VI edycja · 2023

VECTO

RAPORT

Cyberbezpieczeństwo
w polskich firmach

Dell EMC PowerProtect

nowy wymiar zabezpieczeń

SPIS treści

WSTĘP

Pandemia, wojna w Ukrainie, aktywność Chin na arenie międzynarodowej i ich konflikt gospodarczy z USA, których w ostatnich latach świadkami jesteśmy, stanowiły istotny impuls dla dynamicznego wzrostu zagrożeń w obszarze cyberbezpieczeństwa. Coraz groźniejsze incydenty, tak dotkliwie doświadczające firmy na całym świecie, stają się również przykrą rzeczywistością dla wielu polskich firm. Poprzednie edycje Raportu VECTO: Cyberbezpieczeństwo polskich firm niezbicie dowodziły, że skala zagrożeń jest niezmiennie w tendencji rosnącej, kreśląc pesymistyczne perspektywy dla przedsiębiorstw wielu branż i instytucji publicznych. Lektura niniejszego Raportu, podsumowującego badanie w 2023 roku, pozwólcie Państwo, że pozwolę sobie uchylenie rąbka tajemnicy, wskazuje, że nasze przewidywania, a także opinia przytłaczającej większości specjalistów okazały się słuszne. Niemal w każdym tygodniu, media i organizacje monitorujące naruszenia bezpieczeństwa danych, donosiły o kolejnych atakach hakerów, wyciekach danych i coraz nowszych metodach dokonywania przestępstw w sieci. Nie ma żadnych podstaw, aby oczekiwać odwrócenia tego trendu, szczególnie, że cyberprzestępczość wciąż zdaje się być o krok przed „jasną stroną cybernetycznej mocy".

Od wielu lat niezmiennie podkreślamy również, że podstawą do zmiany pesymistycznych trendów jest rosnąca świadomość. Już pierwszej edycji naszego Raportu przyświecał ten właśnie cel – upowszechnienie wiedzy, zrozumienie zagrożeń, identyfikacja mocnych i słabych stron rozwiązań i praktyk stosowanych przez polskie firmy. Wierzymy, że diagnozowanie aktualnego stanu rzeczy w kontekście naszej gotowości do skutecznego przeciwdziałania skutkom cyberprzestępczości, stanowiło i stanowi punkt wyjścia dla wielu rodzimych aby prewencyjnie zabezpieczyć się na wypadek szkody w systemach IT, zanim ona nastąpi.

Serdecznie zapraszam do zapoznania się z wynikami Raportu i zachęcam wszystkie firmy i instytucje, bez względu na wielkość zatrudnienia czy skalę działalności do konsekwentnego konsultowania i analizowania stanu zabezpieczeń informatycznych z ekspertami, działającymi na polskim rynku. Jako przedstawiciel tej branży wiem, że mamy zarówno kompetencje i doświadczenia, jak również dostęp do najlepszych rozwiązań na świecie, które konsekwentnie zwiększają poziom bezpieczeństwa Państwa infrastruktury IT danych i nie pozwalają tracić dystansu w cybernetycznym wyścigu dobra ze złem.

Jakub Wychowański
Prezes Zarządu VECTO

CYBERATAK

Dostępne analizy i opracowania wyraźnie wskazują, że coraz więcej polskich firm deklaruje gotowość na realizowanie ambitnych celów związanych z zapewnieniem należytego poziomu cyberochrony. W naszej ocenie jest to bardzo pozytywny impuls, dający nadzieję, że rozumiemy skalę dzisiejszych zagrożeń. O tym, że czynniki geopolityczne i światowe kryzysy, zachęciły cyberprzestępców do większej aktywności w naszej części Europy wskazują między innymi analizy Comaritech, który uwzględnia nasz kraj w gronie państw najbardziej zagrożonych cyberatakiem. W rankingu NCSI zajmujemy 11. lokatę wśród wszystkich państw, które w najbliższym czasie będą zmagały się z rosnącą liczbą cyberincydentów. Potwierdzeniem tych ekspertyz są liczne, spektakularne ataki na polskie firmy i instytucje, których świadkami byliśmy w tym i mijających latach. Wynikały one głównie z niskiego poziomu zabezpieczeń stron internetowych i wewnętrznych systemów instytucji państwowych, a także firm obsługujących tzw. infrastrukturę krytyczną. Przykłady można mnożyć - wyciek danych dotyczących polskiego uzbrojenia, ujawnienie tajnych danych z KPRM, włamania do systemów kontroli ruchu pociągów. Nie wspominając o korespondencji wieloletniego ministra w kancelarii premiera, która w częściach regularnie była ujawniana na polskich i zagranicznych serwerach.

Według specjalistów CERT Polska (Computer Emergency Response Team), dzięki licznym kampaniom edukacyjnym, informacjom prasowym i ostrzeżeniom publikowanym w mediach społecznościowych - wzrosła wiedza o cyberzagrożeniach. Przełożyło się to na rekordową liczbę zgłoszeń. W 2022 r. do CERT Polska wpłynęło ponad 322 tys. zgłoszeń, co skutkowało obsłużeniem 39 tys. incydentów. To ponad 34 proc. wzrost zarejestrowanych incydentów w zestawieniu z 2021 r., zaś liczba wszystkich zgłoszeń wzrosła o blisko 178 proc.

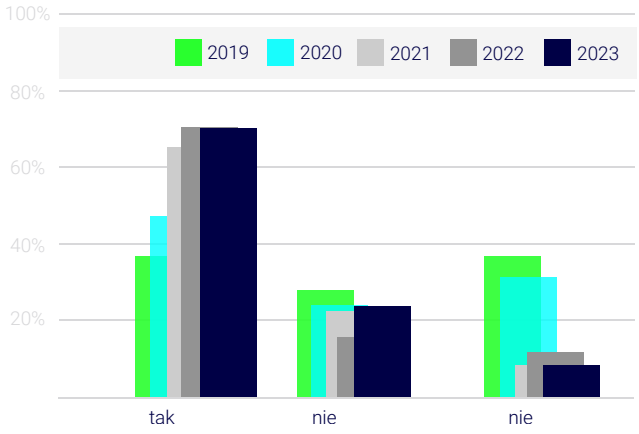
Ubiegły rok na świecie był po raz kolejny rekordowy pod względem cyberataków – ich liczba wzrosła o 38 proc. w porównaniu z poprzednim rokiem, a średnia tygodniowa liczba ataków na organizację na całym świecie osiągnęła poziom ponad 1130.

Jak słusznie zauważył CERT Polska, tak drastyczny skok skali cyberincydentów, szczególnie na podmioty infrastruktury krytycznej, przypomnijmy o 178 proc., wynikał z wybuchu konfliktu zbrojnego za naszą wschodnią granica. Po raz pierwszy, jak czytamy w opracowaniach CERT, możemy obserwować, jak tradycyjne działania wojenne wspierane są przez aktywności w cyberświecie.

Ze wspomnianego raportu wynika również, że wojna nie tylko spowodowała zwiększenie liczby ataków na polskie instytucje, ale stała się też motywem przewodnim dla pospolitych wyłudzeń. Oszuści tworzyli m.in. fałszywe panele do logowania na Facebooka z chwytliwymi artykułami, np. informującymi o śmierci prezydenta Ukrainy. Celem było pozyskanie hasła, co potem służyło do wyłudzania pieniędzy od znajomych ofiary. CERT Polska odnotował też próby wyłudzenia pieniędzy pod przykrywką działań pomocowych, masowych wysyłek fałszywych maili o podłożeniu bomby „z zemsty za pomoc Ukraińcom", czy nawet tworzenia fałszywych sklepów z węglem w czasie wystąpienia braku tego surowca na przełomie 2022 i 2023 roku.

