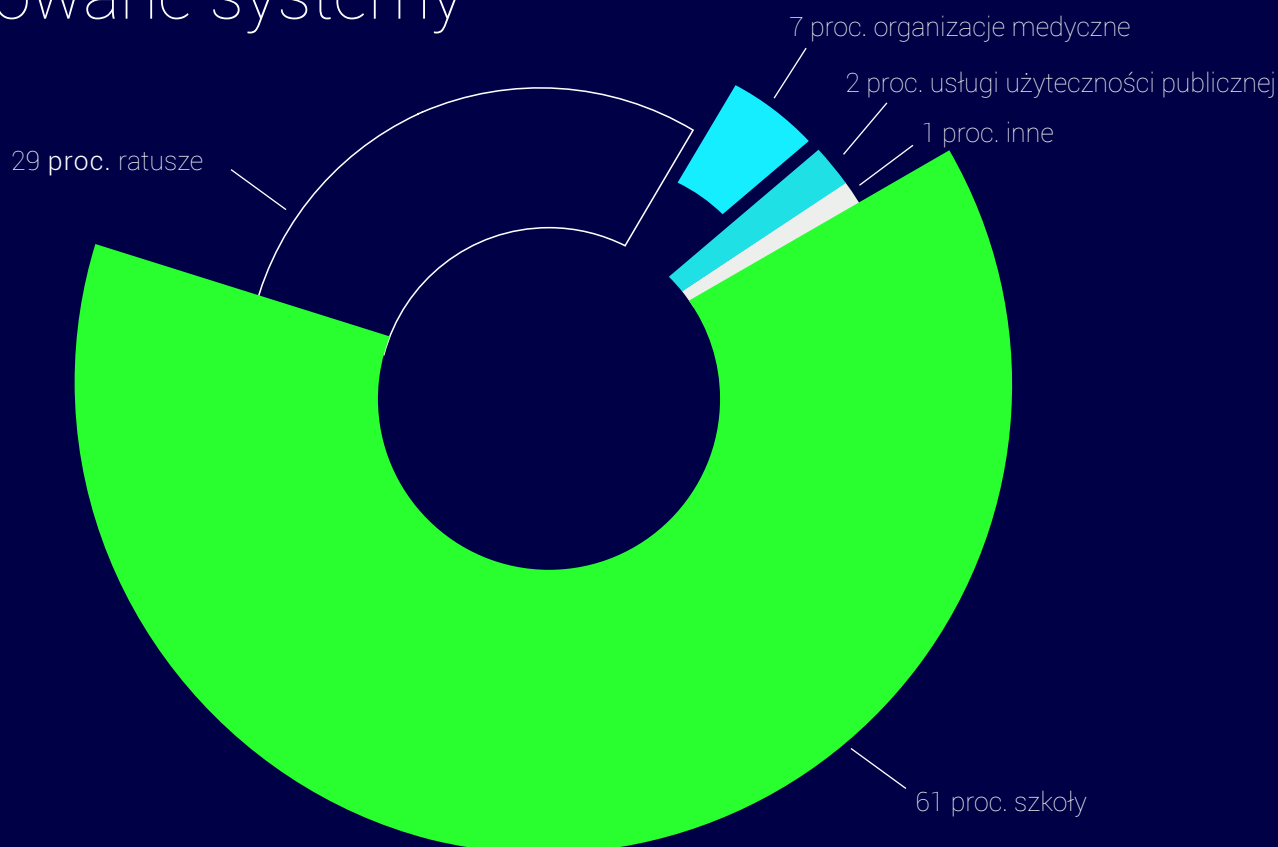
Czy Twoja firma monitoruje zagrożenia wynikające z cyberprzestępczości?

