Digital Security
Progress. Protected.

Cyberportret polskiego biznesu

RAPORT: Bezpieczeństwo cyfrowe oczami ekspertów i pracowników

RAPORT ESET I DAGMA BEZPIECZEŃSTWO IT

SPIS TREŚCI

00

WPROWADZENIE

MICHAL JANKECH
Vice President of Enterprise & SMB/MSP, ESET

Gdzie bylibyśmy w dzisiejszych czasach bez technologii informatycznych? Gwałtowny wzrost ich wykorzystania przyniósł nam wiele korzyści, ale także nowe wyzwania. Rozwój AI radykalnie zmienił krajobraz zagrożeń, przynosząc zarówno korzyści, jak i trudności. Phishing rozwija się dzięki optymalizacji tłumaczeń i automatyzacji pisania tekstów, w dużej mierze dzięki tzw. dużym modelom językowym. Prowadzi to do wzrostu liczby przypadków naruszenia bezpieczeństwa w biznesowych wiadomościach e-mail i kradzieży danych uwierzytelniających.

Jednocześnie cyberwojna w Ukrainie pokazała jak pilna jest potrzeba skoncentrowania wysiłków na ochronie infrastruktury krytycznej. Przeprowadzane jednocześnie, liczne przypadki ataków na łańcuchy dostaw (SolarWinds, MoveIT, CDK Global) i ataki na firmy (Microsoft) przeprowadzane przez zorganizowane jednostki realizujące złożone ataki (APT – Advanced Persistent Threat) pokazały, że cyberprzestępcy wiedzą, gdzie znajdują się pieniądze i dane, bez względu na wielkość przedsiębiorstwa.

Według danych zebranych w naszym raporcie, 88% firm było celem cyberataku lub wycieku danych w ostatnich latach. Niestety, tylko 59% polskich firm twierdzi, że korzysta z oprogramowania antywirusowego. Istnieje wiele ryzyk i zagrożeń związanych z cyberbezpieczeństwem, a jak wcześniej informował ESET, małe i średnie firmy mierzą się z brakiem zaufania do własnych możliwości w zakresie radzenia sobie z nimi wszystkimi. Nie jest więc zaskoczeniem, że trudno im nadążyć za wyzwaniami.

Dlatego też firmy wolą, aby to dostawcy usług IT dbali o ich bezpieczeństwo i bezpośrednio stawiali czoła wyzwaniom związanym z najnowszymi zagrożeniami. Specjaliści ds. cyberbezpieczeństwa nieustannie opracowują nowe rozwiązania, aby odeprzeć ataki cyberprzestępców oraz wyprzedzać ich działania. Ich proaktywne podejście do bezpieczeństwa oparte na działaniach zapobiegawczych, łączy ludzką pomysłowość i dojrzałość oprogramowania z odrobiną mocy sztucznej inteligencji.

Kluczowym wyzwaniem jest teraz dotrzymywanie tempa stale ewoluującym zagrożeniom, czyli swojego rodzaju batalia z cyberprzestępcami, w której ESET bierze udział od ponad trzech dekad. Sukces jednak nie zależy tylko od ESET, ale od całej branży cyberbezpieczeństwa i wymaga wspólnych wysiłków oraz proaktywnego podejścia.

00

WPROWADZENIE

ANNA PIECHOCKA
Dyrektor zarządzająca DAGMA Bezpieczeństwo IT

Żyjemy w świecie tak mocno osadzonym w technologii cyfrowej, że coraz trudniej wskazać obszar, w którym jej jeszcze nie ma. Jesteśmy w niej po prostu zanurzeni. To jest dziś nasz świat. W tym nowym cyfrowym świecie, tak samo jak w świecie fizycznym, mamy niestety do czynienia z przestępczością - włamania, kradzieże, wymuszenia, oszustwa stały się codziennością.

Poruszamy się coraz swobodniej w tej cyfrowej rzeczywistości i nie wyobrażamy sobie dziś życia bez niej. A jednak większość z nas bardzo słabo rozumie technologie i mechanizmy, na których jest zbudowana. To stwarza ogromną przestrzeń dla cyberprzestępców. Korzystając z dobrodziejstw cyfrowego świata, bazujemy na nawykach i logice wyniesionej ze świata fizycznego – skoro widzę osobę, którą znam, słyszę jej głos, dostaję od tej osoby wiadomość, to wszystkie zmysły mówią mi, że to jest rzeczywiście ta osoba. W świecie fizycznym – tak. W świecie cyfrowym – niekoniecznie. Jeżeli ktoś włamie się do naszej firmy i coś wartościowego z niej ukradnie, to przecież natychmiast się zorientuję i zauważę co zginęło. W świecie fizycznym – tak. W świecie cyfrowym – niekoniecznie.

Dla zachowania bezpieczeństwa kluczowe jest rozumienie różnic pomiędzy zagrożeniami w świecie rzeczywistym i wirtualnym. Niezbędna jest edukacja pracowników w zakresie tych właśnie różnic, mechanizmów ataków oraz zasad bezpieczeństwa. Jak pokazuje raport „Cyberportret polskiego biznesu" wydaje się, że szczególnie nienajlepiej jest w zakresie rozumienia przez pracowników mechanizmów ataków oraz tego, w jaki sposób działają cyberprzestępcy. Niestety, ale bez należytej wiedzy i cyberhigieny będziemy wobec nich bezradni.

Warto pamiętać, że nawet najlepsze procedury i zabezpieczenia technologiczne mogą okazać się zupełnie bezużyteczne, gdy zawiedzie człowiek. Raport, który przedstawiamy, pokazuje, że zakres wiedzy, szczególnie w mniejszych firmach, nie jest najlepszy, a przecież bazuje on na samoocenie pracowników – rzeczywistość jest najprawdopodobniej jeszcze mniej kolorowa.

01

Raport w skrócie

WYBRANE USTALENIA RAPORTU

Raport w skrócie

"Cyberportret polskiego biznesu" wygląda niejednoznacznie – jego część mocno niepokoi, inna pokazuje bezprecedensowe szanse rozwoju firm. W niniejszym raporcie konfrontujemy postawy "szeregowych" pracowników z opiniami ekspertów. Z tej konfrontacji wyłania się niejednoznaczny obraz gotowości firm na czekające je wyzwania. Wnioski przedstawione w raporcie oparliśmy na badaniu opinii ponad 1000 pracujących Polek i Polaków, w tym 250 specjalistów ds. cyberbezpieczeństwa*.

Raport ESET przygotowany we współpracy z DAGMA Bezpieczeństwo IT prezentuje postawy firm oraz ich pracowników w obszarze cyberbezpieczeństwa na różnych poziomach działalności organizacji. Przyjrzeliśmy się codziennym postawom pracowników: ich skłonności do niebezpiecznych zachowań, niedozwolonym działaniom na sprzęcie służbowym, a także osobistym doświadczeniom z cyberatakami. Sprawdziliśmy też, jak oceniają swoje własne kompetencje w obszarze cyberbezpieczeństwa i jakie czynniki skłaniają ich do zwiększania wiedzy w tym zakresie.