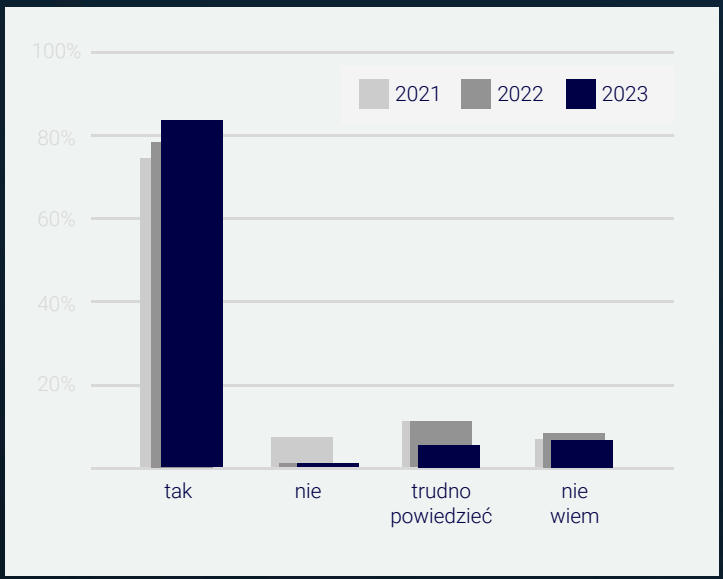
Analiza CERT znajduje odzwierciedlenie w wynikach niniejszego Raportu. 2023 rok jest kolejnym z rzędu, w którym rośnie odsetek firm odnotowujących wystąpienie zdarzenia naruszającego bezpieczeństwo lub integralność danych. W 2023 roku, potwierdza cyberincydenty już 68,9 proc. polskich firm, a porównaniu z 2022 rokiem jest to wzrost o niemal 5 proc.

Zdecydowana większość firm jest świadoma zagrożeń wynikających z cybeprzestepczości. W tegorocznej edycji badania 82,8 proc. odpowiedziało, że zabezpieczanie danych informatycznych w firmie jest ważne. To zdecydowanie wyższy wynik niż w roku ubiegłym, gdy tę odpowiedź wskazało 74 proc. badanych. Podobny trend widać w odpowiedziach na pytanie czy sieć w firmie jest prawidłowo zabezpieczona. Twierdząco odpowiedziało 31,1 proc. ankietowanych i ponownie to wyższy wynik niż przed rokiem – wówczas takiej odpowiedzi udzieliło 23 proc. Z kolei przecząco na to pytanie odpowiada 32 proc. badanych, wobec 28,7 proc. przed rokiem.

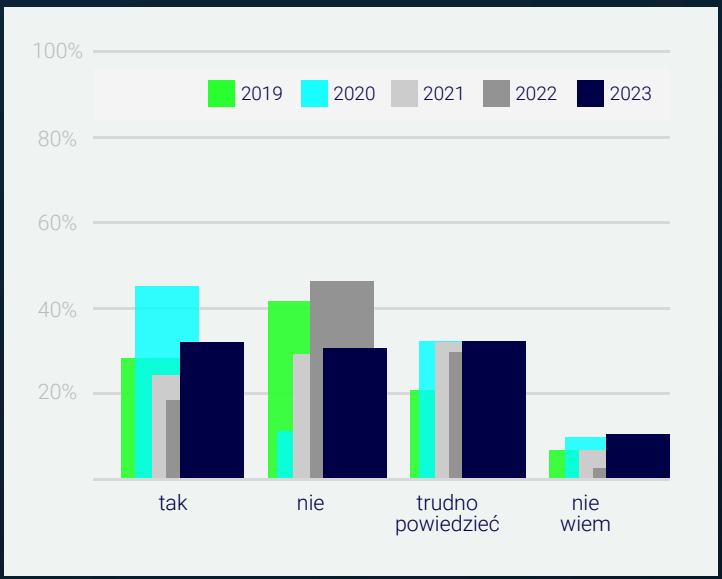


Czy twoja firma zetknęła się kiedykolwiek z cyberatakiem?

Wciąż, wśród wielu polskich firm, pokutuje przeświadczenie, że jeśli dojdzie do kryzysu to uderzy on w przede wszystkim w innych i to pomimo to, że ze skutkami działań hakerów jako społeczeństwo stykamy się regularnie - choćby w postaci zablokowanych stron internetowych banków, portali internetowych czy komplikacjach z funkcjonowaniem sieci kolejowej.



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



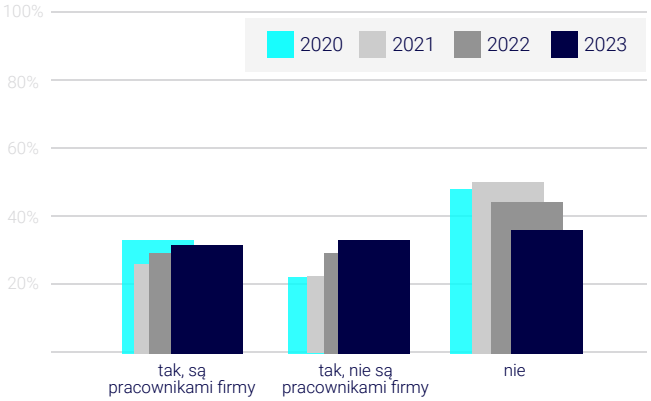
Czy uważasz, że sieć w Twojej firmie jest prawidłowo zabezpieczona?

Co czwarta firma bez cyberochrony

Pomimo regularności tego typu doniesień, specjalistę od bezpieczeństwa danych zatrudnia tylko 28 proc. ankietowanych przedsiębiorstw, co jest minimalnie lepszym wynikiem w porównaniu z ubiegłym rokiem, gdy tę odpowiedź wskazało 26 proc. Zdecydowanie częściej potwierdzano jednak korzystanie z zewnętrznych specjalistów od cyberbezpieczeństwa, w 2023 roku przyznało to 33,4 proc., czyli o 11,5 proc. więcej niż przed rokiem. Spadł również odsetek respondentów twierdzących, że w ich firmach nie korzysta się z usług tego typu ekspertów – z 51 proc. do 38,7 proc. Dane są zatem nieco bardziej obiecujące, niż przed rokiem, ale wciąż wskazujące, że największe wyzwanie dla cyberbezpieczeństwa nie dotyczy procedur, systemów, czy regulacji, a świadomości zagrożeń. Analitycy wskazują, że 60 proc. naruszeń systemów ma w sobie element inżynierii społecznej i wpływu oraz manipulacji wywieranych wprost na ludzi. To właśnie na błędach tzw. czynnika ludzkiego przestępcy najczęściej opierają swoje działania i są w tym aspekcie brutalnie skuteczni. Bez uświadomienia sobie tego zagrożenia problemów będzie z pewnością tylko przybywało.

W świetle odpowiedzi na kolejne pytanie, wspomniany czynnik ludzki może zagrożenia wyłącznie potęgować. Zdaniem 94 proc. ankietowanych wszyscy lub niemal wszyscy zatrudnieni w firmie mają dostęp do firmowej infrastruktury IT, w tym komputerów, smartfonów, tabletów. Skoro takie są realia pracy polskich przedsiębiorstw, to tym bardziej niepokoi niefrasobliwość w zakresie podejścia do stałego monitorowania infrastruktury IT przez specjalistów. Wystarczy bowiem jeden nierozważnie otwarty załącznik do maila lub zainfekowany wirusem pendrive, by cały system IT firmy mógł poważnie ucierpieć. Tymczasem w takich sytuacjach, co podkreślimy w dalszej części Raportu, większość badanych firm nie wiedziałoby jak zareagować. Oznacza to, że błąd ludzki może stanowić najsłabsze ogniwo w całym systemie, nawet jeśli będzie on zabezpieczony odpowiednim oprogramowaniem. Tym bardziej, że hakerzy wymyślają wciąż nowe sposoby, by złamać nawet najlepsze systemy bezpieczeństwa.

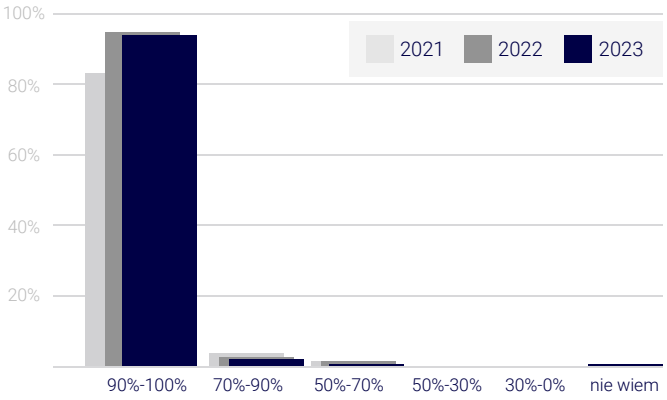
Czy twoja firma zatrudnia specjalistę od bezpieczeństwa danych?