44 proc. ankietowanych uważa, że sieć w ich firmie jest prawidłowo zabezpieczona. W ubiegłym roku takie odczucia miało mniej niż 1 na 3 badanych, co może potwierdzać, że firmy zaczęły aktywnie inwestować w zabezpieczenia. Znacznie zmalał natomiast odsetek odpowiedzi przeczących. W poprzednim badaniu aż 41,3 proc. badanych wskazywało, że sieć firmowa w ich przedsiębiorstwach nie jest prawidłowo zabezpieczona. Obecnie jest to zaledwie 13,4 proc.. Ponad 42 proc. badanych nie jest natomiast w stanie wyrazić jednoznacznej opinii na ten temat lub nie ma wiedzy na temat zabezpieczeń. Jest to dość zastanawiający wynik, biorąc pod uwagę fakt, iż niemal 48 proc. ankietowanych przyznało, że w ich przedsiębiorstwach nie funkcjonuje procedura okresowej zmiany haseł dostępowych, a jak już wspominaliśmy – najpopularniejszym sposobem zabezpieczeń zarówno komputerów, jak też telefo-

nów czy tabletów, są właśnie hasła. Wniosek może być tylko jeden. Świadomość zagadnień związanych z cyberbezpieczeństwem rośnie, ale polskie firmy i wciąż robią zbyt mało, by edukować i minimalizować ryzyka, wynikające z codziennego korzystania z sieci. Niekiedy wystarczy zwykła ostrożność, by uniknąć kłopotów. Ataki typu ransomware bazują przede wszystkim na bezmyślnym otwieraniu załączników, które przychodzą w mailach. Tymczasem, jak informuje Kaspersky, w 2019 roku 174 instytucje miejskie i ponad 3000 podległych organizacji padło ofiarą ataków ransomware* (wzrost o min. 60 proc. w stosunku do roku poprzedniego). Wśród nich 7 proc. stanowiły organizacje medyczne, 2 proc. usługi użyteczności publicznej, 29 proc. ratusze, 61 proc. szkoły i 1 proc. inne. Średnia wartość żądań związanych z okupem wyniosła natomiast 1 032 460.⁵

* ransomware - szkodliwe oprogramowanie komputerowe szyfrujące dane należące do użytkownika sieci, a następnie wymagające wpłaty okupu w zamian za ich odszyfrowanie

