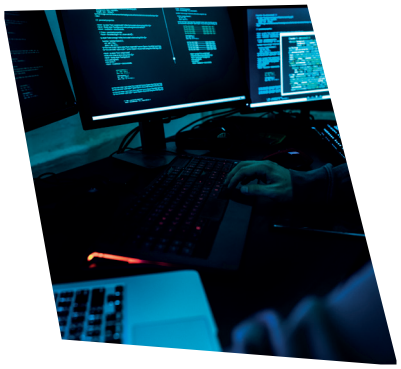
CYBERBEZPIECZEŃSTWO POLSKICH FIRM 2018

VECTO



WSTĘP

Cyberbezpieczeństwo w świetle mocno nagłaśnianych przypadków ataków hakerskich, staje się jednym z priorytetów dla polskich przedsiębiorstw. Chodzi nie tylko o zabezpieczenie wewnętrznych zasobów danych i baz klientów, ale również o ich zaufanie.

Wszyscy zdajemy sobie sprawę z tego, że zagrożenia ze strony grup hakerskich narastają. Według szacunkowych danych w 2017 r. ok. 80% polskich przedsiębiorstw odnotowało przynajmniej jeden cyberincydent. Co trzecia firma zaobserwowała wzrost liczby cyberataków w przeciągu ostatniego roku. Pomimo rosnącej skali tego typu zjawisk, zaledwie tylko co 10 firma o rocznych przychodach przekraczających 50 mln zł, zatrudnia dedykowanego eksperta ds. bezpieczeństwa informacji. Czy zatem nie jest tak, że rozumiemy cyberzagrożenia, ale niespecjalnie inwestujemy w profilaktykę i rozwiązania zwiększające bezpieczeństwo systemów informatycznych?

Postanowiliśmy poświęcić niniejszy raport temu zjawisku. W 2017 roku przeprowadziliśmy badanie polskich firm z różnych branż. Jego celem było zdiagnozowanie świadomości zagrożeń, poznanie stopnia przygotowania przedsiębiorstw na wyzwania związane z bezpieczeństwem danych, a także gotowość na realizację wyzwań, jakie stawia przed polskim biznesem ogromna aktywność i skala działań cyberprzestępców.

W skali globalnej świadomość zagrożeń również rośnie, przy czym jest ona na bardziej zaawansowanym poziomie. Coraz więcej firm aktywnie stara się zabezpieczać swoje systemy informatyczne, a ewentualne ataki rzadko pozostają niezauważone. Skuteczne przeciwdziałanie cyberprzestępstwom zależne jest od procesu wykrywania tego typu zdarzeń, analizowania luk i słabych ogniw systemów, które zostały wykorzystane w przestępstwie, a następnie śledzenie lub ściganie sprawców. Tymczasem, jak wynika z raportu CISCO[1], 44% prób cyberataków pozostaje zupełnie niezbadanych. Przestępcom uchodzi na sucho proceder, wskutek którego w 2017 roku 22% firm straciło klientów, a 29% odczuło stratę przychodów.

Dziś wiemy, że co godzinę dochodzi na świecie do ok. 1000 cyberataków. Skala tego zjawiska rośnie w zastraszającym tempie i wszystko wskazuje na to, że w najbliższej przyszłości również polskie firmy będą musiały zmagać się z konsekwencjami wzrostu aktywności cyberprzestępców. Mamy nadzieję, że niniejszy raport zainspiruje rodzime firmy do skrupulatnej oceny stosowanych przez nie rozwiązań z zakresu cyberbezpieczeństwa, ochrony danych oraz całej struktury informatycznej.

Jakub Wychowański
Sales Manager/członek zarządu
VECTO Sp. z o.o.

54,5%

polskich firm zetknęło się z cyberatakiem

85%

badanych uważa, że zabezpieczanie danych informatycznych w firmie jest ważne

38%

badanych uważa poziom zabezpieczenia sieci w swojej firmie za niewystarczający

61,1%

polskich firm nie korzysta z usług specjalistów od bezpieczeństwa

VECTO

RANSOMWARE ZBIERA ŻNIWO

Wannacry jest dziś synonimem skali i rozmachu działań cyberprzestępców.

Szkodliwe oprogramowanie typu ransomware zebrało żniwo. W maju 2017 roku hakerzy posługujący się 28 językami zainfekowali ponad 300 tys. komputerów w 99 krajach. Blokowali dostęp do plików i danych, żądając zapłaty za odblokowanie. Zaatakowanych zostało wiele firm i osób prywatnych, m.in. w Hiszpanii w ataku ucierpiała firma telekomunikacyjna Telefónica S.A., na świecie zaś FedEx i Deutsche Bahn. W Rosji zainfekowano ponad tysiąc komputerów w ministerstwie spraw wewnętrznych.

Pod koniec czerwca zaatakował z kolei wirus NotPetya, w związku z którym ówczesna premier Beata Szydło powołała nawet specjalny Rządowy Zespół Zarządzania Kryzysowego. Na skrzynkach e-mailowych pojawiło się mnóstwo informacji z podejrzanym oprogramowaniem. Zawierały one złośliwy załącznik, po otwarciu którego rozpoczynało się szyfrowanie komputera odbiorcy, ale nie tylko. Wirus próbował również dotrzeć do wszystkich innych komputerów podłączonych do tej samej sieci. Dlatego w niektórych placówkach, zwłaszcza bankowych, dzień ataku wirusa został ogłoszony dniem wolnym od pracy, aby na bieżąco wyspecjalizowane służby mogły sprawdzić wszystkie elementy firmowych sieci.

Serwis niebezpiecznik.pl podawał wówczas, że atak dotknął wiele dużych i znanych firm jak Raben, InterCars, kilka kancelarii prawnych, TNT w Katowicach, Kronospan czy Mondelez we Wrocławiu.

HAKERZY WCIĄŻ SPRYTNIEJSI...

Dotychczasowe doświadczenia są okazją do nauki, ale niestety hakerzy wciąż zaskakują coraz to nowymi metodami wyłudzania środków finansowych, lub niszczeniem nośników przez zainfekowane pliki.

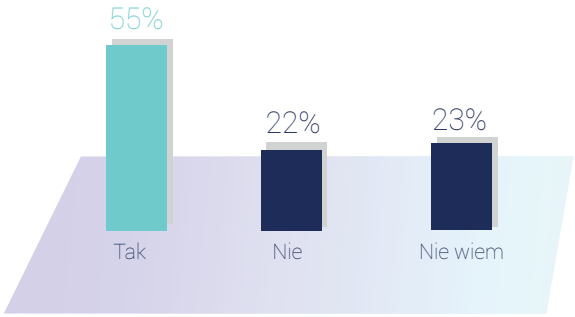
Firma Trend Micro podaje w raporcie[2], że metody działań hakerów bezustannie ewoluują. Jedną z najdłużej znanych taktyk stosowanych przez hakerów jest modyfikowanie stron internetowych, tj. wprowadzanie w serwisach internetowych zmian niekorzystnych lub szkodliwych dla ich właścicieli. Inne metody to podszywanie się pod oficjalną korespondencję z klientami czy kontrahentami w celu zdobycia wrażliwych danych. Mogą one służyć następnie do wyłudzenia z firmy środków finansowych.