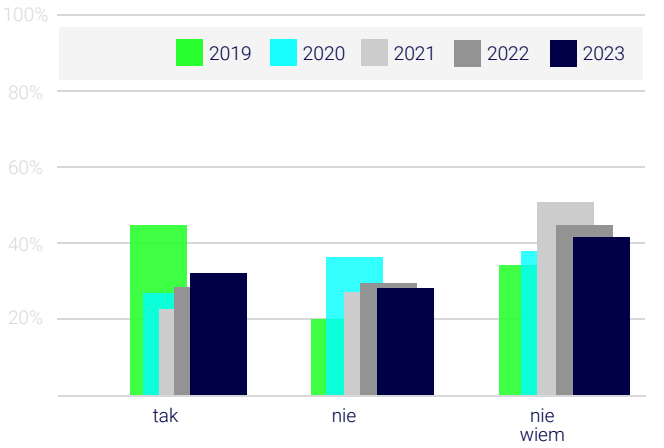
41,3

proc. ankietowanych

nie wie, czy ich firmy monitorują zagrożenia wynikające z cyberprzestępczości



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

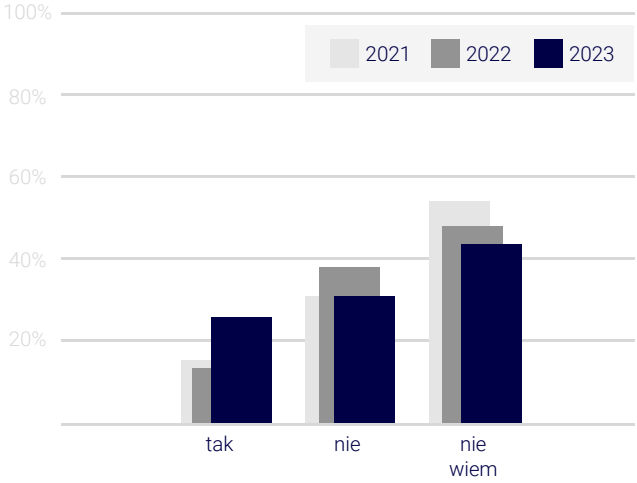


Czy Twoja firma monitoruje zagrożenia wynikające z cyberprzestępczości?

Tylko co czwarta firma wie, jak postępować w chwili ataku

W świetle tych informacji zastanawia również, że aż 41,3 proc. ankietowanych nie wie czy w jakikolwiek sposób ich firmy monitorują zagrożenia wynikające z cyberprzestępczości. Takie działania monitorujące podejmuje jedynie co trzecia pytana firma, ale jednocześnie 27 proc. udzieliła zdecydowanie negatywnej odpowiedzi na to pytanie. Jest zatem nieco lepiej, niż przed rokiem, ale wciąż polskie firmy mają dużo do zrobienia w tym obszarze. Podobny obraz zabezpieczeń rysuje się w rozkładzie odpowiedzi na kolejne pytania. Polskie firmy bowiem równie nieostrożnie podchodzą do scenariuszy postępowania w przypadku wystąpienia incydentu naruszającego bezpieczeństwo danych. Taką procedurę ma przygotowane jedynie 26,4 proc. i choć jest to znacząco lepszy wynik, niż w ubiegłorocznej edycji badania, kiedy istnienie procedur potwierdziło zaledwie 17 proc., ale podkreślmy, że wskazanie potwierdzające opracowanie scenariuszy na wypadek cyberzagrożeń dotyczy zaledwie co 4 badanej firmy. Liczba przeczących odpowiedzi jest podobna do danych z roku ubiegłego - w tym roku to 32,1 proc., czterech na dziesięciu respondentów nie miało wiedzy w zakresie pytania.

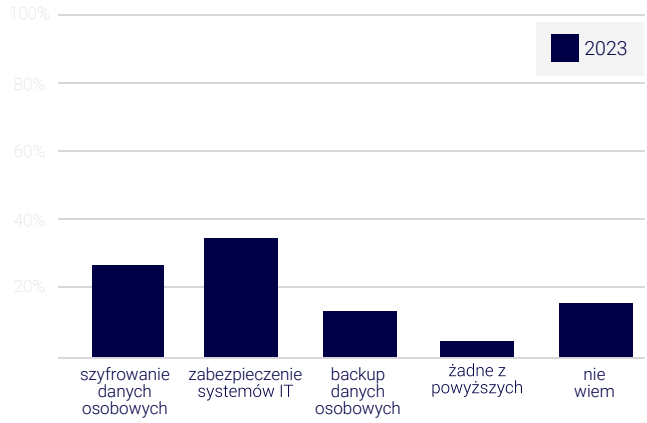
Nieznajomość procedur dotyczących postępowania po naruszeniu integralności danych skłania do wniosku, że w przytłaczającej większości firm takie procedury nie istnieją lub są źle komunikowane pracownikom.



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

RODO

Jest lepiej, ale daleko do ideału



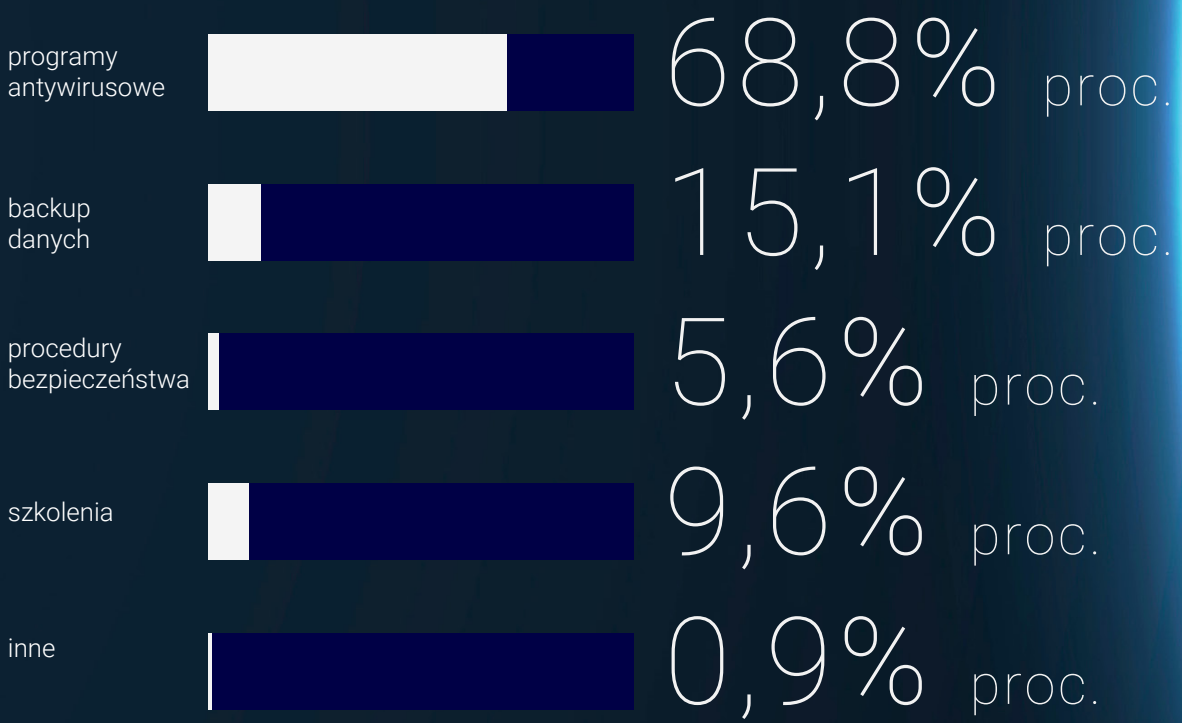
Czy Twoja firma realizuje wytyczne wskazane dyrektywą RODO? Wskaż które.

Bezpieczeństwo danych jest nierozerwalnie powiązane z wytycznymi wskazanymi dyrektywą RODO, czyli mówiąc potocznie z rozporządzeniem o ochronie danych osobowych. Dokument ten zawiera przepisy o ochronie osób fizycznych w związku z przetwarzaniem danych osobowych oraz przepisy o swobodnym przepływie danych osobowych, a naruszenie określonych w nim zasad związanych z ochroną wrażliwych danych np. pracowników i klientów, wiąże się z ryzykiem wysokich kar. Tymczasem z badania wynika, że firmy niespecjalnie rygorystycznie podchodzą do tych zasad, mimo że rozporządzenie obowiązuje od 2018 r. i niejednokrotnie informowano o wysokich karach za jego naruszenie. Tymczasem szyfrowanie danych osobowych stosuje jedynie 26,3 proc. ankietowanych, co oznacza wzrost o 8 proc. w ujęciu rocznym. Z kolei zabezpieczeniami systemów IT na wypadek zewnętrznej, nieuprawionej ingerencji w ich integralność może się pochwalić niecałe 35 proc. Backup i zdolność do szybkiego przywrócenia dostępności danych osobowych i dostępu do nich w razie incydentu fizycznego lub technicznego stosuje więcej firm, niż przed rokiem – 16,1 proc. (wobec jedynie 11 proc. w Raporcie z 2022 r.) 4,2 proc. firm nie stosuje żadnego z powyższych rozwiązań, zaś niemal co piąta nie wie czy są one w ogóle stosowane.