Analizując postawy firm, zweryfikowaliśmy ich aktywność w obszarze szkolenia pracowników i gwarantowania odpowiedniego poziomu wiedzy na temat firmowej polityki bezpieczeństwa. Sprawdziliśmy z jakimi wyzwaniami w obszarze cyberbezpieczeństwa mierzą się w swoim codziennym funkcjonowaniu. Na poziomie strategicznym zapytaliśmy biznes, które kwestie związane z ochroną przed cyberatakami uważa za priorytetowe, jaką część budżetu przeznacza na ten cel, a także jaką rolę cyberbezpieczeństwo odgrywa w jego długofalowych planach.

Wszystkie te wątki odnajdą Państwo w raporcie "Cyberportret polskiego biznesu". Na następnej stronie prezentujemy jego wybrane ustalenia.

*W raporcie w każdym miejscu, w którym piszemy o "pracownikach" referujemy wyniki badania opinii osób pracujących ze sprzętem służbowym przez minimum 3 dni w tygodniu, nie będących ekspertami w obszarze cyberbezpieczeństwa. Natomiast pisząc o "ekspertach", "specjalistach", odnosimy się do wyników dotyczących odpowiedzi osób pracujących na co dzień w cyberbezpieczeństwie.

1 na 5

Cyberataki zdarzają się częściej, niż mogłoby się wydawać. Z badania ESET i DAGMA Bezpieczeństwo IT wynika, że już co piąty polski pracownik padł ofiarą cyberataku w miejscu pracy, a co trzeci ma taką osobę w kręgu swoich znajomych lub w rodzinie.

59%

Tylko 59% badanych polskich firm deklaruje, że używa oprogramowania antywirusowego. Oznacza to duże zagrożenie dla ponad 1/3 przedsiębiorstw.

48%

Na ogólny poziom bezpieczeństwa nie wpływa dobrze także poziom wiedzy pracowników. Mniej niż połowa z nich twierdzi, że potrafią w odpowiednim momencie zareagować na zagrożenie cyberatakiem. Tylko co drugi korzysta z niepowtarzających się haseł na służbowych kontach i urządzeniach, a ⅔ przyznaje się także do faktycznego użytkowania firmowego sprzętu do celów prywatnych.

48%

Niemal połowa ekspertów ds. cyberbezpieczeństwa wśród TOP 5 obszarów wymagających pilnych inwestycji i rozwoju wymienia szkolenia. 31% z nich uważa, że ich firma wydaje zbyt mało środków na szkolenie zespołu w tym zakresie.

32%

Pomimo realnego zagrożenia, zaledwie co trzecia firma przeprowadza regularne testy bezpieczeństwa teleinformatycznego.

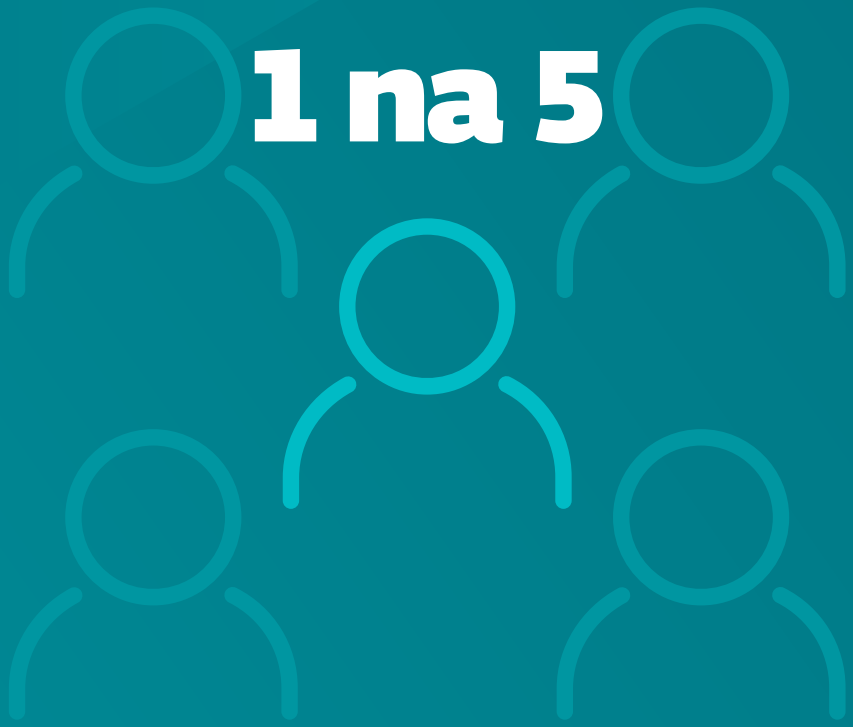
70%

Potrzebę szkoleń widzą też sami pracownicy - większość z nich oceniła, że szkolenie w zakresie cyberbezpieczeństwa pozytywnie wpłynęło na ich poczucie bezpieczeństwa. Mimo to aż 52% pracowników nie wzięło udziału w takim szkoleniu w ciągu ostatnich pięciu lat.

02

Cyberzagrożenia w firmach

PERSPEKTYWA BIZNESU ORAZ OSOBISTE DOŚWIADCZENIA PRACOWNIKÓW



Już co piąty polski pracownik padł ofiarą cyberataku w miejscu pracy, a co trzeci zna osobę, która go doświadczyła.

Z roku na rok cyberprzestępców jest więcej i dysponują oni szerszym wachlarzem szkodliwych narzędzi. Badanie wskazuje, że cyberataki stają się stałym elementem naszej rzeczywistości zarówno w życiu zawodowym, jak i prywatnym. Co pracownicy polskich firm powinni wiedzieć o cyberzagrożeniach i ich potencjalnych skutkach? Dlaczego to prezesi powinni mieć się szczególnie na baczności?

Cyberzagrożenia w firmach

Razem z rozwojem technologicznym i cyfryzacją zasobów firmowych, cyberbezpieczeństwo stało się jednym z najważniejszych wyzwań dla firm na całym świecie. Rośnie liczba ataków i stają się one coraz bardziej wyrafinowane oraz zaawansowane technicznie. Z uwagi na ich potencjalne konsekwencje w postaci poważnych strat finansowych, uszczerbku na reputacji firmy oraz naruszenia prywatności danych, przedsiębiorstwa są zmuszone do ciągłego monitorowania i wzmacniania swoich systemów zabezpieczeń. Szczególną rolę pełni edukacja, zwłaszcza w temacie odpowiedniej profilaktyki, bezpiecznych nawyków oraz skutków incydentów. Na początku raportu "Cyberportet polskiego biznesu" przyglądamy się rodzajom zagrożeń jakie dotykają firmy, świadomości oraz podatności na ataki wśród osób na różnych stanowiskach w organizacji.

SKALA CYBERZAGROŻEŃ W ŻYCIU ZAWODOWYM I PRYWATNYM

Na cyberataki jesteśmy narażeni przez 24 godziny na dobę, dlatego odpowiednia profilaktyka jest równie ważna dla urządzeń służbowych, jak i prywatnych. Skala zagrożeń w obu sferach jest bardzo duża. 20% badanych pracowników polskich firm przyznaje, że padli ofiarą cyberataku w miejscu pracy. Kolejnych 17% ma trudności z ustosunkowaniem się do tego zdania, a nieco mniej niż 2/3 jest pewnych, że nigdy nie doświadczyli takiej sytuacji w środowisku zawodowym. Warto także zauważyć, że 34% respondentów zna osobę, która była ofiarą cyberataku podczas wykonywania obowiązków służbowych. Dane te wskazują, że tego typu zagrożenia dawno przestały być już marginalną kwestią.