Tę przestępczą koniunkturę dodatkowo potęgują konflikty polityczne czy dramatyczne wydarzenia, które wstrząsają światową opinią publiczną. Przykładem jest fala ataków na strony WWW po zamachu terrorystycznym na redakcję Charlie Hebdo czy zniszczenie syryjskiego miasta Aleppo. Nie są one powiązane z próbami wyłudzeń, a wyłącznie z nagłośnieniem danej sprawy. Takie ataki są szczególnie niebezpieczne, ponieważ skala rażenia jest naprawdę wysoka, a zainfekowane pliki rozpowszechniane są bez żadnego systemu i schematu. Jednak hakerzy często rozpoczynając działalność od spraw z zabarwieniem ideowym, szybko przechodzą do wydobywania z nich pieniędzy co jest jeszcze bardziej niebezpieczne.

POLSKI INTERNET ZAGROŻONY?

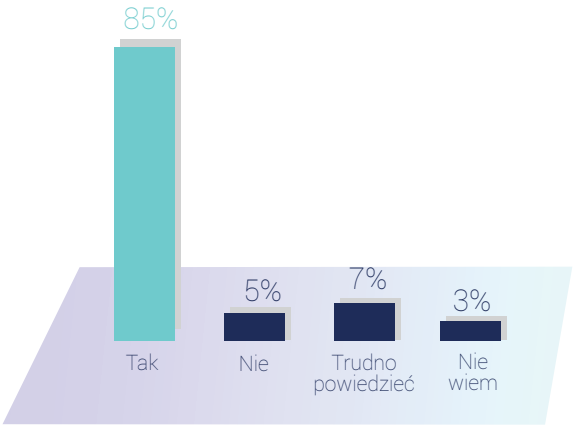
Czy zjawisko cyberprzestępstw występuje w takim natężeniu również w Polsce?

Okazuje się, że choć może nie mamy swoich przedstawicieli wśród 500 najbardziej innowacyjnych technologicznie firm świata, to polskie firmy zdecydowanie są celem do nadużyć. Badanie VECTO wskazuje, że skala zjawiska jest duża. Na pytanie czy firma kiedykolwiek zetknęła się z cyberatakiem, twierdząco odpowiedziało ponad 54,5% ankietowanych. Przeciwnego zdania było z kolei niemal co czwarte przedsiębiorstwo. Różnice w stosunku do innych badań można łatwo wytłumaczyć rozmaitymi interpretacjami tego, co można uznać za atak hakerski. Często ankietowani przeceniają ich liczbę uznając właśnie hakerów za przyczynę wszelkich kłopotów technicznych w firmie, prowadzących do wyłączenia całych systemów informatycznych.



Czy Twoja firma zetknęła się kiedykolwiek z cyberatakiem?

ŚWIADOMOŚĆ ZAGROŻEŃ ROŚNIE

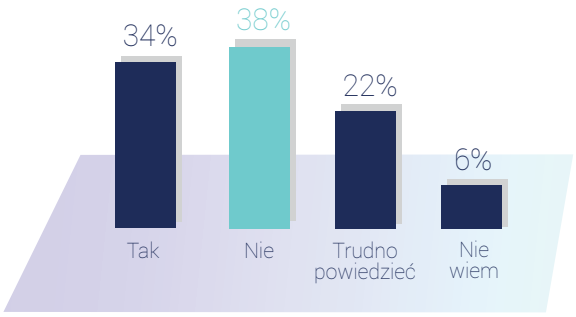


Czy uważasz, że zabezpieczanie danych informatycznych w firmie jest ważne?

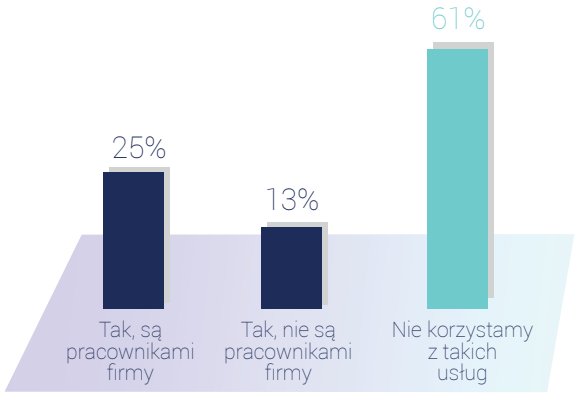
Na poziomie ogólnym polskie firmy wydają się być świadome dzisiejszych cyberzagrożeń, a zdaniem niemal 85% badanych kwestia zabezpieczania firmowych danych jest bardzo istotna. Jedynie 5,6% było przeciwnego zdania, a pozostali nie wiedzieli, bądź nie byli w stanie wskazać żadnej odpowiedzi.

Kwestie oceny poziomu zabezpieczeń firmowych sieci są bardziej pesymistyczne. Tylko 36% ankietowanych przedstawicieli firm uznało, że w ich przedsiębiorstwach sieć jest prawidłowo zabezpieczona. Niestety 38% jest przeciwnego zdania, a niemal co trzecia osoba nie wiedziała bądź wskazała odpowiedź „trudno powiedzieć". Jest to dość mocno niepokojąca perspektywa, biorąc pod uwagę fakt, iż analitycy spodziewają się dalszego wzrostu poziomu zagrożeń w zakresie ataków na firmowe sieci.

Skala przygotowań polskich przedsiębiorstw jest na bardzo wstępnym etapie, co pokazują również odpowiedzi przedstawicieli na kolejne pytania. Analiza VECTO potwierdza problem sygnalizowany już w raporcie KPMG odnośnie zatrudniania ekspertów zajmujących się wyłącznie kwestiami ochrony danych w firmach. Spośród ankietowanych, tylko co czwarta firma przyznała, iż zdecydowała się na taki krok, zaprzeczyło temu zdecydowanie 13,3% badanych. Największa grupa aż 61,1% ankietowanych nie miała zdania bądź nie wiedziała.