Konserwatywne podejście do zabezpieczeń

W zakresie świadomości istniejących rozwiązań zabezpieczających infrastrukturę IT, respondenci mają dość konserwatywne podejście. Zdaniem 68,8 proc. ankietowanych metodą, która jest najskuteczniejsza w ochronie przed cyberzagrożeniami są programy antywirusowe. Kolejne odpowiedzi są już wskazywane zdecydowanie rzadziej, choć istotny wzrost odnotowano we wskazaniu rozwiązań backupu danych – z 8 proc. w 2022 roku do 15,1 proc. Zważywszy, że dostępne dziś narzędzia backupowe należą do jednych z najskuteczniejszych broni w walce z efektami ataków, również typu ransomware, to istotny i optymistyczny prognostyk na przyszłość. Omawiane wcześniej procedury bezpieczeństwa wskazało 5,6 proc., ważne z punktu widzenia niemal 10 proc. respondentów są również szkolenia z zakresu cyberbezpieczeństwa.

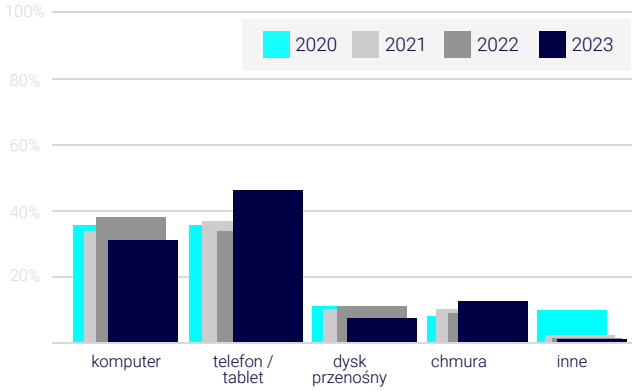
Według respondentów najskuteczniejszą metodą w ochronie przed cyberzagrożeniami jest:



Raport VECTO potwierdza trendy zaobserwowane już w innych publikacjach. NIK opublikował raport z kontroli krajowego systemu cyberbezpieczeństwa – i jego wyniki są bardzo krytyczne. Kontrolerzy NIK wskazują, że lawinowo rośnie liczba e-przestępstw, których ofiarami stają się także zwykli obywatele. Wynika z niego również, że skutki wojny odczuliśmy już w pierwszym jej dniu, 24 lutego 2022 roku, gdy rosyjski atak zakłócił działanie sieci Viasat, oferującej usługi łączności satelitarnej. Zdaniem CERT Polska, nasz kraj był też częstym obiektem ataków typu DDoS.

Jednym z głównych sprawców takich ataków miał być Killnet. - W przeciwieństwie do innych wysoko wykwalifikowanych rosyjskich grup cyberprzestępczych (Sandworm i FancyBear), Killnet nie jest wyspecjalizowaną i dobrze zorganizowaną grupą. Jest częściowo ustrukturyzowana i składa się z mniejszych, mniej znanych grup, które również sympatyzują z Rosją – czytamy w publikacji. CERT aktywność Killnetu wiąże m.in. z atakami na stronę Sądu Najwyższego i Narodowego Banku Polskiego, jednak również na szpitale w mniejszych miejscowościach oraz firmy, jak np: Castorama, mBank czy Orange. - Trudno ustalić, w jaki sposób Killnet i podległe jemu grupy wybierają swoje cele – pisze CERT. Takie sytuacje tym bardziej powinny unaocznić firmom z jaką skalą zagrożenia się mogą zderzyć i faktem, że skutki mogą dotknąć w zasadzie każdej polskiej firmy lub instytucji.

Konserwatyzm i raczej zachowawczość w zakresie podejścia do bezpieczeństwa widać też po tym, w jaki sposób firmy przechowują najcenniejsze dla siebie dane. Pomimo rozwoju technologii i pojawiających się coraz to nowszych narzędzi i rozwiązań, nadal najpopularniejsze są te znane od lat. Jedynie 15,2 proc. uczestniczących w badaniu firm przyznało, że przechowuje najcenniejszych dane w chmurze (wzrost o 5 proc. w skali roku). Za to 31,5 proc. w tym kontekście wymieniło po prostu komputer/laptop. Z 38 proc. do 45 proc. wzrosło zaś wskazanie na telefon lub tablet, co potwierdza, że coraz częściej korzystamy w pracy z urządzeń mobilnych. Dyski przenośnie stosuje jedynie 7,9 proc. ankietowanych.

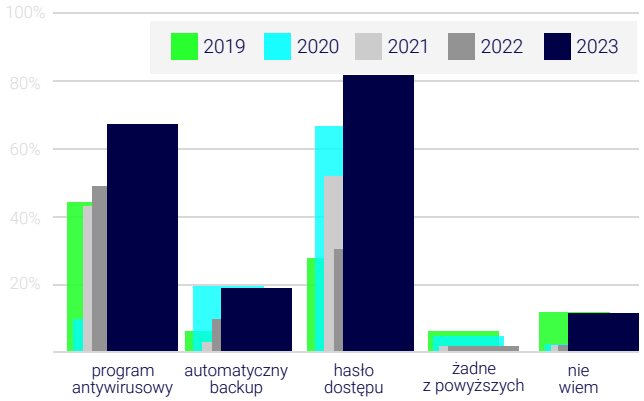


Gdzie przechowujesz najcenniejsze dla siebie dane?

Urządzenia mobilne najsłabszym ogniwem systemu IT?

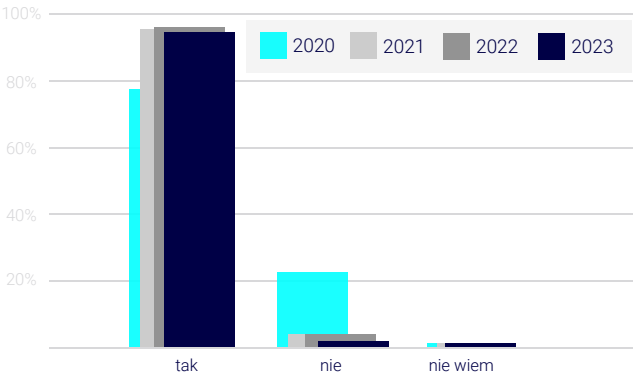
Powszechne korzystanie z urządzeń mobilnych nie przekłada się technologiczny wzrost poziomu zabezpieczeń tego typu sprzętu, na którym zgodnie z poprzednimi odpowiedziami przechowywane są najcenniejsze dane. Solidarnie, 81 proc. respondentów stosuje hasła dostępu, komputery stacjonarne i laptopy częściej zabezpieczamy programami antywirusowymi – 68 proc. vs. 37 proc. urządzenia mobilne – przy czym zapewne użytkownicy nie wiedzą, że wiele obecnie dostępnych na rynku smartfonów ma zainstalowane fabrycznie aplikacje antywirusowe. Ponownie zdecydowanie wyższe wskazanie odnotowały narzędzia backupowe – dla komputerów to wzrost z 7 proc. w 2022 roku do 19 proc. w 2023, dla sprzętu mobilnego z 7 proc. do 20 proc. w analogicznym okresie.