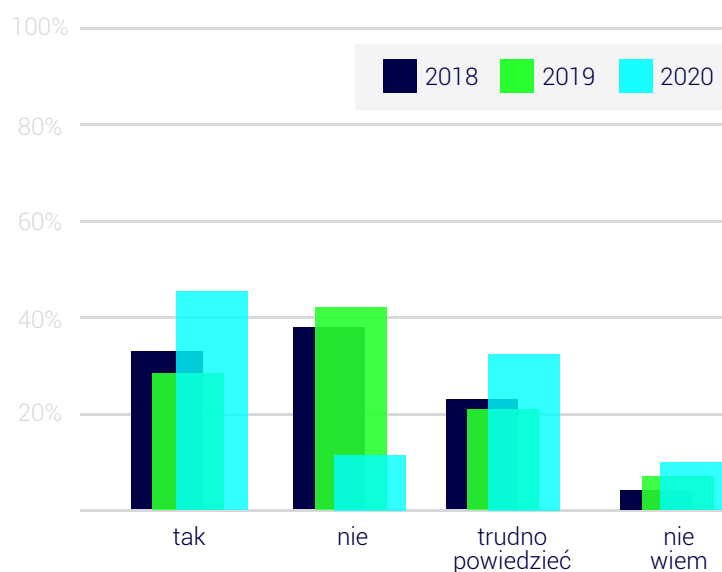
Atakowane systemy



Średnia wartość żądań okupu: 1 032 460 \$

Nie trudno więc dojść do wniosku, że nie ze wszystkich zagrożeń zdajemy sobie sprawę. Według 5 edycji badania CISO Benchmark Study 2019 aż 65 proc. Respondentów przyznaje, że ma trudności z określeniem zakresu naruszeń bezpieczeństwa, ograniczaniem ich wpływu, a także zapobieganiem im w przyszłości.⁶ Znaczenie ma tu przede wszystkim niewystarczające edukowanie pracowników i brak procedur bezpieczeństwa. Opieszałość w podnoszeniu kompetencji na tym polu bywa kosztowna. Z pewnością wielu z czytających ten raport otrzymało maila z informacją o przejęciu kontroli nad skrzynką pocztową czy komputerem przez osoby nieuprawnione, oczekujące okupu lub innej gratyfikacji za nieudostępnianie danych, do których rzekomo cyberprzestępcy uzyskali dostęp. Wiadomości tego typu to najczęściej bluff, jednak część odbiorców takiej korespondencji decyduje się na spełnienie zawartych w niej żądań. Tego typu phishing stał się dziś niezwykle powszechnym zjawiskiem i pomimo nagłośniania w mediach i powszechnym dyskusjom na forach internetowych, ofiarami tego typu ataków może być aż ¼ internautów.⁷

Jak widać cyberprzestępcy stają się coraz bardziej zuchwali. Jednak my sami często też ułatwiamy sprawę. Wszystko przez... narzędzia mające nam ułatwić życie. Wystarczy chociażby spojrzeć na Google Play. Często sięgamy tam w poszukiwaniu różnego rodzaju aplikacji, biorąc za pewnik bezpieczeństwo sklepu. Nic jednak bardziej mylnego. Zaledwie kilka miesięcy temu z Google Play usunięte zostały 42 aplikacje zawierające malware*, które pobrano aż 8 milionów razy. Ich działanie opierało się przede wszystkim na wyświetlaniu użytkownikom dużych, uciążliwych reklam. Z kolei około pół miliona razy pobrano aplikacje z wirusem Joker, który automatycznie rejestrował użytkowników androida w serwisach subskrypcyjnych. Jak donosiły media, wirus ten potrafił przechwytywać kody SMS. Złośliwe oprogramowanie znaleziono w 24 aplikacjach. Instalacja każdej z nich na służbowym telefonie z podpętą firmową kartą mogła mieć kosztowne skutki.



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

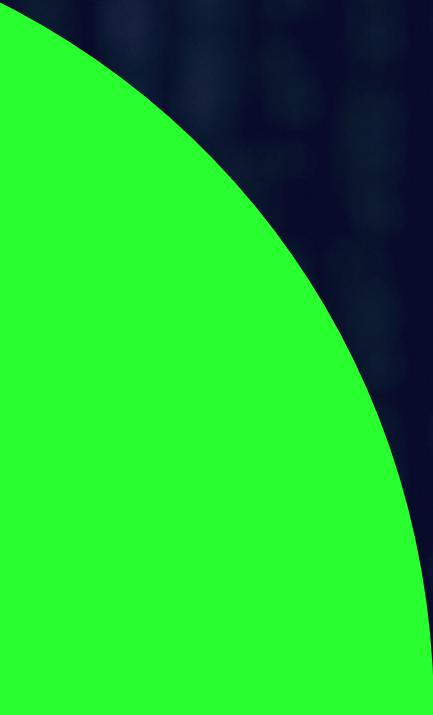


Według 5. edycji badania CISO Benchmark Study 2019 aż

65 proc.

respondentów przyznaje, że ma trudności z określeniem zakresu naruszeń bezpieczeństwa, ograniczaniem ich wpływu, a także zapobieganiem im w przyszłości.

* malware - oprogramowanie komputerowe o działaniu szkodliwym dla komputerów lub systemów komputerowych (<http://nowewyrazy.uw.edu.pl/>)



44,78 proc.

ankietowanych przyznało, że ich firma
zetknęła się z cyberatakiem.



15,92 proc.

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

32,84 proc.

ankietowanych nie potrafi określić, czy sieć
w ich przedsiębiorstwach jest prawidłowo
zabezpieczona.