W życiu prywatnym te statystyki są jeszcze bardziej niepokojące. 29% pracowników stwierdziło, że zdarzyło im się paść ofiarą cyberataku na swoim prywatnym sprzęcie, a prawie co drugi (45%) ma taką osobę w kręgu swojej rodziny i znajomych. Jedną z kwestii, które mogą mieć na to wpływ, może być większa skłonność do zachowań ryzykownych na prywatnych urządzeniach (np. pobieranie filmów z nielegalnych źródeł, niezweryfikowane zakupy online czy klikanie w linki obecne w social mediach).

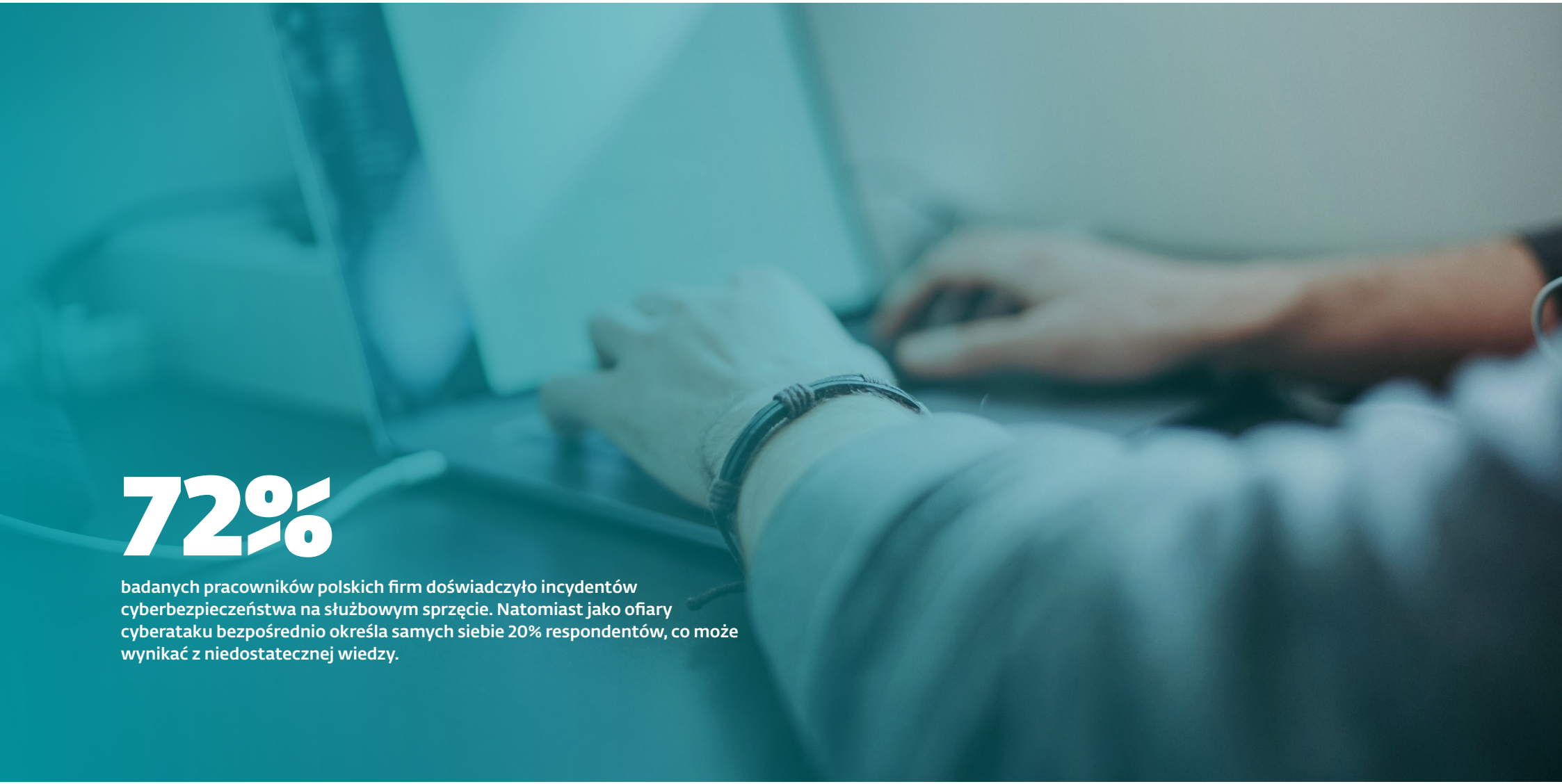
Już co piąty polski pracownik padł ofiarą cyberataku w miejscu pracy, a co trzeci ma taką osobę w kręgu swoich znajomych lub rodziny.

Warto zaznaczyć, że podane liczby dotyczą tylko ataków uświadomionych. Rzeczywista liczba osób, które padły ofiarą cyberataków może być większa z uwagi na niewystarczającą wiedzę i świadomość na temat zagrożeń oraz obawy przed stygmatyzacją ze względu np. na nieostrożność w kwestii cyberbezpieczeństwa. Wiele osób również przez długi czas nie wie, że mogło paść ofiarą cyberataku.

PRACOWNICY: TYPY INCYDENTÓW, KTÓRYCH DOŚWIADCZYLI

Jeszcze ciekawszy obraz wyłania się z analizy odpowiedzi na pytanie, w którym pracownikom podane zostały różne rodzaje incydentów. Choć wcześniej tylko co piąty uznawał się za ofiarę cyberataku w pracy, to już tylko 28% nie miało do czynienia z żadnym z wymienionych przez nas incydentów bezpieczeństwa. To kolejny dowód na to, że diagnoza pracowników może być niedoszacowana, a część zdarzeń mogą postrzegać jako niezwiązane z cyberbezpieczeństwem.

Wachlarz różnego rodzaju zagrożeń jest szeroki, ale nie wszystkie typy ataków są powszechnie znane. Na czele rankingu najczęstszych incydentów wyróżniają się dwa. Blisko połowa badanych pracowników (47%) otrzymała wiadomość z niebezpiecznego źródła, która nie została przechwycona przez filtry antyspamowe. Drugie w kolejności są telefony z nieznanych numerów i nietypowych lokalizacji zagranicznych (41%). Podium zamykają alerty z programu antywirusowego o potencjalnym zagrożeniu – takie powiadomienie otrzymał co trzeci pracownik (32%).



72%

badanych pracowników polskich firm doświadczyło incydentów cyberbezpieczeństwa na służbowym sprzęcie. Natomiast jako ofiary cyberataku bezpośrednio określa samych siebie 20% respondentów, co może wynikać z niedostatecznej wiedzy.

Należy wziąć pod uwagę, że niższe wyniki takich odpowiedzi jak włamanie do firmowego systemu czy przejęcie poufnych danych firmowych mogą nie odzwierciedlać rzeczywistości. Część incydentów mogła pozostać niewykryta, zwłaszcza w firmach, które nie zatrudniają nikogo odpowiedzialnego za cyberbezpieczeństwo. Warto również pamiętać, że część badanych może nie przyznawać się do tego typu doświadczeń z obawy przed stygmatyzacją lub o nich nie wiedzieć.