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



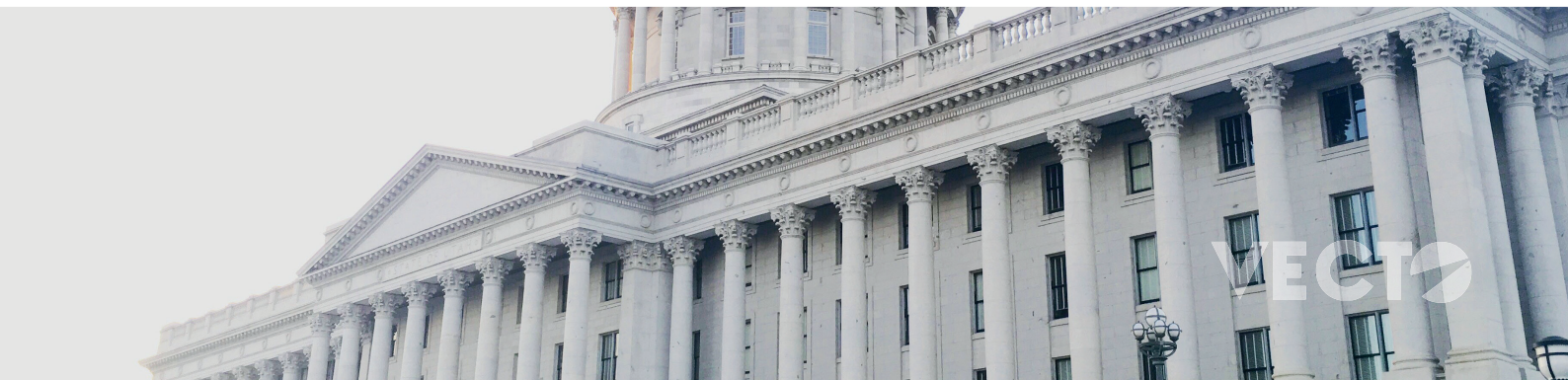
Czy Twoja firma zatrudnia specjalistę od bezpieczeństwa danych w firmie?

Tymczasem warto zwrócić uwagę, że poprawa bezpieczeństwa firmowych zasobów informatycznych nie jest ściśle związana z kosztownymi inwestycjami. Należy jednak uważnie przeanalizować stosowane w firmie procedury oraz rozsądnie zarządzać ryzykiem informatycznym. Dobrym rozwiązaniem jest przeprowadzenie audytu przez wyspecjalizowaną firmę, dzięki któremu precyzyjnie określimy słabe ogniwa systemu, luki lub furtki, poprzez które przestępcy z łatwością włamują się do struktury IT. Racjonalnym rozwiązaniem jest wdrożenie narzędzi automatycznego backupu, segmentacji sieci wewnętrznej, czy hartowanie systemów.

WOJNY „NA GÓRZE" MAJĄ WPŁYW NA BEZPIECZEŃSTWO SYSTEMÓW IT

Zagrożeń będzie przybywało, ponieważ hakerzy są często wykorzystywani jako narzędzie w walce politycznej.

Co więcej, niektóre rządy znane są z traktowania takich metod jako normalnych w swojej działalności. Najlepszym przykładem jest Korea Północna, regularnie stająca za atakami na zachodnie instytucje. Przekonał się o tym koncern Sony, produkujący prześmiewczy film o dyktatorze tego państwa. Ponieważ Sony nie chciało wycofać się z dystrybucji filmu „The Interview", hakerzy wykradli z baz firmy 100 terabajtów danych, wśród których znalazły się m.in. informacje o pracownikach i ich numerach ubezpieczeń społecznych oraz szczegóły kontraktów z aktorami i twórcami filmowymi. Po ich upublicznieniu wybuchł skandal, osoby z najwyższych szczebli managementu firmy podały się do dymisji. Korea Północna oficjalnie nie przyznała się do ataku i konsekwentnie unika odpowiedzialności. Podobnie było, gdy FBI oficjalnie potwierdziło identyfikację koreańskie próby złamania amerykańskich zabezpieczeń. Zarzuty o korzystanie z pomocy hakerów dla realizowania celów politycznych czy biznesowych padały też regularnie pod adresem rządu Chin, Rosji oraz również USA. Skala zagrożeń powoduje, że wydatki firm na zabezpieczenia rosną w coraz szybszym tempie. Według analizy firmy badawczej Gartner[3] w 2017 r. w ujęciu globalnym firmy przeznaczą na ten cel 86,4 mld dol., 7%. więcej niż w 2016 r. Analitycy Gartnera prognozują również, że w 2018 r. poziom wydatków na ten cel sięgnie 93 mld dol.



RODO ZNACZY REWOLUCJA

Liczba i rozmiary przeprowadzanych ataków pokazują, że hakerzy czują się coraz pewniejsi.

Liczba i zasięgi przeprowadzanych ataków pokazują, że hakerzy czują się coraz pewniejsi. Zwłaszcza jeśli korzystają z ochrony określonych państw, ich ściganie jest bardzo trudne, a czasem niemożliwe. Dlatego eksperci prognozują, iż 2018 r. będzie pod tym względem pełen wyzwań. W ocenie VECTO, jednym z największych wyzwań tego roku będzie implementacja nowych regulacji w ochronie danych osobowych. Pod polskim skrótem RODO (ang. GDPR) kryje się prawdziwa rewolucja. Jak podaje PwC[4], to unijne rozporządzenie jest największą zmianą w podejściu do ochrony danych osobowych od dwudziestu lat. RODO wprowadza dużo nowości. Największą jest bezpośrednia odpowiedzialność podmiotu przetwarzającego dane. Co to oznacza dla firm? Organizacje przetwarzające dane osobowe pochodzące z innych firm, w trakcie świadczenia usług na ich rzecz (jak na przykład firmy dostarczające rozwiązania w chmurze czy firmy hostingowe), będą ponosić bezpośrednią odpowiedzialność za złamanie zapisów RODO, włączając w to również otrzymanie kary finansowej.

Co więcej, będą wymagane bardziej restrykcyjne niż dotychczas obowiązki w zakresie tworzenia umów o przetwarzaniu, natomiast odszkodowania i ograniczenia odpowiedzialności najprawdopodobniej będą podlegać renegocjacji. Obowiązkiem administratorów danych będzie zgłaszanie w ciągu 72 godzin od wykrycia, do właściwego organu nadzoru, przypadków naruszeń, które mogą skutkować zagrożeniem praw i swobód osób, których dane zostały naruszone.