Zarówno doświadczenie inżynierów VECTO, wynikające z analizowania najsłabszych ogniw w infrastrukturze IT, jak i licznych studiów przypadków

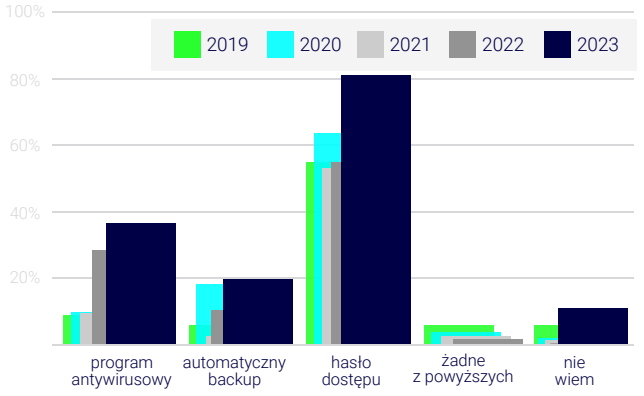


Czy komputer w Twojej firmie jest zabezpieczony (wielokrotny wybór):

skutecznie przeprowadzonych ataków wskazują, że to właśnie urządzenia mobilne są coraz częściej wykorzystywane do forsowania systemów IT. Dostrzegając lukę w zabezpieczeniach, w 2023 roku zorganizowaliśmy liczne szkolenia z zastosowania rozwiązań monitorujących i zabezpieczających ruch w sieci z urządzeń zdalnych. Kilka z nich zrealizowaliśmy również w formule bezpłatnych webinarów z cyklu Vtorki Technologiczne. Zasadność budowania świadomości zagrożeń wynikających z zastosowania sprzętu mobilnego potwierdzają również odpowiedzi na kolejne pytania. Aż 94,4 proc. ankietowanych przyznało, że używa firmowego sprzętu do celów prywatnych. Oznacza to również, że na te urządzenia ściągamy aplikacje służące do rozrywki, technologii IoT, korzystamy z nich do obsługi prywatnej poczty, zakupów czy aktywności w mediach społecznościowych i komunikatorach, a zatem w obszarach, które ze względu na brak czynnika „służbowego" osłabiają naszą powściągliwość w otwieraniu załączników czy niesprawdzonych linków.



Czy używasz firmowego komputera/telefonu do celów prywatnych?



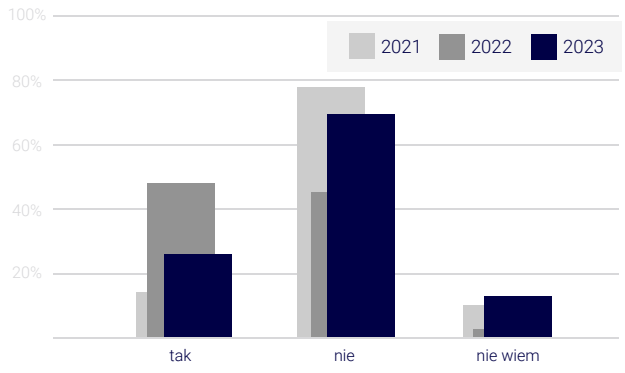
Czy Twój służbowy telefon/tablet jest zabezpieczony (wielokrotny wybór):

Tymczasem, jak donosi CERT Polska, najczęściej zgłaszanym incydentem jest phishing, wykorzystujący inżynierię społeczną, czyli technikę polegającą na wykorzystaniu nieuwagi i podejmowania działań, do których zachęcają cyberprzestępcy. Podszywają się oni m.in. pod firmy kurierskie, urzędy administracji, operatorów telekomunikacyjnych, popularne sklepy internetowe czy nawet znajomych ofiary, starając się wyłudzić jej dane do logowania, np. do kont bankowych, kont w mediach społecznościowych czy systemów biznesowych. Takich incydentów CERT Polska w ubiegłym roku odnotował aż 25 625, co stanowi 64 proc. wszystkich zdarzeń obsłużonych w 2022 r. przez tę instytucję. W tej kategorii najczęściej zgłaszano oszustwa z wykorzystywaniem wizerunku takich firm jak InPost, Facebook czy Vinted – nawet po kilka tysięcy w każdym przypadku.

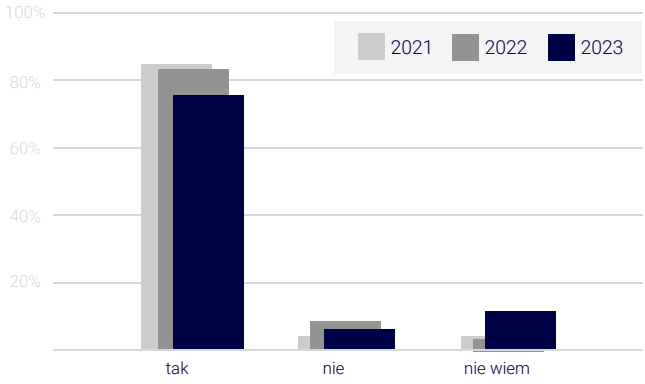
Zdalnie i niebezpiecznie

Nowe modele pracy zdalnej, które na stałe wpisały się w popandemiczny krajobraz systemów zatrudnienia, w opinii zdecydowanej większości firm (84,3 proc.) wprost przekładają się na wzrost potencjalnych cyberzagrożeń. Nieco mniej, niż w roku ubiegłym, bo 77,5 proc. respondentów przyznaje, że praca zdalna wpływa bezpośrednio na konieczność inwestowania w rozwiązania IT, ale tylko co czwarta firma wprowadziła z tego tytułu dodatkowe zabezpieczenia, choć i tak liczba ta jest ponad 2 razy większa, niż w roku 2022.

Praca zdalna, Twoim zdaniem:



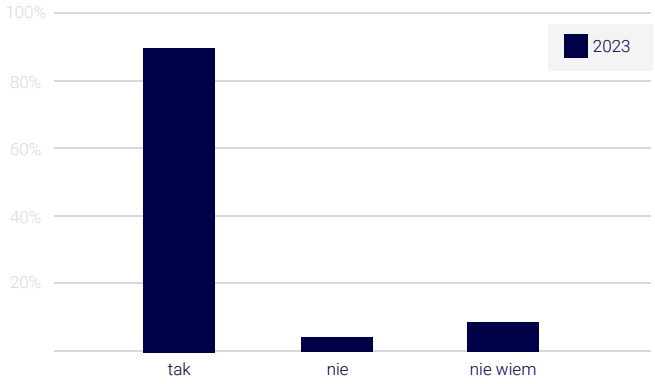
Czy Twoja firma wprowadziła dodatkowe zabezpieczenia dla pracowników pracujących zdalnie?



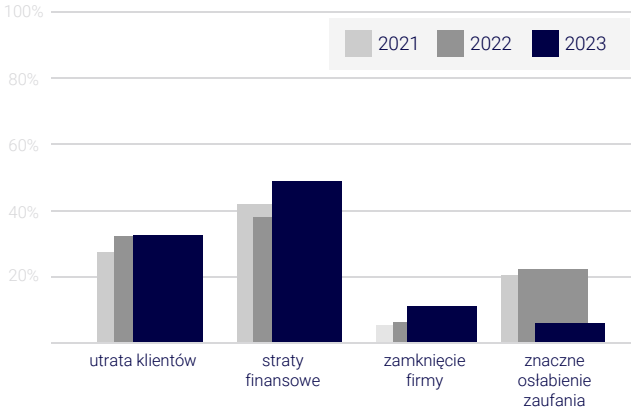
Czy praca zdalna, Twoim zdaniem, wpłynęła bezpośrednio na konieczność inwestowania w rozwiązania IT w Twojej firmie?