PRACOWNICY NAJBARDZIEJ NARAŻENI NA CYBERATAKI

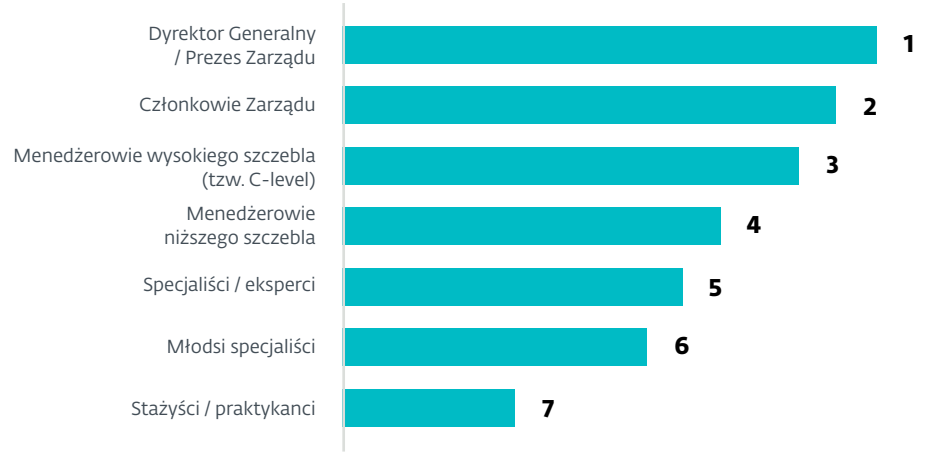
Opinie pracowników w badaniu postanowiliśmy uzupełnić o perspektywę ekspertów ds. cyberbezpieczeństwa. Na ataki narażeni są wszyscy, ale poziom zagrożenia różni się w zależności od zajmowanego stanowiska. Badanie ESET i DAGMA Bezpieczeństwo IT potwierdza, że im wyższe stanowisko zajmuje pracownik, tym bardziej narażony jest na cyberataki. Wynika to z poziomów dostępu do danych – prezes zarządu czy menadżerowie wysokiego szczebla, mają dostęp do większej liczby cennych informacji i zasobów w porównaniu do szeregowych specjalistów czy kadry juniorskiej, dlatego dla cyberprzestępców są dużo bardziej wartościowym celem ataku.

Im mniej doświadczeni i przeszkoleni są pracownicy, tym większe ryzyko błędu wpływającego negatywnie na cyberbezpieczeństwo firmy. W tym kontekście ataki ilościowe mają większą szansę sukcesu, ze względu na większą liczebność pracowników niższego szczebla. Jednak z drugiej strony skala wpływu incydentu na firmę jest dużo wyższa na poziomie np. prezesa czy członka zarządu. Tym bardziej, że wysoko postawieni pracownicy często mają dostęp do ważniejszych zasobów czy też są zwolnieni z niektórych blokad związanych z poufnymi czy wrażliwymi danymi. To stwarza dodatkowe zagrożenia, dostrzegalne przez osoby odpowiadające za bezpieczeństwo IT.

Typy incydentów doświadczanych przez pracowników

Hierarchia zagrożenia cyberatakami według poziomu stanowiska - opinie ekspertów ds. cyberbezpieczeństwa

(kolejność od najbardziej do najmniej zagrożonych)



Na potrzeby badania zapytaliśmy ekspertów ds. cyberbezpieczeństwa o siedem poziomów stanowisk oraz stopień ich zagrożenia cyberatakami. Eksperci oceniali, które ze stanowisk ich zdaniem są najbardziej narażone na działania cyberprzestępców. Jako najbardziej zagrożonych ocenili prezesów zarządu oraz dyrektorów generalnych, niewiele niżej znaleźli się członkowie zarządu. Biorąc pod uwagę uzyskane odpowiedzi, grupą najrzadziej wybieraną jako cel ataku okazują się stażyści i praktykanci. Z uwagi na ograniczone dostępy do danych i zasobów, nie są dla przestępców równie atrakcyjnymi celami, mimo potencjalnie mniejszego doświadczenia i wiedzy w temacie cyfrowego bezpieczeństwa.

Różnić mogą się także narzędzia wykorzystywane przez przestępców w zależności od stanowiska pracowników. Można założyć, że bardziej celowane i złożone metody będą wymierzone w wyżej usytuowanych w hierarchii pracowników podczas gdy np. najpowszechniejsze, szeroko rozsyłane odmiany cyberataków mogą trafiać w kadrę mniej doświadczoną i mniej wyedukowaną w kwestii cyberbezpieczeństwa.

PAWEŁ JUREK

Business Development Director, DAGMA Bezpieczeństwo IT

Z jednej strony firmy mierzą się z cyberatakami podobnego rodzaju, co indywidualni użytkownicy. Przywołać tu można popularne mechanizmy wyłudzeń, przy których cyberprzestępcy zarabiają dzięki wykorzystaniu efektu skali. Przykładami są masowe kampanie phishingowe, wykorzystanie kont w mediach społecznościowych do wyłudzeń czy oprogramowanie wymuszające okup (ransomware). Podjęcie tysięcy prób zawsze przynosi cyberprzestępcom pewien odsetek osób zaatakowanych „z sukcesem", dzięki którym takie masowe kampanie nadal się opłacają.

Jednak z punktu widzenia firm znacznie trudniejszym rodzajem ataków są te, w których cyberprzestępcy biorą na cel konkretną organizację i konsekwentnie przygotowują wieloetapowy scenariusz przestępstwa. Jest to pewien szczególny rodzaj phishingu, nazywany „spear phishingiem". W jego ramach cyberprzestępcy zbierają wszelkie dostępne informacje na temat struktury wewnętrznej organizacji, imion, nazwisk, powiązań służbowych, aby uprawdopodobnić treści fałszywych wiadomości. Tego typu działania są znacznie trudniejsze do wykrycia i spędzają sen z powiek szefom nawet dobrze zabezpieczonych organizacji. Takie ataki, choć znacznie rzadsze i kosztowne w przygotowaniu – są szczególnie groźne, jeśli zostaną zastosowane wobec wyższej kadry zarządzającej.

EKSPERCI: NAJCZĘŚCIEJ ODNOTOWYWANE RODZAJE CYBERZAGROŻEŃ

Najczęstszym cyberzagrożeniem dla firm są ataki phishingowe. Powszechność tego typu ataków wynika z łatwości ich przeprowadzenia – nie wymagają szerokiej wiedzy technicznej i opierają się w dużym stopniu na socjotechnice.

Co trzeci (34%) badany ekspert od cyberbezpieczeństwa wskazał, że w ciągu ostatniego roku jego firma doświadczyła ataku phishingowego. Na kolejnym miejscu znalazły się ataki na sieć Wi-Fi (22%), których celem jest najczęściej zakłócenie pracy sieci i tym samym firmy. Trzecim najczęściej wymienianym rodzajem zagrożenia są ataki z wykorzystaniem trojanów i ataki na aplikacje internetowe (po 19%).