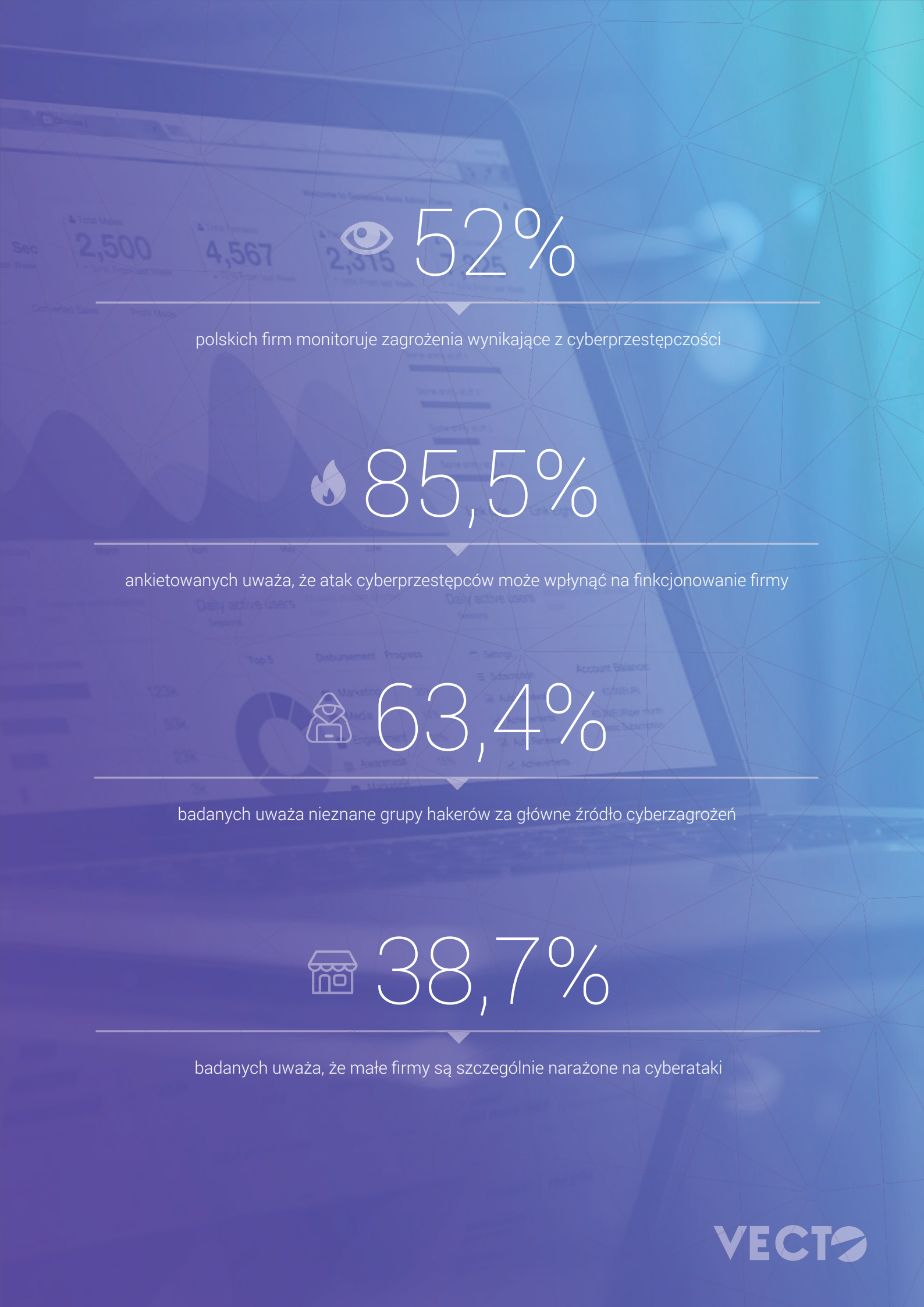
Nowe uprawnienia zyskają też konsumenci, którzy znacznie łatwiej niż dzisiaj będą mogli skorzystać z tzw. „prawa do bycia zapomnianym". Oznacza to usuwanie „na żądanie" wszelkich danych na temat konkretnej osoby. Dla firm już samo w sobie będzie to gigantycznym wyzwaniem, a dodatkowo RODO może stać sie narzędziem w rękach hakerów. Mogą oni zasypywać firmy wnioskami choćby o usunięcie danych, a to spowoduje konieczność ich weryfikacji. Każdy atak może być polem do naruszeń ustawy o danych osobowych, zatem będzie musiał zostać władzom zgłoszony.

Poza RODO, wyzwaniem w zakresie cyberbezpieczeństwa mogą być nowe zabezpieczenia dla systemów opierających się na rozwiązaniach typu chmura danych czy rosnąca popularność kryptowalut. Coraz więcej klientów oczekuje możliwości korzystania z tego typu metod płatności, co dokłada kolejne ryzyko w postaci choćby spekulacji kursami wirtualnych walut, czy ich kradzieży.

INTERNET RZECZY – IOT RÓWNIEŻ GROŹNY

Rynek wykorzystuje nowe technologie w coraz to szerszych obszarach, w tym również takich, z których chętnie korzystamy ze względu na ich walory ułatwiania życia czy poprawy jego komfortu.

Świetnym przykładem takiego trendu jest choćby tzw. „Internet Rzeczy", czyli komunikowanie się urządzeń gospodarstwa domowego przez sieć. Jednak dokładanie modułów wi-fi np. do pralek, lodówek, czy firmowych systemów klimatyzacji powoduje, że stają się one bezwolnym narzędziem w działalności przestępczej. W USA firmy specjalizujące się w systemach zabezpieczeń już kilkukrotnie alarmowały, że właśnie lodówki czy telewizory, stale podłączone do internetu, były często wykorzystywane jako furtki do prowadzenia ataków. Według różnych szacunków, do 2020 roku do globalnej sieci podłączonych będzie już 50 mld urządzeń, w tym również samochodów. Skutki wykorzystania dostępu takie jak przejęcie kontroli nad maszynami czy autami mogą być dramatyczne.



52%

polskich firm monitoruje zagrożenia wynikające z cyberprzestępczości

85,5%

ankietowanych uważa, że atak cyberprzestępców może wpłynąć na finkcjonowanie firmy

63,4%

badanych uważa nieznane grupy hakerów za główne źródło cyberzagrożeń

38,7%

badanych uważa, że małe firmy są szczególnie narażone na cyberataki

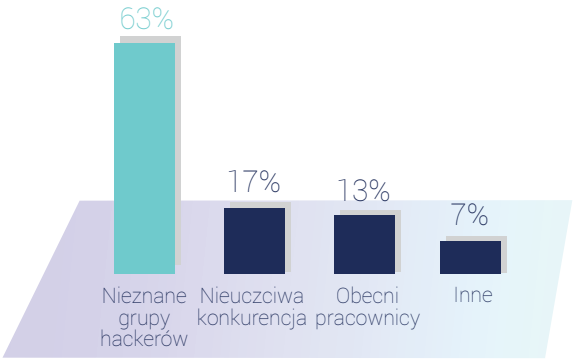
VECTO

ŹRÓDŁA ZAGROŻEŃ

Diagnozy dotyczące potencjalnych źródeł zagrożeń związanych z cyberprzestępczością, jeśli chodzi o polskie firmy, są zbliżone do badań globalnych.

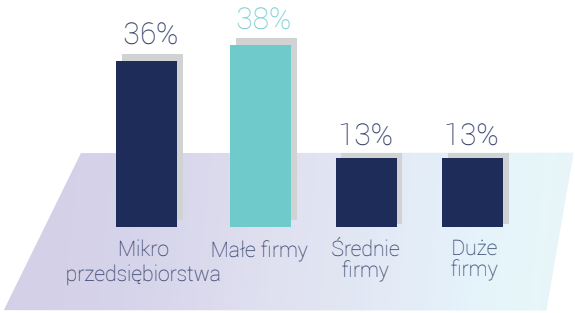
Zdaniem 64,3% ankietowanych w badaniu VECTO, głównym zagrożeniem są nieznane grupy hakerów. Z kolei już tylko nieco ponad 17% widzi takie ryzyko w swoich konkurentach, którzy mogliby stać za tego rodzaju nielegalnymi działaniami.