Polskie firmy obawiają się cyberataków

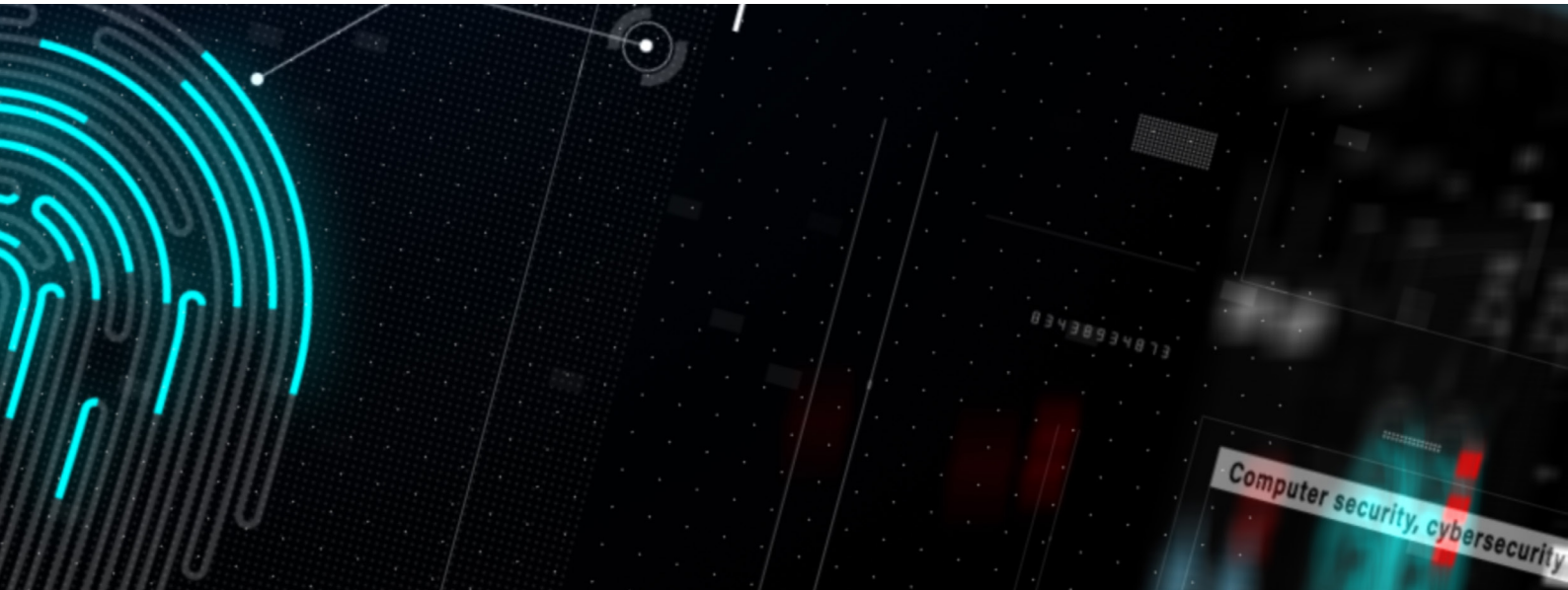
87 proc. polskich firm, a zatem o niemal 8 proc. więcej niż w poprzedniej edycji badania, deklaruje, że w ich ocenie atak cyberprzestępców na system informatyczny może wpłynąć na funkcjonowanie firmy. Potencjalnie najdotkliwszym skutkiem cyberincydentu w opinii respondentów badania są potencjalne straty finansowe (48,4 proc.) Co trzecia firma szczególnie obawia się utraty klientów, a niemal 12 proc. wskazuje niebezpieczeństwo zamknięcia/likwidacji firmy. Zdecydowany spadek odnotowaliśmy we wyborze odpowiedzi dotyczącej znacznego osłbienia wizerunku i zaufania w efekcie skutecznego ataku. Widmo zaszkodzenia reputacji przedsiębiorstwa wskazało 7 proc., co w porównaniu do 20 proc. w danych za 2022 rok może dowodzić, że zaczynamy dostrzegać coraz większą skalę zjawiska cyberprzestępczości, a w kontekście dotychczasowych doświadczeń polskich firm dotkniętych atakami, dotkliwsze mogą okazać się skutki bezpośrednio przekładające się na bieżącą działalność biznesową. Warto tu wspomnieć m.in. case polskiego producenta gier komputerowych CD Projekt Red, którego akcje giełdowe poszybowały w dół po wycieku całych kodów źródłowych gier tworzonych przez studio, notując – dodajmy - jeden z najbardziej spektakularnych spadków cen akcji największych spółek WIG20 warszawskiej Giełdy Papierów Wartościowych.



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



Wskaż potencjalnie najdotkliwszy skutek ewentualnego ataku cyberprzestępców na system IT oraz dane Twojej firmy:



Czy Twoja firma realizuje wytyczne wskazane dyrektywą RODO?

26,3 proc.

stosuje szyfrowanie danych osobowych

35 proc.

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

16,1 proc.

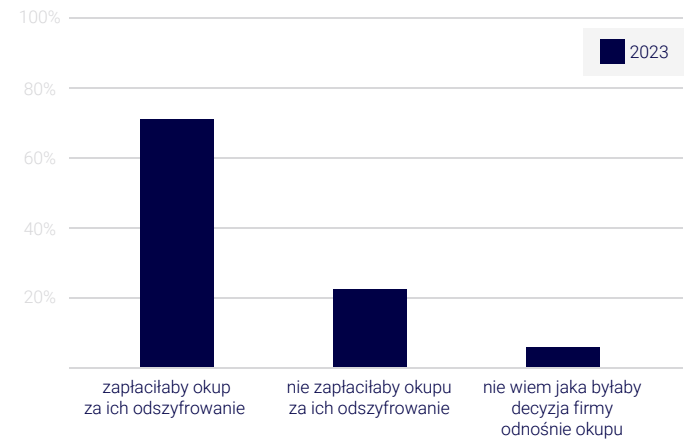
przeprowadza backup i zdolność do szybkiego przywrócenia dostępności danych osobowych i dostępu do nich w razie incydentu fizycznego lub technicznego

RANSOMWARE

Ponad 70 proc. firm rozważa płacenie okupu

O przykładach skutecznie przeprowadzonych ataków typu ransomware, DDoS, a także wyciekach, przejęciu i publikacji całych baz danych w 2023 roku media informowały zdecydowanie częściej, niż w roku poprzednim. Tym bardziej, że do licznego grona polskich firm dotkniętych cyberatakami, dołączyły instytucje publiczne i jednostki samorządu terytorialnego. Te ostatnie, często niedofinansowane stawały się łatwym celem dla przestępców, a wykradzione informacje, obejmujące dane wrażliwe mieszkańców cennym towarem. Jednak oprócz mniejszych ośrodków administracyjnych – powiatowych i gminnych, hakerzy dokonywali ataków na urzędy Ministerialne, jak choćby Ministerstwo Cyfryzacji (system ePUAP), Urzędy Miasta w Poznaniu i Olsztynie, Polski Fundusz Rozwoju czy śląski system Śląskiej Karty Usług Publicznych. W części z nich, ataki oparte na ransomware, prowadziły do całkowitego paraliżu pracy, a odmowa opłacenia okupu za odszyfrowanie danych skutkowała koniecznością ich żmudnego odtwarzania.

Po skutecznie przeprowadzonym ataku typu ransomware, skutkującym zaszyfrowaniem wszystkich danych, Twoja firma?

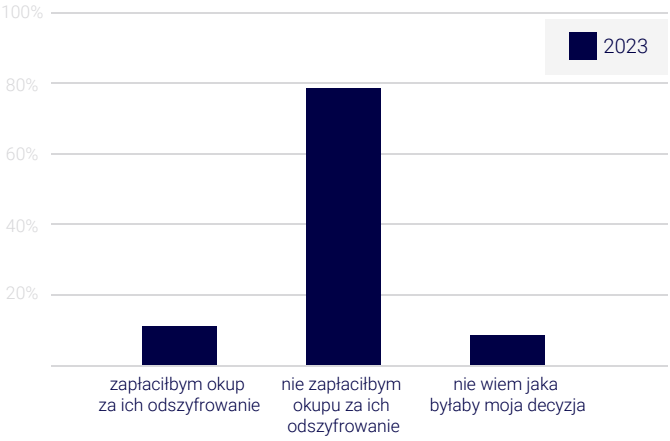


Zważywszy na rosnącą liczbę ataków ransomware w Polsce, po raz pierwszy w historii naszego badania zapytaliśmy respondentów o kwestię ich gotowości do spełniania żądań cyberprzestępców. Aż 72,2 proc. uczestników badania przyznało, że zapłaciłoby okup za ich odszyfrowanie – przeciwnego zdania jest zaledwie co piąty pytany. Powyższe wpisuje się w globalny trend, wskazujący, że firmy, choć rzadko się do tego przyznają, najczęściej współpracują z hakerami i płacą za odszyfrowanie dostępu do danych. Ponadto, najczęściej starają się zachować w tajemnicy fakt wystąpienia ataku, bowiem może być on odebrany jako przyznanie się do porażki firmowych zabezpieczeń i słabych kompetencji zespołu odpowiedzialnego za ochronę danych. Nie bez znaczenia jest również fakt, że ransomware krytycznie wpływa na ciągłość procesów w firmie, szczególnie, gdy stopień jej digitalizacji jest zaawansowany i w dużej mierze oparty na cyfrowych bazach danych. Z doświadczenia VECTO wynika również, że niestety dopiero po zapłaceniu okupu, zaatakowane firmy i instytucje na poważnie zaczynają dbać o kwestie należytego zabezpieczenia infrastruktury IT.