Na stosunkowo odległym, bo 10. miejscu znajdują się ataki związane z usługami chmurowymi. Trwająca obecnie w wielu firmach cyfrowa transformacja zakłada przenoszenie zasobów do chmury, natomiast kwestia bezpieczeństwa tego procesu jest obiektem szerokich dyskusji. Badania pokazują jednak, że tylko średnio co dziewiąty (11%) specjalista od cyberbezpieczeństwa spotkał się z tym rodzajem ataku w ciągu ostatnich dwunastu miesięcy.

Warto podkreślić, że w dłuższej perspektywie czasowej cyberataki okazują się elementem, który zdarza się w zdecydowanej większości firm zatrudniających ekspertów ds. cyberbezpieczeństwa. Aż 88% respondentów z tej grupy przyznaje, że w ich firmie doszło do cyberataku w ciągu ostatnich pięciu lat.

EKSPERCI: AKTUALNY KRAJOBRAZ CYBERATAKÓW

W ostatnich kilku latach obserwujemy wzrost świadomości zagrożeń cyberbezpieczeństwa i ich konsekwencji dla firm. To pozytywny trend, ale wynika on głównie ze zwiększonej liczby ataków i szkód z nimi związanych.

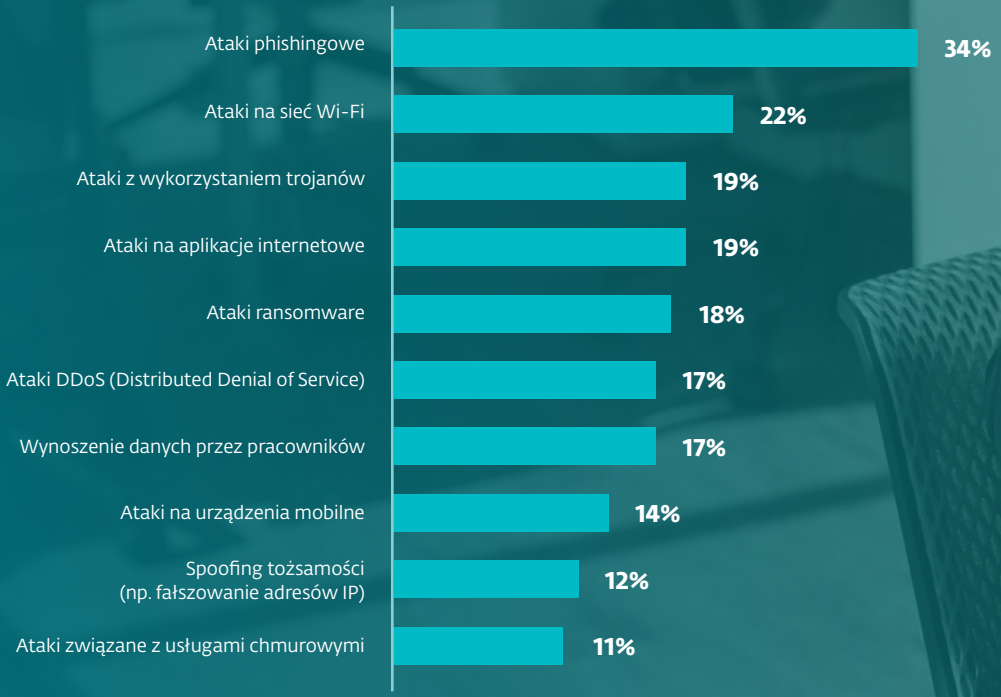
59% badanych ekspertów ds. cyberbezpieczeństwa zgodziło się z tezą, że w ich firmie w ciągu ostatnich kilku lat wzrosła świadomość cyberzagrożeń wśród kierownictwa. Jednocześnie 39% twierdzi, że w ostatnim roku liczba ataków na ich firmę wzrosła a niemal co drugi uważa, że zwiększyła się także ich różnorodność. Cyberprzestępcy coraz śmielej dokonują ataków i zwiększają ich repertuar. Odczuwają to firmy, które ich doświadczyły. Co trzeci (33%) specjalista ds. cyberbezpieczeństwa pracował w firmie, która w wyniku cyberataku doznała strat finansowych. Podobny odsetek (34%) twierdzi, że miał okazję pracować w firmie, której reputacja została nadszarpnięta w wyniku cyberataku.

EKSPERCI: OBAWY PRZED SKUTKAMI CYBERATAKÓW

Niemal zawsze cyberataki wiążą się z negatywnymi konsekwencjami – nawet jeśli nie wymiernymi w postaci strat finansowych, to prowadzącymi do nadszarpnięcia reputacji. W konsekwencji aż 96% badanych ekspertów obawia się konsekwencji cyberataków. Potencjalne straty finansowe są jednak najbardziej dotkliwe i to widać w nastawieniu specjalistów ds. cyberbezpieczeństwa względem cyfrowych zagrożeń.

Co trzeci ekspert cyberbezpieczeństwa obawia się strat finansowych firmy w efekcie cyberataku.

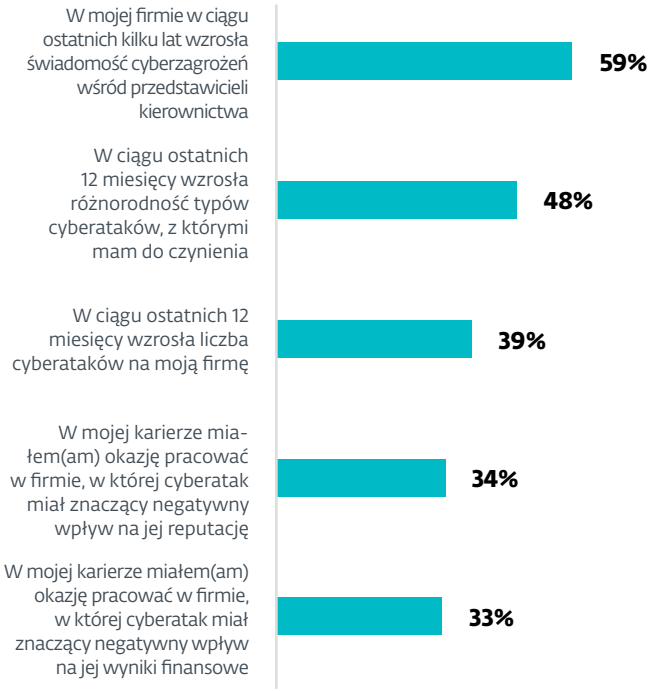
Typy zagrożeń napotykane przez firmy w ciągu ostatnich 12 miesięcy



88%

badanych firm doświadczyło cyberataku lub wycieku danych w ciągu ostatnich pięciu lat.

Eksperci ds. cyberbezpieczeństwa - odsetek zgadzających się z opiniami



Wśród konsekwencji, których najbardziej obawiają się specjaliści do spraw cyberbezpieczeństwa, są również te dotyczące wizerunku firmy. Co piąty (22%) wskazał, że w wyniku potencjalnego ataku najbardziej obawia się gorszej reputacji marki. Podobny odsetek wskazał na potencjalny spadek zaufania klientów biznesowych oraz detalicznych (w obu przypadkach 23%).