Co zaskakujące ponad 13% widzi takie ryzyko wśród swoich obecnych pracowników. Jak widać zmiana sytuacji na rynku pracy prowadzi nie tylko do pozytywnych sytuacji. Zwłaszcza w zakresie bezpieczeństwa. Przy rosnącej konkurencji i deficycie specjalistów, rośnie również ryzyko sięgnięcia po metody nielegalne, jak jednoczesne wykradanie danych i blokowanie systemów byłego pracodawcy, na czym zyskuje obecny. Niestety bez kompleksowych zabezpieczeń i procedur dostępu, przeprowadzenie takiej operacji jest stosunkowo łatwe.



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

Dość ciekawie rozłożyły się głosy w pytaniu o to, jakiej wielkości firmy mogą wydawać się najbardziej prawdopodobnym celem cyberataku. Aż 36,1% wskazało, że dane w ten sposób mogą utracić głównie firmy mikro, a zdaniem 37,8% – małe przedsiębiorstwa. Jedynie 12,8% widzi to ryzyko w odniesieniu do firm średnich, a 13,3% – dużych. Trudno powiedzieć jakie mogą być powody takiego wartościowania ryzyka. Wydaje się, że w opinii badanych, to przede wszystkim duże firmy dysponują środkami, umożliwiającymi wdrożenie innowacyjnych rozwiązań, zwiększających bezpieczeństwo infrastruktury informatycznej.

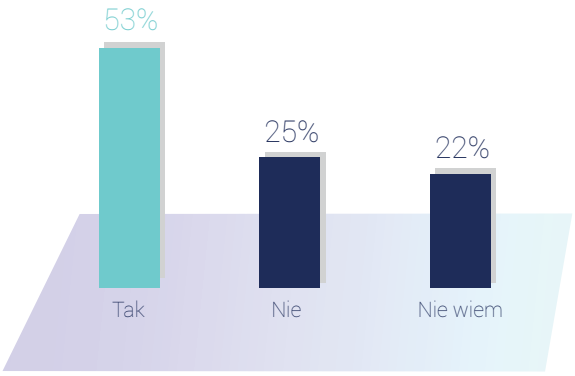


Jakie firmy są Twoim zdaniem szczególnie narażone na utratę danych?

Dotychczasowe doświadczenia pokazują, że to właśnie duże przedsiębiorstwa są celami ataków, ponieważ paraliż systemów IT dla dużych podmiotów oznacza ogromne koszty. Częściej są też skłonne złamać się i pójść na ustępstwa dotyczące wypłaty pieniędzy, aby ataku uniknąć. Małe firmy się na taką opcję nie zdecydują, chyba że w ich bazach są na tyle ważne informacje, iż zrobią wszystko, aby nie dopuścić do złamania zabezpieczeń.

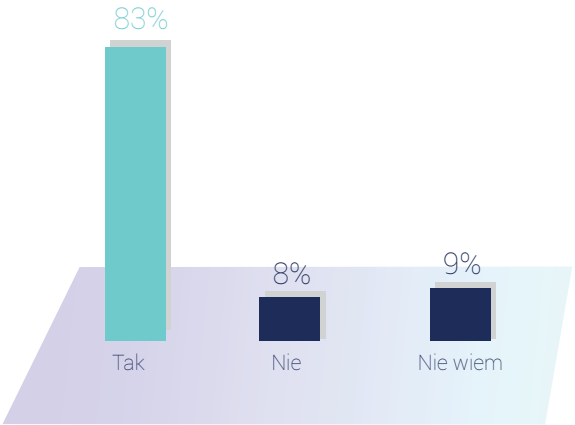
ZABEZPIECZENIA – JAK TO ROBIĄ POLSKIE FIRMY?

O ile sytuacja związana z ogólną świadomością cyberzagrożeń wzrasta, o tyle konieczność poniesienie kosztów minimalizacji ryzyk nie znajduje się na czele priorytetowych działań polskich firm.



Czy Twoja firma monitoruje zagrożenia wynikające z cyberprzestępczości?

Według badania VECTO, tylko nieznacznie ponad 52% z nich monitoruje zagrożenia związane z cyberprzestępczością, co jest zaskakująco niskim poziomem. Tym bardziej, że w następnym pytaniu potwierdzają one wpływ takich zdarzeń na funkcjonowanie przedsiębiorstw – to opinia aż 82,5% badanych.



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

Choć o cyberprzestępczości mówi się coraz częściej i firmy widzą potrzebę zabezpieczania się przed taka ewentualnością, to póki co dość sceptycznie oceniają skuteczność stosowanych zabezpieczeń. W pięciopunktowej skali, najwięcej uznania znalazło w ich oczach zastosowanie programów antywirusowych – średnia ocena tego sposobu to 3,85 pkt. Zdaniem ekspertów jest to dość zachowawcze podejście, ponieważ program antywirusowy jest w stanie obronić tylko przed niektórymi typami ataków. Dodatkowo hakerzy są w stanie skutecznie wykorzystywać wszelkie luki w systemach, więc nawet dobry i regularnie aktualizowany program nie gwarantuje spokoju w tym zakresie.

Nieco mniejsze, choć nadal dość wysokie, uznanie ankietowanych dotyczy zastosowania w firmach procedur bezpieczeństwa. Może to wynikać z wciąż małego zainteresowania zatrudnianiem specjalistów dedykowanych procedurom bezpieczeństwa, co było już sygnalizowane wcześniej. Z drugiej strony tylko odpowiednia kadra jest w stanie wypracować efektywne i mało dokuczliwe procedury, które będą mogły zabezpieczyć firmę. Często wiąże się to z określonymi utrudnieniami dla pracowników - jak zakaz korzystania w miejscu pracy z prywatnych telefonów komórkowych, a zwłaszcza skrzynek e-mail czy profili na serwisach społecznościowych.

Częstym źródłem problemów jest nieostrożne korzystanie ze smartfonów, które zważywszy na ich funkcjonalność są przez użytkowników traktowane jako podręczne komputery. Zapominamy jednak, że w ich przypadku również musimy stosować określone zabezpieczenia. Do tego często użytkownicy korzystają ze smartfonów przy użyciu darmowych, ogólnodostępnych sieci wi-fi, w zasadzie zapraszając przestępców do instalowania na swoim telefonie szkodliwych treści, które mogą się uaktywnić np. gdy telefon jest podłączony do komputera. Tymczasem, aż 72% z wszystkich wykrytych w 2017 roku zagrożeń dotyczyło smartfonów i tabletów.

Co 10 sekund pojawia się nowa odmiana złośliwego oprogramowania atakującego system Android, zwiększając niebezpieczeństwo zainfekowania aż o 50% względem ubiegłego roku. W wielu przypadkach to właśnie urządzenia mobilne stanowią furtkę, przez którą cyberprzestępcy dokonują ingerencji w system IT, kradną lub szyfrują dane, niszczą zasoby informatyczne.