Procederowi płacenia okupów sprzeciwia się społeczność międzynarodowa. Na przełomie października i listopada 2023 r. koalicja 48 państw pod przewodnictwem Stanów Zjednoczonych, a także państw Unii Europejskiej oraz Interpolu zapowiedziała intensyfikację działań, których celem jest ograniczenie skali płacenia okupów po ataku ransomware. Według obserwatorów i ekspertów to wyraz determinacji po fali spektakularnych incydentów, które w ostatnich miesiącach dotknęły firmy i instytucje na całym świecie. Zgodna odmowa płacenia haraczy może zmniejszyć motywację hakerów, a także ograniczyć dystrybucję złośliwego oprogramowania.

Zobowiązanie to podjęto na niedawnym spotkaniu Międzynarodowej Inicjatywy ds. Zwalczania Ransomware, podczas którego kraje połączyły siły, aby utworzyć zjednoczony front przeciwko grupom przestępczym stojącym za atakami oprogramowania ransomware.

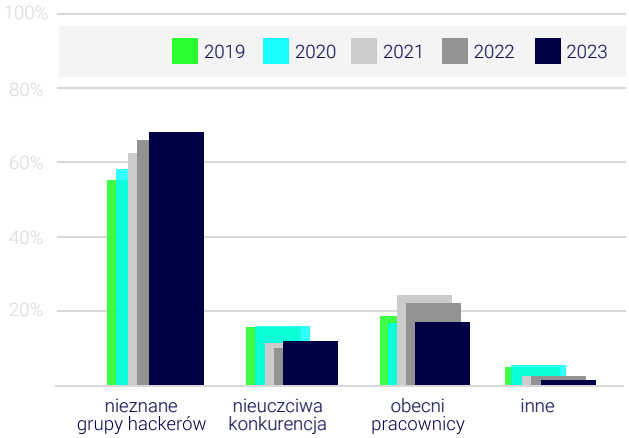
W chwili zamykania niniejszego Raportu (koniec listopada 2023 r.), jedno z największych centrów diagnostyki medycznej w Polsce, spółka ALAB, poinformowała o skutecznie przeprowadzonym ataku ransmoware na infrastrukturę IT, który



Czy gdyby atak ransomware dotyczyłby wyłącznie Twoich danych prywatnych:

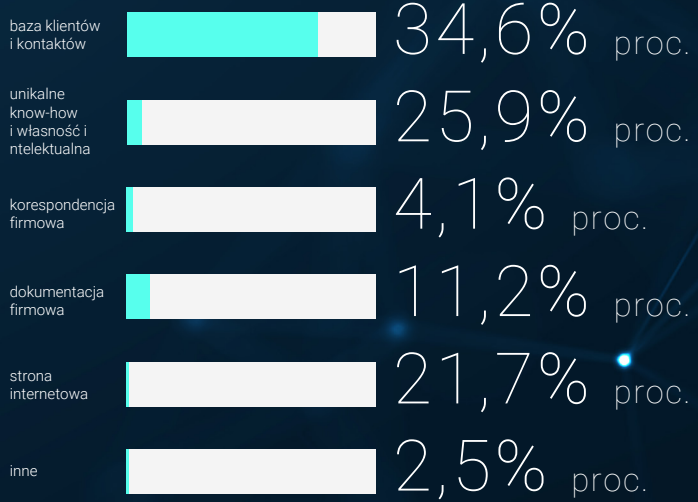
doprowadził do wycieku obejmującego niemal ćwierć TB danych z wynikami badań pacjentów, a także m.in. ich nazwiskami oraz adresami zamieszkania. Część wykradzionej bazy, uwzględniająca informacje wrażliwe pacjentów z Warszawy, Łodzi i podwarszawskich Łomianek już została opublikowana, co może świadczyć o odmowie zapłacenia okupu przez ALAB. O skali tego wycieku niech świadczy fakt, że autorzy ataku, hakerzy grupy RA World, udostępnili wycinek przejętej bazy, który obejmuje „zaledwie" 50 tys. rekordów z danymi pacjentów, dla których wykonywano badania w latach 2017-2023. Co istotne, baza obejmuje również informacje wrażliwe osób, które nie korzystały bezpośrednio z usług ALAB, gdyż w centrach diagnostycznych tej firmy analizowano próbki na zlecenie zewnętrznych partnerów, jak choćby pacjentów placówek prywatnej służby zdrowia, np. Medicover, z którego usług korzysta obecnie ok. 800 tys. osób. Powagę tego incydentu podkreśla również fakt, że Ministerstwo Cyfryzacji uruchomiło specjalne narzędzie do weryfikacji (poprzez Profil Zaufany), czy konkretne dane znalazły się w publikowanych przez przestępców bazach.

O ile w kontekście danych firmowych, respondenci w zdecydowanej większości gotowi są zapłacić okup za ich odzyskanie, to perspektywa diametralnie się zmienia, gdy pytamy o dane prywatne. Tylko 13,5 proc. badanych zapłaciłoby haracz za ich odszyfrowanie - 78,8 proc. deklaruje brak gotowości do pertraktowania z przestępcami. Musimy mieć jednak świadomość, że atak ransomware pozwala na przejęcie wszystkich danych na zaatakowanym nośniku, w tym zdjęć i prywatnych filmów oraz innych materiałów, które mogą posłużyć do dyskredytacji ofiary, a w przypadku osób publicznych, również szantażu i prób zmuszania do określonego zachowania (np. osób decyzyjnych, notabli, celebrytów). W przypadku statystycznego Kowalskiego zapewne utrata danych nie ma aż tak dużego znaczenia, choć oczywiście przejęcie prywatnej korespondencji, haseł dostępowych do kont bankowych, a nawet archiwum rodzinnych zdjęć może być bolesna.



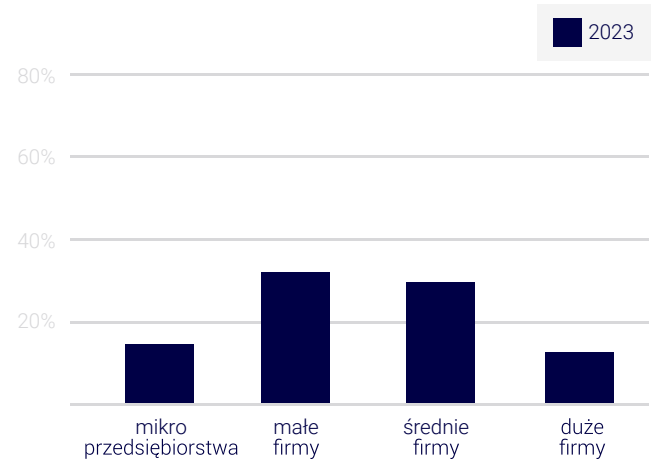
Wskaż główne, Twoim zdaniem, źródła cyberzagrożeń dla Twojej firmy:

Wskaż obszar, w którym Twoja firma najbardziej obawia się cyberataku:



Kto stoi za atakami według respondentów?

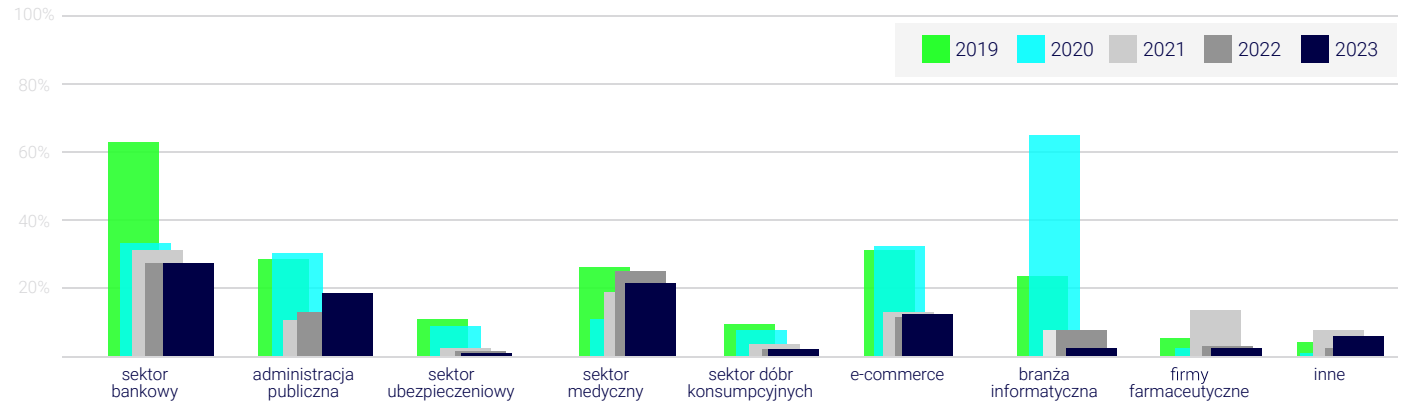
Niezmiennie, większość respondentów badania, jako główne źródło cyberzagrożeń wskazuje nieznane grupy hakerów - 67,9 proc., ale warto zauważyć, że odsetek ten wzrósł o niecałe 7 proc. w skali roku. 12 na 100 ankietowanych uważa, że za cyberincydentami stać może nieuczciwa konkurencja, a niemal co piąty twierdzi, że obecni pracownicy. W kontekście wystąpienia cyberataku, zdecydowanie najwięcej badanych firm obawia się utraty bazy klientów i kontaktów (34,6 proc.), unikalnego know-how i własności intelektualnej (25,9 proc.), a także utraty kontroli nad stroną internetową (21,7 proc.). Rzadziej martwimy się o korespondencję firmową czy dokumentację (kolejno 11,2 proc. oraz 4,1 proc.). Możemy zatem wnioskować, że wiele z badanych firm identyfikuje swoje mocne strony w konkurencyjności, przede wszystkim opartej na wypracowanych relacjach z otoczeniem biznesowym, unikalności produktów i usług, kompetencjach pracowników, własnych technologiach czy patentach. Obawiamy się również efektów ataku na stronę internetową, co jest z pewnością związane z faktem, że coraz częściej jest to podstawowy kanał dotarcia do klientów i kontrahentów.