39%

twierdzi, że w ciągu ostatnich 12 miesięcy wzrosła liczba cyberataków na jego firmę

33%

specjalistów ds. cyberbezpieczeństwa obawia się strat finansowych w wyniku cyberataku

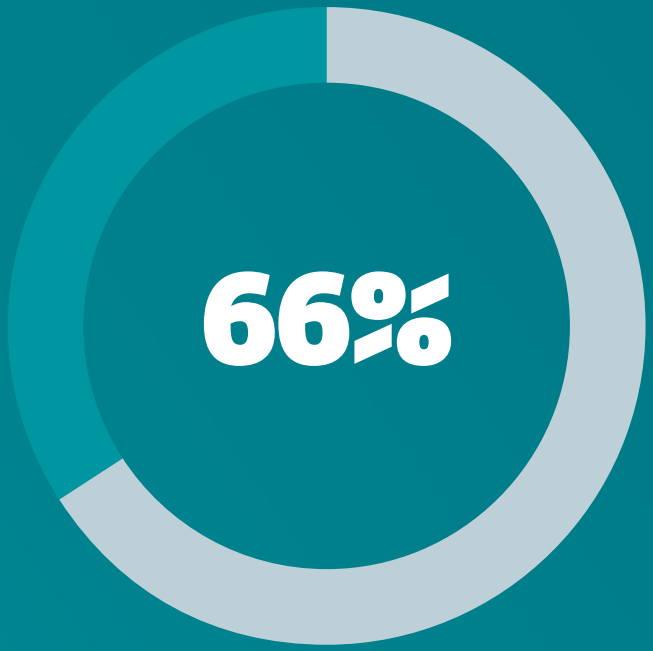
26%

obawia się dodatkowych kosztów technicznych (np. związanych z infrastrukturą)

03

Niebezpieczne zachowania i higiena cyfrowego bezpieczeństwa

JAK PRACOWNICY ŁAMIĄ ZASADY I REAGUJĄ NA RYZYKA



66% pracowników w Polsce badanych przez ESET korzystało ze służbowego sprzętu do celów prywatnych.

Odpowiednia profilaktyka to pierwsza i najważniejsza linia obrony przed cyberatakami. Co na temat dobrych praktyk wiedzą polscy pracownicy, a jaka jest skala ich ryzykownych zachowań? Dlaczego tak chętnie korzystamy ze służbowych urządzeń do celów prywatnych i jakie mogą być tego konsekwencje?

Niebezpieczne zachowania i higiena cyfrowego bezpieczeństwa

Jednym z kluczowych aspektów zapewnienia odpowiedniego poziomu bezpieczeństwa w środowisku firmowym jest zrozumienie i przeciwdziałanie niebezpiecznym zachowaniom użytkowników oraz promowanie higieny cyfrowej. Sprawdziliśmy, jak powszechne są działania i nawyki pracowników, które stanowią zagrożenie oraz w jakim stopniu są oni świadomi dobrych praktyk w zakresie cyberbezpieczeństwa. Ocenie poddaliśmy także skalę wykorzystywania urządzeń służbowych do celów prywatnych.

PRACOWNICY: DOBRE PRAKTYKI BEZPIECZEŃSTWA

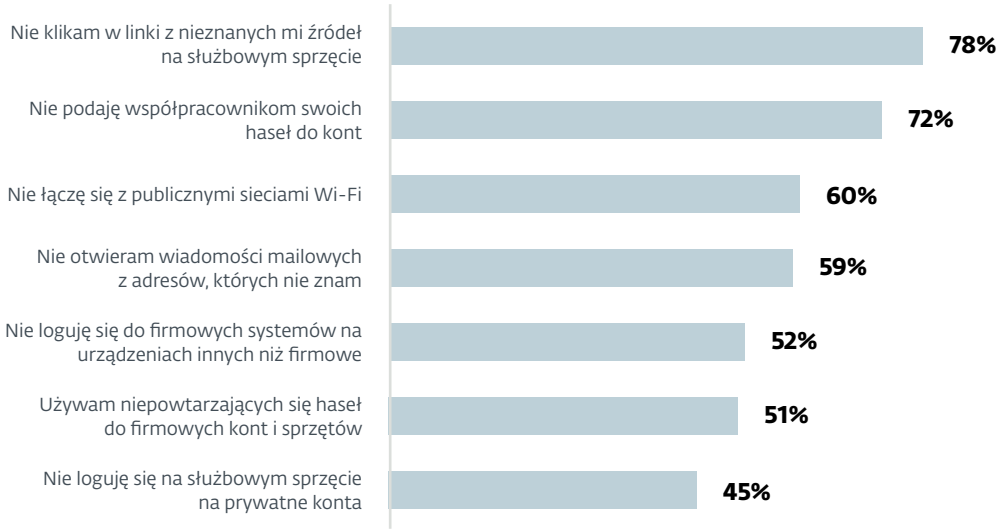
Najlepszym sposobem, aby uniknąć cyberzagrożeń jest wiedza na ich temat i odpowiednia profilaktyka. Istnieje kilka prostych zasad, które funkcjonują od dawna w dyskursie publicznym, wzmacniane zarówno przez różnego rodzaju kampanie jak i wypowiedzi ekspertów. Nie wszystkie jednak są przez pracowników przyswojone i wdrożone w wystarczającym stopniu.

Najczęstszą dobrą praktyką, którą stosuje blisko 8 na 10 pracowników (78%) jest nieklikanie w linki z nieznanych źródeł na służbowym sprzęcie. Niewiele mniej, bo 72% deklaruje, że nie dzieli się swoimi hasłami ze współpracownikami. Publicznych sieci Wi-Fi unika 60% pracowników.

Mimo powszechności wiedzy na temat podstawowych zasad higieny cyberbezpieczeństwa, wciąż dla dużej części pracowników pozostają one obce. To pierwsza linia obrony przed cyberatakami, dlatego na tych zagadnieniach powinna skupić się dalsza edukacja. W tym obszarze wciąż są duże rezerwy.

Eksperci ESET i DAGMA Bezpieczeństwo IT zwracają uwagę, że samoocena pracowników w kwestii unikania niebezpiecznych linków może być nadmiernie optymistyczna i wynikać z różnej interpretacji tego typu zagrożeń. Kluczowa pod tym względem jest wiedza. Popularna porada "nie klikaj w nieznane linki" bywa zbyt mało konkretna, zwłaszcza w świetle coraz bardziej zaawansowanych ataków phishingowych i coraz lepszego odwzorowywania

Odsetek pracowników firm przestrzegających zasad cyberbezpieczeństwa



przez cyberprzestępców wyglądu witryn zaufanych instytucji czy firm. W tym kontekście część z respondentów może wielu takich zdarzeń nie identyfikować z zagrożeniami czy też nieznanymi źródłami - ze względu na bardzo umiejętne podszywanie się pod zaufane źródło.

PRACOWNICY: RYZYKO NA SŁUŻBOWYM SPRZĘCIE

Według badań, blisko 2 na 3 pracowników (65%) podejmuje ryzykowne działania na swoim służbowym sprzęcie. Do najczęstszych należy ignorowanie powiadomień o potrzebie aktualizacji oprogramowania – zadeklarowało to 24% badanych. Z kolei co piąty pracownik zapisuje hasła do swoich kont w miejscach, z których łatwo je wykraść – np. w przeglądarkach, notatkach, mailach czy komunikatorach. Aż 29% badanych przyznało się do posiadania jednego, podobnego hasła do większości swoich służbowych kont.