Niemal 3,8 pkt. w pięciopunktowej skali zebrał backup danych - jako metoda na zabezpieczanie firmy przed cyberprzestępczością. Jej efektywność mogła wypaść niżej, ponieważ jest to zagadnienie często kojarzone z określonymi niedogodnościami dla zespołu, a przecież nikt nie lubi, gdy mu się dokłada obowiązków. Zwłaszcza, jeśli pracownik nisko ocenia skuteczność tworzenia kopii zapasowych. Trzeba jednak wyraźnie zaznaczyć, że jest to akurat rozwiązanie szczególnie doceniane przez tych, którzy już doświadczyli cyberataku. Backup co prawda nie jest w stanie zabezpieczyć firmy przed wszystkimi atakami, ale na pewno może bardzo skutecznie ograniczyć negatywne skutki takiego wydarzenia i w krótkim czasie przywrócić zasoby informatyczne sprzed włamania lub zaszyfrowania danych. Firma minimalizuje tym samym potencjalne ryzyko utraty swoich danych, a w wielu przypadkach to przecież podstawowy kapitał przedsiębiorstwa.

Nieco mniejsze, ocenione na 3,66 pkt., uznanie badanych znalazły szkolenia w zakresie bezpieczeństwa. To na pewno bardzo ogólna materia, ale podnoszenie wiedzy w tym

Tak ankietowani w skali 1 do 5 ocenili skuteczości metody ochrony przed cyberzagrożeniami:
(1-mało prawdopodobne, 5-bardzo prawdopodobne):

programy antywirusowe	3.9/5
backup danych	3.8/5
procedury bezpieczeństwa	3.8/5
szkolenia	3.7/5
inne	2.6/5

zakresie warto na każdym etapie popierać. Skuteczność wielu, nawet bardzo prostych ataków wynika właśnie z niewiedzy i niefrasobliwości użytkowników. Objawia się to choćby otwieraniem załączników w mailach z niewiadomych źródeł czy wypełnianiem formularzy na nieznanych stronach.

3,9/5

tak ankietowani określili skuteczność programów antywirusowych
jako metody ochrony przed cyberatakami

4,2/5

tak badani określili ryzyko znacznego osłabienia wizerunku formy w przypadku cyberataku

4,1/5

tak ankietowani określili dotkliwość utraty unikalnego know-how w skutek cyberataku

35%

badanych uważa sektor bankowy za szczególnie narażony na atak
ze strony cyberprzestępców

VECTO

ZAUFANIE KLIENTÓW BEZCENNE

Większe zaangażowanie u ankietowanych wywołało pytanie o konsekwencje potencjalnego ataku na ich przedsiębiorstwo.

Wśród zaproponowanego zestawu spodziewanych skutków takiego zdarzenia, na najwyższy średni wynik - niemal 4,2 pkt. - zasłużyło znaczne osłabienie wizerunku oraz zaufania. Nieco mniej, bo na 4,1 pkt. wskazano ryzyko, iż atak może doprowadzić do strat finansowych przedsiębiorstwa. Taki rozkład odpowiedzi – choć różnice są wciąż niewielkie – pokazuje, że w mentalności doszło do poważnej przemiany. Potencjalne straty wizerunkowe ocenione zostały bowiem jako bardziej dotkliwe, niż spadek przychodów. Widać zarówno przedsiębiorcy jak i pracownicy doceniają już, że straty finansowe można odrobić łatwiej, niż pozbyć się skazy, jeśli chodzi o zaufanie, zarówno u klientów jak i kontrahentów.

Jeszcze mniej wskazań, poniżej 4 pkt., zebrała opinia, iż efektem ataku może być utrata dotychczasowych klientów, a na 3,6 pkt. oceniono ryzyko, że rezultatem cyberataku może być nawet konieczność zlikwidowania firmy. Z raportu CSO z grupy IDG[5] wynika, że koszty cyberataków w ujęciu globalnym w 2021 r. wyniosą już 6 bln dol. Oznacza to podwojenie poziomu notowanego w 2015 r. Cyberprzestępczość zwiększy ponad trzykrotnie liczbę nieobsadzonych, specjalistycznych miejsc pracy w cyberprzestrzeni, która do 2021 r. ma wynieść 3,5 miliona.

Tak ankietowani w skali 1 do 5 ocenili skutki ewentualnego ataku cyberprzestępców na system IT oraz dane firmy
(1-mało prawdopodobne, 5-bardzo prawdopodobne):

może doprowadzić do utraty klientów	3.9/5
może doprowadzić do strat finansowych	4.1/5
może doprowadzić do zamknięcia firmy	3.6/5
może doprowadzić do znacznego osłabienia wizerunku i zaufania	4.2/5

POLSKA SPECYFIKA?

Jeszcze więcej informacji na temat podejścia polskich firm do cyberzagrożeń pokazują odpowiedzi na pytanie, jak ankietowani oceniają obszary, w których utrata danych byłaby dla firmy najbardziej dotkliwa.

Odpowiedzi ponownie oceniano w pięciopunktowej skali i najwyższą średnią ocenę uzyskało niebezpieczeństwo utraty unikalnego know-how i własności intelektualnej. Ten aspekt został oceniony na łącznie 4,1 pkt., co także pokazuje, iż firmy coraz większą wartość przywiązują do swoich niematerialnych zasobów. To kolejny znak czasów. Wiele nowocześnie zarządzanych firm opiera się właśnie na unikalnych kompetencjach, często zarządzanych wyłącznie w sferze cyfrowej. Tym bardziej trzeba się na takie ewentualności przygotować. Szczególnie biorąc pod uwagę, że polskie firmy idąc za globalnym trendem, coraz bardziej się cyfryzują. Jednak doceniając ich wysiłki trzeba zauważyć, że dystans do nadrobienia w stosunku do najbardziej rozwiniętych gospodarek, nadal jest długi.

Jakie inne ryzyka w atakach widzą ankietowani? Na ponad 4 pkt. oceniają szkodliwość utraty firmowej dokumentacji, tylko nieco mniej problematyczna byłaby utrata korespondencji firmowej. Na 3,7 pkt.

Tak ankietowani w skali 1 do 5 ocenili obszary, w których utrata danych byłaby dla firmy najbardziej dotkliwa
(1-mało prawdopodobne, 5-bardzo prawdopodobne):

baza klientów i kontaktów	3.7/5
unikalne know-how i własność intelektualna	4.1/5
korespondencja firmowa	3.8/5
dokumentacja firmowa	4.0/5
strona internetowa	3.7/5
inne	2.2/5

oceniono obawę o stracenie takiego zasobu jak baza klientów i kontaktów, choć jest to akurat coś, co przy sprawnie prowadzonym back-up'ie danych jest w bardzo łatwy i szybki sposób do odtworzenia. Widać zatem, że wciąż bardzo dużo jest na tym polu do zrobienia, zwłaszcza jeśli chodzi o mentalność. Możliwości techniczne dla przeprowadzenia takiej operacji szybko i regularnie ma w zasadzie każda firma. Podobną ocenę zebrało ryzyko utracenia kontroli nad strona internetową. Widać, że nadal jest ona traktowana jako podstawowy wyraz technologicznego rozwoju firmy. Zasoby można odtworzyć szybko, o ile firma na taką ewentualność jest w jakikolwiek sposób przygotowana.