OUTSOURCING IT

Wycena obsługi w **48 godzin**

Dzięki strategii **#outIT** zyskasz



20 min - maksymalny czas
reakcji obsługi zdalnej



24h wsparcie techniczne

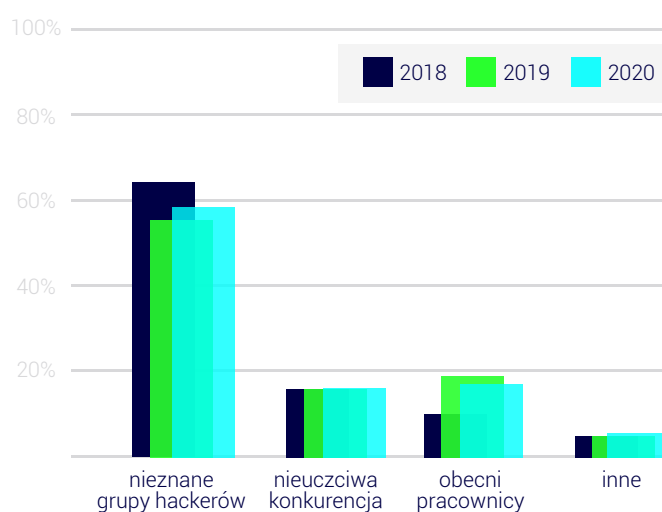


nawet 40 proc. oszczędności
w stosunku do kosztów własnego
działu IT

Sprawdź ofertę
www.vecto.pl/outsourcing-it

Czy Twoja firma jest w grupie ryzyka?

Za główne źródła zagrożeń cyfrowych dla przedsiębiorstw nadal uważamy nieznane grupy hackerów. Odpowiedziało w ten sposób 59 proc. ankietowanych. Ponad 16 proc. uważa, że jest nimi nieuczciwa konkurencja, a niemal 18 proc. wini obecnych pracowników. Jedynie niewiele ponad 6 proc. twierdzi, że zagrożenia pochodzą z innych źródeł. Podobnie odpowiedzi kształtowały się w roku ubiegłym. Wówczas również większość odpowiedzi (55,7 proc.) wskazywała, że za niebezpieczeństwem stoi nieznana grupa hackerów. Niemal 20 proc. respondentów za winnych naruszeń uważało obecnych pracowników. Możemy to jednak rozpatrywać dwojako. Wciąż nie dostrzegamy własnych niedociągnięć i nieostrożności, takich jak używanie służbowego sprzętu w celach prywatnych, czysto rozrywkowych, czy też braku odpowiednich zabezpieczeń. Ostatecznie warto sobie zadać pytanie czy to nie my sami stanowimy największe zagrożenie dla bezpieczeństwa firmowych danych i systemów IT.