Powyższe dane pokazują, że edukacja na temat odpowiedniej profilaktyki w zakresie cyberbezpieczeństwa nie jest wystarczająca. Warto również pamiętać, że badani mają tendencję do zawyżania swoich kompetencji i rzeczywista skala niebezpiecznych praktyk może być jeszcze większa.

PRACOWNICY: SŁUŻBOWE, CZYLI CZASEM... PRYWATNE

Mimo faktu, że firmy w swoich regulaminach zabraniają wykorzystywania urządzeń służbowych do celów prywatnych, problemu w tym nie widzi 32% badanych pracowników. Do faktycznego użytkowania firmowego sprzętu do prywatnych zastosowań przyznaje się aż 2/3 pracowników. Wynika to z wygody i dostępności, a wachlarz czynności do jakich są wykorzystywane jest szeroki.

Co drugi polski pracownik korzysta z różnych, niepowtarzających się haseł na służbowych kontach i urządzeniach.

65%

pracowników podejmuje ryzykowne działania na sprzęcie służbowym

24%

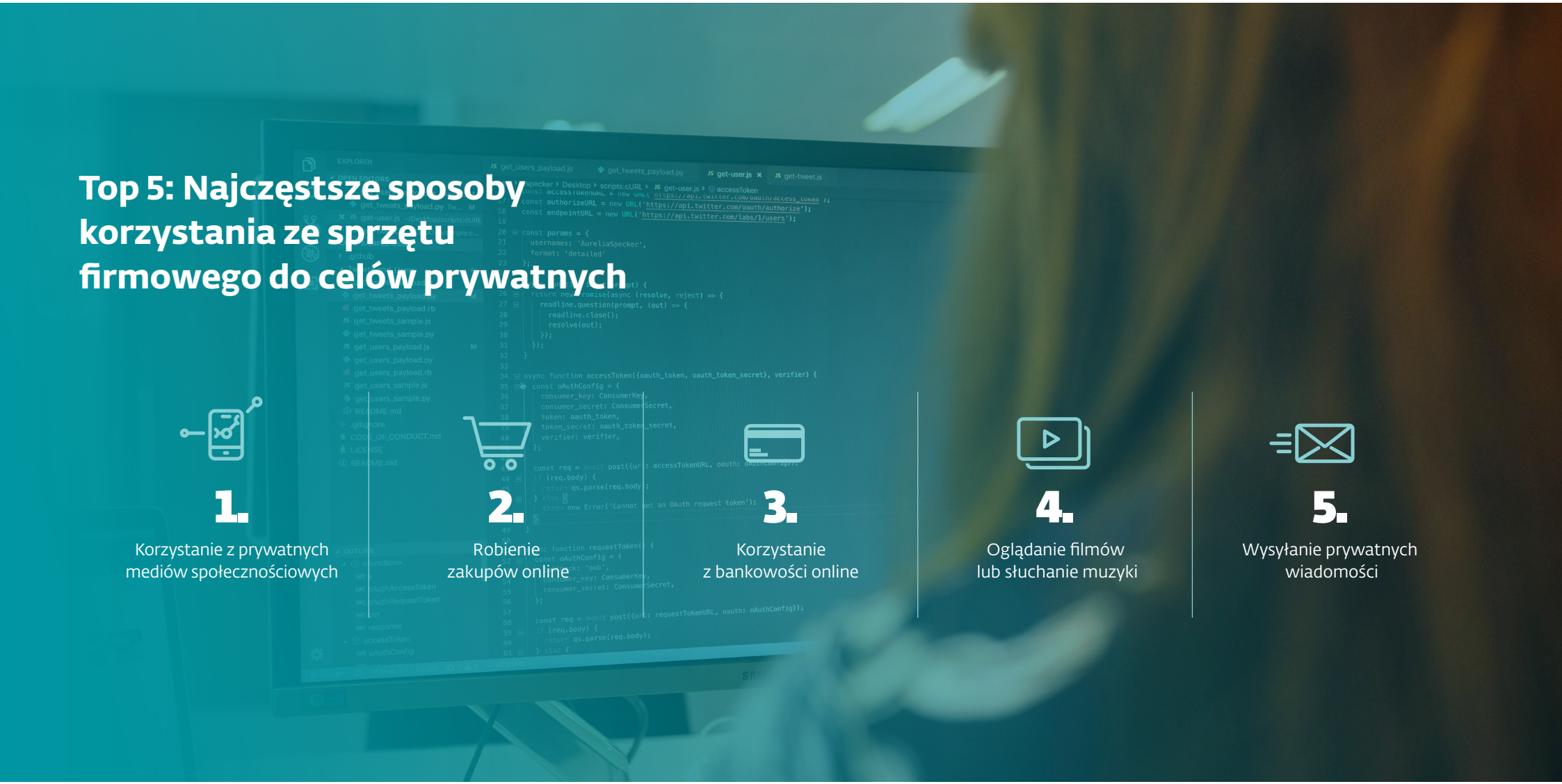
ignoruje powiadomienia o potrzebie aktualizacji oprogramowania

29%

posiada jedno podobne hasło do większości swoich służbowych kont

20%

zapisuje hasła do swoich kont w miejscach, z których łatwo je wykraść – np. w przeglądarkach czy notatkach



Top 5: Najczęstsze sposoby korzystania ze sprzętu firmowego do celów prywatnych

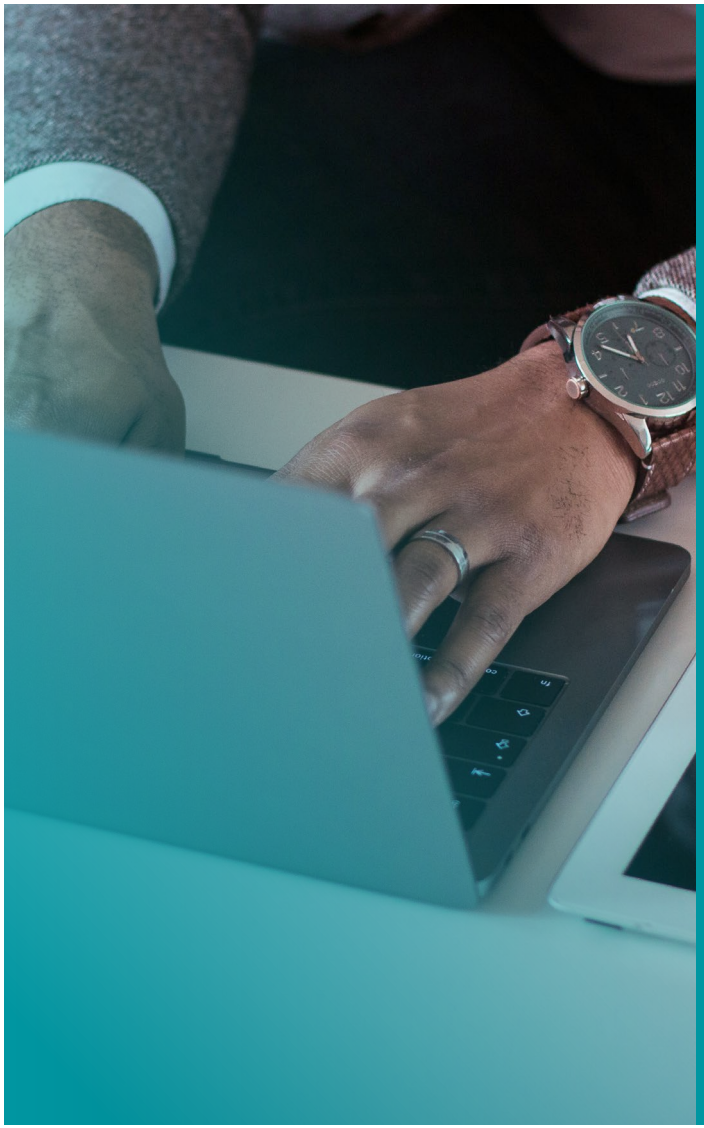
1. Korzystanie z prywatnych mediów społecznościowych