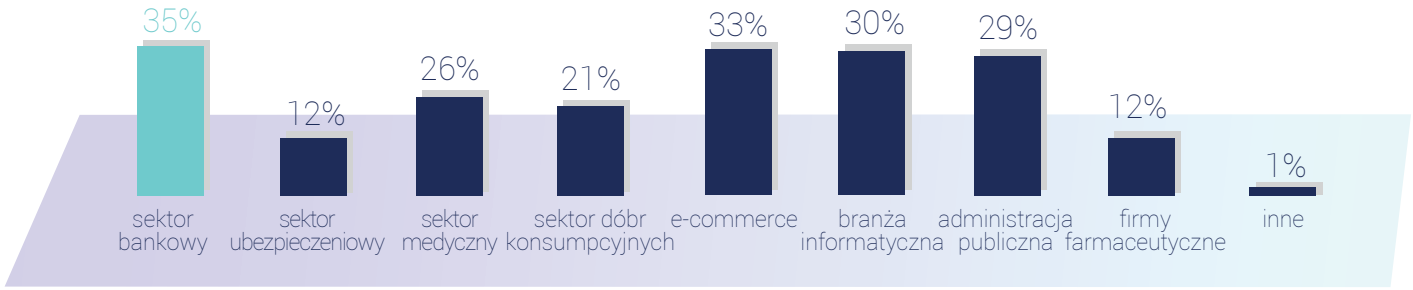
BRANŻE SZCZEGÓLNIE ZAGROŻONE

Autorzy badania pokusili się też o sprawdzenie jakie sektory, zdaniem ankietowanych przedsiębiorstw, są najbardziej narażone na wystąpienie ataku hakerskiego.

Obyło się bez wielkich zaskoczeń, zdaniem największej grupy jest to sektor bankowy. Wskazało go aż niemal 35% badanych, co jest zgodne z trendami ogólnoświatowymi. Instytucje te odpowiadają za bezpieczeństwo powierzonych im przez klientów środków finansowych, dlatego bardzo często stają się obiektem takich ataków.

2017 rok obfitował w spektakularnie przeprowadzone ataki na instytucje bankowe. Bank Centralny Bangladeszu w wyniku działań cyberprzestępców stracił ok. 100 mln dol., a ponad 30 mln dol. zniknęło z kont banku Centralnego Rosji. Sektor komercyjny jeszcze częściej był wystawiany na takie zagrożenia, brytyjska grupa finansowa Lloyds stała się celem jednego z największych ataków, choć firma podkreślała, że na zdarzeniu jej klienci nie ucierpieli. Poszkodowanych można wymieniać długo, również polskie banki stawały się celem agresji międzynarodowych grup hakerskich, aczkolwiek oficjalnie nigdy nie potwierdzały, że do takiego zdarzeń kiedykolwiek miało dojść.

W grudniu 2017 r. okazało się, że celem ataku można stać się łatwiej niż kiedykolwiek. W oficjalnym sklepie Google Play pojawiły się dwie niebezpieczne aplikacje CryptoMonitor i StorySaver. Choć firma bardzo szybko zareagowała i usunęła podejrzane treści, to aplikacje zdążyło pobrać kilka tysięcy Polaków. Aplikacje, zamiast sprawdzać kursy kryptowalut na międzynarodowych rynkach i śledzić profile na Instagramie, błyskawicznie podszywały się pod mobilne aplikacje polskich banków. Nieostrożność użytkowników doprowadzała do przechwycenia loginów i haseł do kont bankowych. Jak podkreślają eksperci, obie aplikacje potrafiły



Branże szczególnie narażone na atak hakerów według ankietowanych

również bez wiedzy użytkownika przechwytywać wiadomości SMS, zawierające kody do autoryzowania transakcji online.

Banki szybko zareagowały i wydały stosowne ostrzeżenia, jednak brak jest oficjalnych danych odnośnie do tego, jak dużo osób zostało poszkodowanych.

E-COMMERCE NA DRUGIM MIEJSCU

Drugim, szczególnie zagrożonym sektorem, według uczestników badania VECTO, jest handel internetowy.

Tu pole do nadużyć jest również ogromne, ponieważ Polacy dopiero poznają taką formę robienia zakupów, stąd wielu zasad postępowania muszą się jeszcze nauczyć. Tymczasem konta użytkowników na popularnych serwisach handlowych są dla hakerów cennym łupem. Zawierają bowiem komplet danych, włącznie z często podawanymi numerami kart kredytowych, co pozwala – niestety skutecznie – wyczyścić bankowe konto.

Inne sektory, wskazywane przez grupę ok. 30% ankietowanych, to branża medyczna, informatyczna oraz administracja publiczna. Zwłaszcza w ostatnim przypadku, postępująca informatyzacja ogromnych baz danych powoduje wzrost ryzyka cyberataków. Społeczeństwo oczekuje, iż coraz więcej spraw urzędowych będzie można załatwić przez Internet. W ślad za rozwojem tego sektora usług, musi zatem pójść jeszcze szybszy rozwój systemów zabezpieczających bazy przed atakami. Inne sektory, w których przypadku występuje ryzyko ataku cyberprzestępców, to dobra konsumpcyjne, farmacja czy branża ubezpieczeniowa. Widać zatem doskonale, że problem ten dotyczy w zasadzie całej gospodarki. Opieszałość w dostosowaniu się do dynamicznie zachodzących zmian w zakresie cyberbezpieczeństwa może być niezwykle trudna dla każdej firmy, niezależnie od branży, w której funkcjonuje.

PODSUMOWANIE

O powadze ryzyk związanych z cyberprzestępczością nikogo nie trzeba przekonywać. Wśród przedsiębiorców świadomość takich zagrożeń jest dość wysoka. Z cyberatakiem kiedykolwiek zetknęło się ponad 54,5% ankietowanych. Przeciwnego zdania było z kolei niemal co czwarte przedsiębiorstwo. Idąc dalej, zdaniem 85% badanych kwestia zabezpieczania firmowych danych jest istotna.

Jednak jak wynika z raportu firmy VECTO na tym kończą się dobre wiadomości, jeśli chodzi o kwestię zabezpieczeń przed nowymi zagrożeniami z cyfrowej przestrzeni. Jedynie 33,6% ankietowanych oceniło poziom zabezpieczeń w swoich firmach jako prawidłowe, a 38% miało przeciwne zdanie. Na świecie firmy bardzo szybko zwiększają wydatki na modernizację systemów informatycznych i wszelkiego rodzaju zabezpieczenia, a w Polsce niestety dominuje nastrój oczekiwania. Mobilizująco może podziałać poważny atak, w wyniku którego firmy stracą swoje dane.