Wskaż główne, Twoim zdaniem, źródło zagrożeń cyfrowych dla Twojej firmy

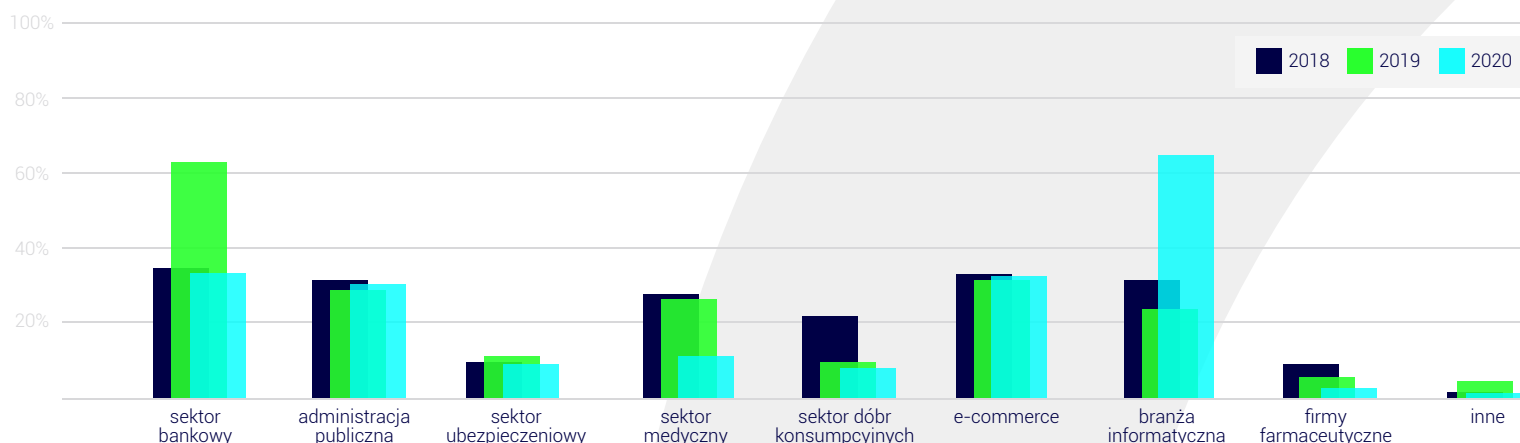
Kto jest narażony najbardziej?

Za najbardziej narażoną na cyberataki ankietowani uznali branżę IT. Na kolejnym miejscu wskazany został sektor bankowy – 35 proc. i e-commerce – niemal 33 proc..

Co ciekawe, gdy spojrzymy na przedstawicieli branż reprezentowanych przez respondentów, najliczniejszą grupę stanowi właśnie przemysł komputerowy – łącznie 23 proc. Na drugim miejscu zaś plasuje się bankowość i finanse – 17 proc. respondentów – a na trzecim instytucje rządowe i samorządowe (administrację publiczną wśród najbardziej zagrożonych sektorów wskazało niemal 28 proc. respondentów), które reprezentowało niemal 11 proc. ankietowanych. Wygląda na to, że za najbardziej zagrożone branże uznajemy najczęściej te, które sami reprezentujemy. Jak jednak dowodzą badania prowadzone przez Kaspersky, to właśnie polska energetyka jest najbardziej narażona na cyberataki. Zgodnie z nimi w pierwszym półroczu 2019 roku aż 41,6 proc. komputerów używanych w systemach za-

ządzania przedsiębiorstwami energetycznymi mogło być celem cyberataku.⁹

Ponad 23 proc. respondentów uważa, że najbardziej narażone na cyberataki są mikroprzedsiębiorstwa, a niemal 30 proc., że są to duże firmy. Ponownie największa grupa respondentów wskazała, że ich zdaniem do najbardziej narażonych należą duże firmy.





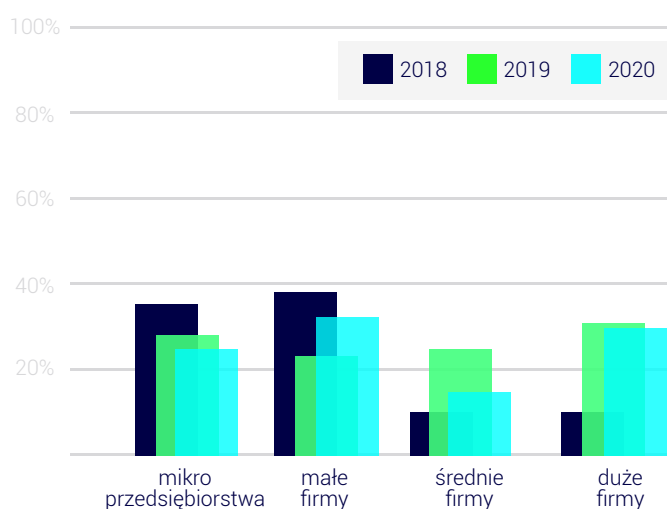
Według badań
prowadzonych
przez Kaspersky,
najbardziej narażona
na cyberataki
jest **polska
energetyka.**