Jakie firmy są Twoim zdaniem szczególnie narażone na utratę danych?

Zagrożone branże

Zmiany w porównaniu z badaniem z ubiegłego roku obserwujemy również w kontekście oceny respondentów branż, które są szczególnie narażone na działania cyberprzestępców. O ile wciąż uważamy, że widomo ataku hakerskiego to codzienność dla podmiotów sektora finansowego i bankowego (25,5 proc.) oraz sektor usług medycznych (20,7 proc.), to na trzecie miejsce awansowała administracja publiczna, która zanotowała wzrost wskazań z 7 proc. w 2022 roku do 18,1 proc. w tegorocznym badaniu. Na kolejnych lokatach uplasowały się: e-commerce (15,8 proc.), branża informatyczna (3,9 proc.), firmy farmaceutyczne (spadek z 10 proc. do 3,1 proc.). Kategorię „inne" wskazało 7,2 proc. badanych.



Wskaż branżę, która Twoim zdaniem jest szczególnie narażona na działania cyberprzestępców:

PODSUMOWANIE

Cyberprzestępczość i jej skutki stały się codziennym doświadczeniem tysięcy polskich firm i milionów użytkowników internetu. Skala szkód generowanych szkodliwym oprogramowaniem, wycieków i utraty kontroli nad danymi dynamicznie wzrasta i staje się realnym wyzwaniem zarówno dla polskiego biznesu, jak i władz państwowych, które coraz częściej aktywnie włączają się w ochronę przestrzeni cyfrowej podejmując inicjatywy legislacyjne i wzmacniając kampanie, których celem jest zwiększenie świadomości zagrożeń. Wiele dzieje się również w kontekście regulacji Unii Europejskiej, która sukcesywnie realizuje opublikowany przez Komisję Europejską w 2022 roku pięciopunktowy plan na rzecz ochrony infrastruktury krytycznej w priorytetowych obszarach: gotowości, reagowania i współpracy międzynarodowej. Plan priorytetowo traktuje kluczowe sektory energii, infrastruktury cyfrowej, transportu i przestrzeni kosmicznej. Międzynarodowa współpraca kreśli również ramy stworzenia europejskiej cybertarczy, o której już w kwietniu 2023 roku informował Komisarz UE ds. rynku wewnętrznego. Za jej skuteczność odpowiedzialnych będzie siedem centrów operacyjnych cyberbezpieczeństwa (SOC) – poinformował Breton. Nowe regulacje obejmują również partnerstwo między państwami członkowskimi w celu wzmocnienia odporności infrastruktury krytycznej w Unii Europejskiej, w tym lotnisk, elektrowni, gazociągów czy sieci elektroenergetycznych. Bez wątpienia to właściwy kierunek, biznes nie może być osamotniony w walce z cyberprzestępczością, a regulacje prawne muszą być nowelizowane wraz z pojawianiem się nowych metod dokonywania ataków, a te ostatnie skutecznie wykrywane i sankcjonowane surowymi karami.

Według różnych szacunków, codziennie powstaje ponad 316 tysięcy wariantów złośliwego oprogramowania. Już w 2022 roku przeciętny okup za odszyfrowanie danych kosztował polskie przedsiębiorstwa średnio 670 tys. zł., co często stanowi kwotę wielokrotnie wyższą, niż inwestycje w skuteczne rozwiązania chroniące firmową infrastrukturę IT. Podkreślić należy, że mówimy o uśrednionych kosztach ataków, wiemy bowiem o przypadkach strat liczonych w dziesiątkach milionów złotych.

Zdaniem ekspertów i obserwatorów rynku cyberbezpieczeństwa kolejne lata przyniosą dalsze wzrosty zagrożeń. Postępująca digitalizacja w każdym wymiarze biznesu i codziennego życia społeczeństw na całym świecie, które jak nigdy dotąd doświadczają zalet i wad niesionych pojęciem globalnej wioski, rozwijająca się technologia IoT, a nawet rozpalająca opinię publiczną dyskusja o przyszłości sztucznej inteligencji stanowić będą podatny grunt dla kreatywności i zwiększania skuteczności działań cyberprzestępców. To dość pesymistyczna perspektywa, którą wszyscy powinniśmy uwzględniać w definiowaniu najważniejszych wyzwań dla polskich przedsiębiorstw i instytucji w nadchodzących latach.

Analiza tegorocznych wyników badania VECTO wskazuje jednak, że świadomość zagrożeń rośnie. Nie możemy jednak zapominać, że w dużej mierze jest to nauka na błędach niemal 70 proc. polskich przedsiębiorstw, które potwierdziły wystąpienie ataków naruszających bezpieczeństwo i integralność danych. Dziś żadna firma, podmiot, instytucja, żaden indywidualny użytkownik sieci internetowej nie powinien zadawać sobie pytania czy jego infrastruktura IT zostanie zaatakowana. Właściwe pytanie brzmi bowiem: kiedy to nastąpi. Warto zatem wykorzystać czas, by się do tego doświadczenia stosownie przygotować. Tym bardziej, że innowacyjnych, skutecznych rozwiązań, a również ekspertów dysponujących odpowiednimi kompetencjami do ich wdrożenia na polskim rynku nie brakuje.

METODOLOGIA

Badanie zostało przeprowadzone w formie ankiety internetowej, telefonicznej i papierowej od czerwca do grudnia 2023 roku na próbie 380 przedsiębiorstw i instytucji, działających w 2023 roku na polskim rynku.

Największą grupę respondentów stanowili przedstawiciele branży finansów i bankowości (16,8 proc), instytucji rządowych i samorządowych (12,3 proc.) oraz osoby związane z branżą medyczną (12,3 proc.). Wśród uczestników ankiety dominowali przedstawiciele podmiotów zatrudniających powyżej 250 osób – 37,5 proc. Na drugim miejscu znalazły się przedsiębiorstwa i instytucje zatrudniające od 50-250 osób (22,6 proc.). 21,7 proc. ankietowanych zatrudnionych jest w firmie lub instytucji, której poziom zatrudnienia wynosi od 5-50 osób.

Przedstawiciele najmniejszych podmiotów (zatrudnienie do 5 osób) stanowili 18,2 proc. ogółu badanych

Reprezentowana branża	
budownictwo / architektura / wykończenie wnętrz	2,9 proc.
edukacja / badania naukowe	3,1 proc.
finanse / bankowość	16,8 proc.
hotelarstwo / turystyka / rekreacja / sport	6,3 proc.
handel hurtowy i detaliczny	5,1 proc.
instytucje rządowe i samorządowe	12,3 proc.
łączność / telekomunikacja	3,8 proc.
media / kultura i sztuka / rozrywka	3,1 proc.
medycyna / ochrona zdrowia	12,3 proc.
produkcja / dystrybucja / logistyka	3,8 proc.
przemysł komputerowy / oprogramowanie	11,4 proc.
przemysł komputerowy / sprzęt	5,2 proc.
usługi dla firm / usługi dla klientów indywidualnych	7,3 proc.
usługi internetowe	4,1 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.linkedin.com/company/vectospzoo/


VECTO.PL