Tylko połowa firm monitoruje zagrożenia związane z cyberprzestępczością, co jest zaskakująco niskim poziomem. Choć z drugiej strony, zdaniem ponad 82,5% ankietowanych, atak cyberprzestępców na system informatyczny może wpłynąć na funkcjonowanie przedsiębiorstwa. Widać zatem zadziwiającą niekonsekwencję.

Tym bardziej, że jednocześnie badane firmy sceptycznie oceniają skuteczność stosowanych zabezpieczeń. W pięciopunktowej skali najwięcej uznania znalazły programy antywirusowe, – średnio ocenione na 3,85 pkt. Niemal 3,8 pkt. zebrał backup danych, a 3,66 pkt. szkolenia w zakresie bezpieczeństwa. Z drugiej strony, tylko co czwarta firma przyznała, iż zdecydowała się na zatrudnienie specjalisty, zajmującego się wyłącznie ochroną danych, zaprzeczyło temu zdecydowanie 13,3% badanych. Największa grupa 61% ankietowanych nie miała zdania bądź nie wiedziała. Takie podejście można oczywiście tłumaczyć oszczędnościami, ale w przypadku zwłaszcza dużych firm, to także przykład niefrasobliwości i odsuwania od siebie zagrożenia. Dopiero utrata danych, klientów czy nawet upokorzenie, gdy na firmowej stronie internetowej znajdą się nieodpowiednie treści np. pornografia, mogą skłonić do bardziej zdecydowanych działań. Firmy doskonale zdają sobie sprawę, że atak jest bardzo realny, ale mają nadzieję, że jeszcze teraz ich takie zdarzenie nie spotka.

Tymczasem analitycy zgodnie oceniają, że hakerzy decydują się na odważniejsze kroki i uderzają w coraz to nowe sektory czy państwa. Polskie firmy już kilka razy przekonały się jak dokuczliwe może to być zdarzenie, choć zmasowanych akcji na wielką skalę, póki co jeszcze większość nie doświadczyła. Niestety taki stan rzeczy może się długo nie utrzymać. Cyberzagrożenia to jeden z absolutnych priorytetów na 2018 r. i czas, aby polskie firmy również zaczęły podchodzić do tego zagadnienia w taki sposób. Gdy zaczną działać dopiero po wystąpieniu ataku, na reakcję będzie za późno. Wtedy skutków nie uda się zminimalizować, co może doprowadzić do likwidacji firmy. Ważna jest zmiana podejścia w tym aspekcie. To po prostu wojna, tylko że cyfrowa i w wirtualnym świecie, choć często za prawdziwe pieniądze.

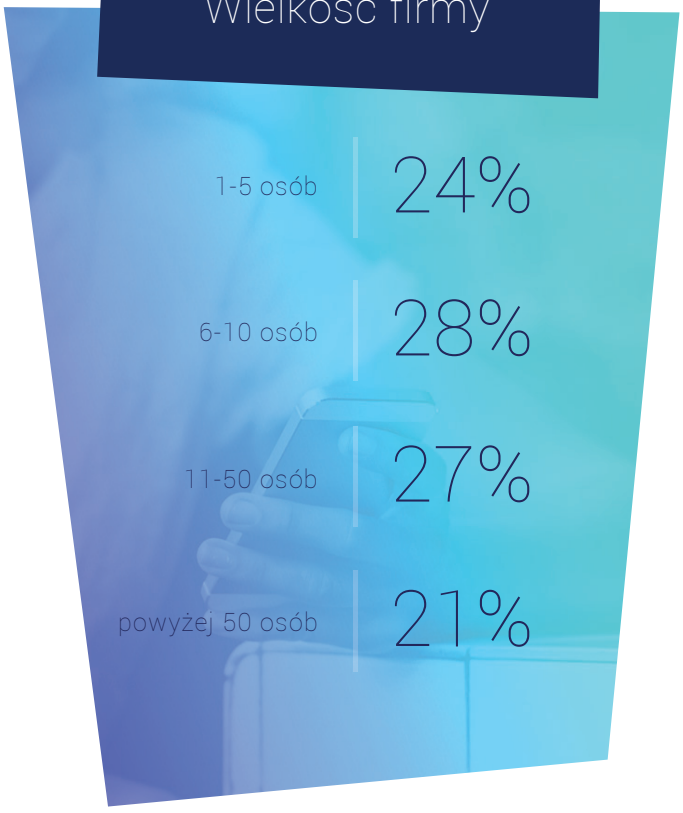
METODOLOGIA

Badanie zostało przeprowadzone od kwietnia do końca września 2017 r. na próbie niemal 430 respondentów. Największa próba poddana została badaniu w formie kwestionariusza internetowego, stosowane były też ankiety w formie papierowej oraz e-mailowej.

Największą grupę badanych stanowili przedstawiciele sektora usługowego (ponad 13% udziału w ogólnej liczbie), odpowiednio – po ponad 10% stanowiły też przedsiębiorstwa zajmujące się medycyną i ochroną zdrowia, oraz sektora finansowego i bankowości, jak również przedstawiciele branży IT.

Dominowali przedstawiciele firm średnich i dużych. Przedsiębiorstwa zatrudniające 6-10 osób stanowiły 28,4% ogółu badanych, te z zatrudnieniem 11-50 osób – 26,8 %. Co czwarta ankietowana firma była reprezentantem firm małych, z zatrudnieniem do 5 osób, a firmy największe z ponad 50-osbowymi zespołami stanowiły 21,2% badanych przedsiębiorstw.

Wielkość firmy



1-5 osób	24%
6-10 osób	28%
11-50 osób	27%
powyżej 50 osób	21%

Reprezentowana branża

budownictwo / architektura / wykończenie wnętrz	1%
edukacja / badania naukowe	2%
finanse / bankowość	11%
hotelarstwo / turystyka / rekreacja / sport	3%
handel hurtowy i detaliczny	9%
instytucje rządowe i samorządowe	9%
łączność / telekomunikacja	5%
media / kultura i sztuka / rozrywka	4%
medycyna / ochrona zdrowia	10%
produkcja / dystrybucja / logistyka	9%
przemysł komputerowy / oprogramowanie	10%
przemysł komputerowy / sprzęt	4%
usługi dla firm / usługi dla ludności	13%
usługi internetowe	3%
inna	4%

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

VECTO Sp. z o.o.
al. Lotników 32/46, blok XV
(teren Instytutu Fizyki)
02-668 Warszawa
www.vecto.pl

PRZYPISY

1. https://www.cisco.com/c/m/en_au/products/security/offers/annual-cybersecurity-report-2017.html
2. https://www.trendmicro.com/vinfo/gb/security/news/cyber-attacks/web-defacements-exploring-the-methods-of-hacktivists
3. https://www.gartner.com/newsroom/id/3784965
4. https://www.pwc.pl/pl/artykuly/2017/10-najwazniejszych-zmian-ktore-wprowadza-rodo.html
5. https://www.csoonline.com/article/3153707/security/top-5-cybersecurity-facts-figures-and-statistics.html