Reprezentowana branża

budownictwo / architektura / wykończenie wnętrz	3,0 proc.
edukacja / badania naukowe	2,4 proc.
finanse / bankowość	17,3 proc.
hotelarstwo / turystyka / rekreacja / sport	3,0 proc.
handel hurtowy i detaliczny	4,9 proc.
instytucje rządowe i samorządowe	11,0 proc.
łączność / telekomunikacja	4,0 proc.
media / kultura i sztuka / rozrywka	6,5 proc.
medycyna / ochrona zdrowia	8,9 proc.
produkcja / dystrybucja / logistyka	3,0 proc.
przemysł komputerowy / oprogramowanie	5,0 proc.
przemysł komputerowy / sprzęt	19,0 proc.
usługi dla firm / usługi dla klientów indywidualnych	7,0 proc.
usługi internetowe	2,0 proc.
inna	3,0 proc.

W tym roku VECTO ponownie sprawdziło również, które obszary prowadzenia działalności biznesowej są dla przedsiębiorstw najcenniejsze. Wśród obszarów, których utrata byłaby najbardziej dotkliwa dla firm, ankietowani najczęściej wymieniali bazę klientów i kontaktów – 3,6 pkt. W równym stopniu wskazywane były również unikalne know-how i własność intelektualna – 3,3 pkt., korespondencja firmowa – 3,3 pkt oraz dokumentacja firmowa – 3,3 pkt. Najrzadziej wspomnianą była natomiast strona internetowa przedsiębiorstwa – 2,9 pkt.

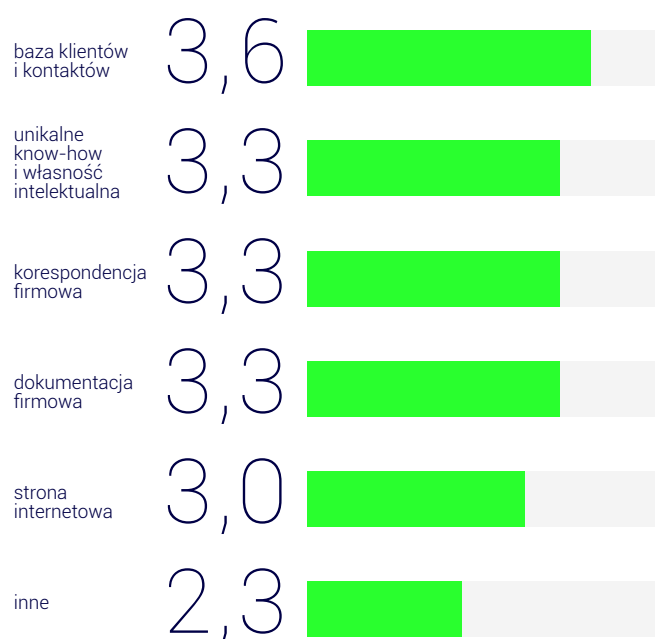
Nie tylko straty związane z bazą klientów i dokumentacją firmową budzą nasze obawy. Wśród najbardziej prawdopodobnych skutków cyberataków wymieniamy bowiem możliwość wystąpienia strat finansowych - odpowiedź ta otrzymała niemal 4 pkt. Niemal równie bardzo obawiamy się również osłabienia wizerunku firmy i zaufania otoczenia biznesowego - 3,47 pkt. w 5 stopniowej skali - utraty klientów (3,31 pkt.) oraz zamknięcia firmy (3,11 pkt.).



Jakie firmy są Twoim zdaniem szczególnie narażone na utratę danych?

Oceń obszary, w których utrata danych byłaby dla Twojej firmy najbardziej dotkliwa

(1 – mało dotkliwa, 5 – bardzo dotkliwa)



Podsumowanie

Granice digitalizacji otaczającego nas świata wciąż są przesuwane. Innowacyjne rozwiązania informatyczne coraz zuchwalej wkraczają w nasze codzienne życie, determinując rozkład dnia, podejmowane decyzje czy dotychczasowe modele pracy i prowadzenia biznesu. Dziś praca zdalna nie budzi zdziwienia, aplikacje wykorzystujemy do czynności, które dotychczas wykonywaliśmy bez cyfrowego wsparcia. Generujemy gigantyczne ilości danych, których liczbę w samym internecie szacuje się na 10 jottabajtów. Ten przyrost nie zwolni, wręcz przeciwnie, ludzkość będzie produkowała coraz więcej informacji i kluczowe dla naszej przyszłości będzie to, jak poradzimy sobie z zarządzaniem tak ogromnym zbiorem danych. Dotyczy to oczywiście również i działalności biznesowej. Umiejętne wykorzystanie danych już obecnie wpływa bezpośrednio na konkurencyjność i sukces firm. Z wykorzystaniem rozwiązań IT skracamy czas produkcji, przetwarzania zamówień, procesy decyzyjne determinowane są przez analizę dostępnych danych.

Dane i informacje wyznaczają tempo i kierunek funkcjonowania świata. Musimy zatem o nie dbać, chronić je i umieć przetwarzać w sposób, który zapewni nam dalszy rozwój i bezpieczeństwo. Czy polskie firmy z należytą atencją podchodzą do tych wyzwań? Wyniki niniejszego Raportu wyraźnie wskazują, że wciąż mamy z tym problem. Polskie firmy są świadome zagrożeń, ale rozpatrujemy je w kategoriach zdarzeń hipotetycznych. Zwykle kierujemy się wiarą, że prowadzimy biznes w segmencie lub skali, która nie jest

objęta zainteresowaniem cybergrup przestępczych. Wciąż zapominamy, że o wzięciu naszej firmy na cel przez hakerów nie decyduje wyłącznie obecność w gronie przedsiębiorstw o strategicznym znaczeniu dla państwa czy gospodarki. Cyberprzestępcy i szkodliwe oprogramowanie zbierają żniwa przede wszystkim tam, gdzie atak jest łatwy do wykonania i wiąże się z najmniejszym ryzykiem wykrycia. To narzędzia skanujące luki w zabezpieczeniach systemów IT definiują czy staniemy się obiektem ataku.

Jeśli chcemy myśleć o bezpieczeństwie polskich przedsiębiorstw musimy podjąć wyzwanie i zredukować ryzyko ponoszenia kosztów cyberincydentów. A te są niemałe. Według badania 2019 CISO Benchmark Study, 45 proc. respondentów wskazało, że koszt pojedynczego cyberataku na ich organizację wyniósł ponad pół miliona dolarów. Zapewne większość polskich przedsiębiorstw nawet nie wyobraża sobie konieczności poniesienia tak dużych wydatków na naprawianie szkód wynikających z utraty danych lub naruszenia ich integralności. Tymczasem nie robimy zbyt wiele, by utrudniać cyberprzestępcom ich szkodliwą działalność. Oszczędności w stosowaniu ochrony antywirusowej i rozwiązań backupowych komputerów stacjonarnych i mobilnych przez polskie firmy dobitnie wybrzmiewa w niniejszym Raporcie. Dodatkowym zagrożeniem stają się smartfony i tablety, które zwykle stanowią najłabsze ogniwo w firmowym systemie IT. Wykorzystujemy je chętnie do celów prywatnych, zostawiamy w miejscach publicznych i korzystamy z ogólnodostępnych sieci wi-fi.

W końcu, instalujemy aplikacje bez sprawdzenia stosownych certyfikatów bezpieczeństwa.

To, że Polska znalazła się w gronie 20 państw najbardziej zagrożonych cyberatakami stało się faktem. Dotychczasowe doniesienia o atakach na przedsiębiorstwa energetyczne czy spektakularny atak typu DDoS na największą firmę hostingową w Polsce wyraźnie tego dowodzą. W ubiegłym roku za wyciek danych słono zapłacił sklep internetowy morele.net. Urząd Ochrony Danych Osobowych nałożył na przedsiębiorcę 2,8 mln zł kary za wyciek danych, do którego doszło w grudniu 2018 r. Nie istnieją dane, na podstawie których moglibyśmy jednoznacznie oszacować rzeczywiste koszty cyberincydentów w Polsce. Warto nadto podkreślić, że firmy niechętnie dzielą się tego typu informacjami, traktując cyberatak jako szkodę wizerunkową i zagrożenie w utrzymaniu pozytywnych relacji z otoczeniem biznesowym. Tymczasem niemal połowa badanych przez nas firm potwierdziła odnotowanie cyberataku, a wynik ten z pewnością nie tworzy optymistycznej perspektywy na przyszłość.

Przedsiębiorcy mają możliwość skorzystania z szerokiego katalogu rozwiązań, które znacząco zwiększają bezpieczeństwo IT. 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, aby zweryfikować kwestię zabezpieczenia danych i infrastruktury IT. Tylko dbając o bezpieczeństwo firmowych danych i zasobów informatycznych, możemy skutecznie zadbać o przyszłość naszego biznesu.

Jakub Wychowański,
członek zarządu VECTO



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, uzależniając 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

Metodologia

Badanie zostało przeprowadzone w formie ankiety internetowej i papierowej od kwietnia do grudnia 2019 r. na próbie 201 przedsiębiorstw.

Największą grupę respondentów stanowili przedstawiciele przemysłu komputerowego - łącznie 23 proc. badanych. 17,4 proc. badanych stanowili przedstawiciele finansów i bankowości, a 10,9 instytucje rządowe i samorządy. Wśród respondentów dominowali przedstawiciele przedsiębiorstw zatrudniających 11-50 osób - 43,7 proc. Na drugim

miejscu znalazły się przedsiębiorstwa zatrudniające powyżej 50 osób (24,3 proc.). 18,9 proc. były to przedsiębiorstwa zatrudniające 1-5 osób, zaś najmniejszą liczbę respondentów stanowiły firmy zatrudniające 6-10 osób (12,9 proc.).

Przypisy końcowe

1. www.wdib.uw.edu.pl/attachments/article/2535/FOM0%202019_Raport.pdf
2. www.pbi.org.pl/raporty/polscy-internauci-w-grudniu-2019
3. www.teamsid.com/1-50-worst-passwords-2019
4. www.research.fb.com/blog/2016/02/three-and-a-half-degrees-of-separation
5. <https://prawo.gazetaprawna.pl/artykuly/1449785,polska-ue-zgloszenia-incydentow-z-rodo-raport.html>
6. <https://www.kaspersky.pl/o-nas/informacje-prasowe/3205/oprogramowanie-ransomware-kontra-instytucje-miejskie-w-2019-r-liczba-ofiar-wynosi-174-i-wciaz-rosnie>
7. <https://www.cyberdefence24.pl/wymagane-sprawdzenie-poprawnosci-hasla-nie-daj-sie-oszukac-cyberprzestepcom>
8. www.businessinsider.com.pl/firmy/zarządzanie/cyberataki-w-firmach-raport-ciso-benchmark-study-2019/tjet737
9. www.archiwum.rp.pl/artikul/1413387-Energetyka-na-pierwszej-linii-frontu.html

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



**GAZELE
XX BIZNESU**

EDYCJA

RANKINGU NAJBARDZIEJ DYNAMICZNYCH MAŁYCH I ŚREDNICH FIRM



Spółka VECTO znalazła się w gronie laureatów tegorocznej edycji Gazel Biznesu.