2. Robienie zakupów online

3. Korzystanie z bankowości online

4. Oglądanie filmów lub słuchanie muzyki

5. Wysyłanie prywatnych wiadomości



KAMIL SADKOWSKI
Analityk laboratorium antywirusowego, ESET

Powszechna dostępność laptopów służbowych sprawia, że w wielu przypadkach pracownicy nie inwestują we własne niezależne urządzenia, tylko wykorzystują otrzymany od firm sprzęt do prywatnych celów. Niepokojące są dane, że jednym z najczęstszych sposobów użytkowania sprzętu firmowego do celów prywatnych jest korzystanie przez pracowników z prywatnych mediów społecznościowych, a jednocześnie co piąty pracownik klika na służbowym urządzeniu w linki z nieznanych źródeł.

To właśnie media społecznościowe często wykorzystywane są przez cyberprzestępców do propagowania poprzez linki różnego rodzaju oszustw oraz złośliwego oprogramowania. Może to prowadzić do wycieku tajemnic danego przedsiębiorstwa, w zależności oczywiście od rodzaju pracy danego pracownika, jego pozycji w hierarchii firmowej, a także przechowywanych na urządzeniu służbowym poufnych firmowych dokumentów.

Należy również zwrócić uwagę na sytuację odwrotną – co drugi pracownik loguje się do firmowych systemów z prywatnego sprzętu. Taka praktyka jest o tyle niepokojąca, że urządzenia prywatne na ogół pozbawione są odpowiednich zabezpieczeń, takich jak ograniczenia uprawnień systemowych czy monitoring wszelkich podejrzanych zdarzeń i aktywności w systemie przez zespół ds. bezpieczeństwa.

Wykorzystywanie prywatnego sprzętu do łączenia się z systemami i sieciami firmowymi może okazać się swoistą puszką Pandory dla organizacji, zwłaszcza gdy taki sprzęt użytkuje grono członków rodziny o zróżnicowanych stopniach świadomości zagrożeń internetowych.

04

Kompetencje w obszarze cyfrowego bezpieczeństwa

OCZEKIWANIA KONTRA RZECZYWISTOŚĆ W CODZIENNEJ PRACY ZESPOŁÓW

Mniej niż połowa pracowników deklaruje, że potrafiliby w odpowiednim momencie zareagować na zagrożenie cyberatakiem w miejscu pracy.

W polskich firmach istnieje potrzeba edukacji w zakresie bezpieczeństwa cybernetycznego. Tylko 42% badanych pracowników sądzi, że posiadają wystarczające kompetencje w tym obszarze. Co trzeci pracownik nie ma pewności, komu w firmie zgłosić cyberatak, a tylko połowa – czuje się współodpowiedzialna za unikanie zagrożeń cyberbezpieczeństwa.

Kompetencje w obszarze cyberbezpieczeństwa

Rosnące zaawansowanie technologiczne środowisk pracy sprawia, że dbałość o cyberbezpieczeństwo dawno przestała być wyłącznie kwestią osób bezpośrednio odpowiedzialnych za ten obszar w firmie. Pracodawcy mogą oczekiwać, że pracownicy będą potrafili odpowiednio reagować w przypadku zagrożenia. Z tą gotowością bywa jednak różnie. Mniej niż połowa z badanych przez nas pracowników jest przekonana, że są przygotowani na cyberatak. Choć pewność siebie zespołu w tym względzie jest często wyższa w większych firmach, także w nich jest wiele do zrobienia. Z drugiej strony, na pewien optymizm pozwala fakt, że osoby które realnie spotkały się incydentami bezpieczeństwa rzadko zatajały ten fakt przed pracodawcą.

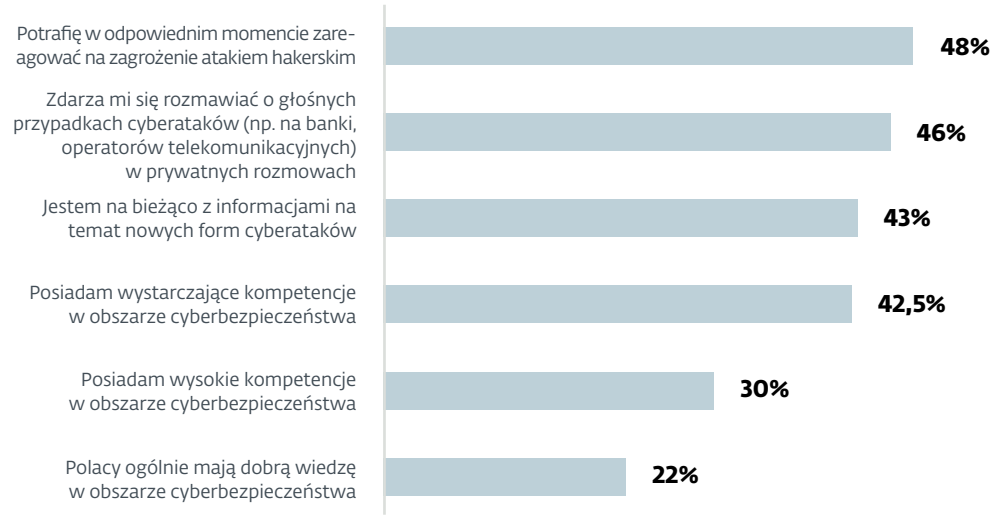
PRACOWNICY: ILE WIEMY O CYBERBEZPIECZEŃSTWIE

Pod względem opinii na temat własnych kompetencji w obszarze cyberbezpieczeństwa badani z grupy ogólnej nie wypadają najlepiej. Zaledwie niecała połowa (48%) respondentów twierdzi, iż potrafi w odpowiednim momencie zareagować na zagrożenie cyberatakiem.

Nieco ponad czterech na dziesięciu badanych pracowników uważa, że posiadają wystarczające kompetencje w obszarze cyberbezpieczeństwa. Wprost wskazuje to na potrzebę ciągłego kształcenia zespołów w tym zakresie. Jak pokazują badania i doświadczenie, duża część wycieków danych spowodowana jest błędami ludzkimi. Swoje kompetencje jako wysokie w tym obszarze ocenia zaledwie 30% pracowników.

Niedostateczna wiedza może wynikać ze stosunkowo niewielkiego zainteresowania tematyką zagrożeń cybernetycznych, które znalazło odbicie w danych. Mniej niż połowa pracowników przyznaje, że zdarza im się rozmawiać ze współpracownikami o głośnych przypadkach cyberataków, takich jak ataki na banki czy operatorów telekomunikacyjnych.

Opinie pracowników o kompetencjach w zakresie cyberbezpieczeństwa. Zgadzający się ze stwierdzeniami



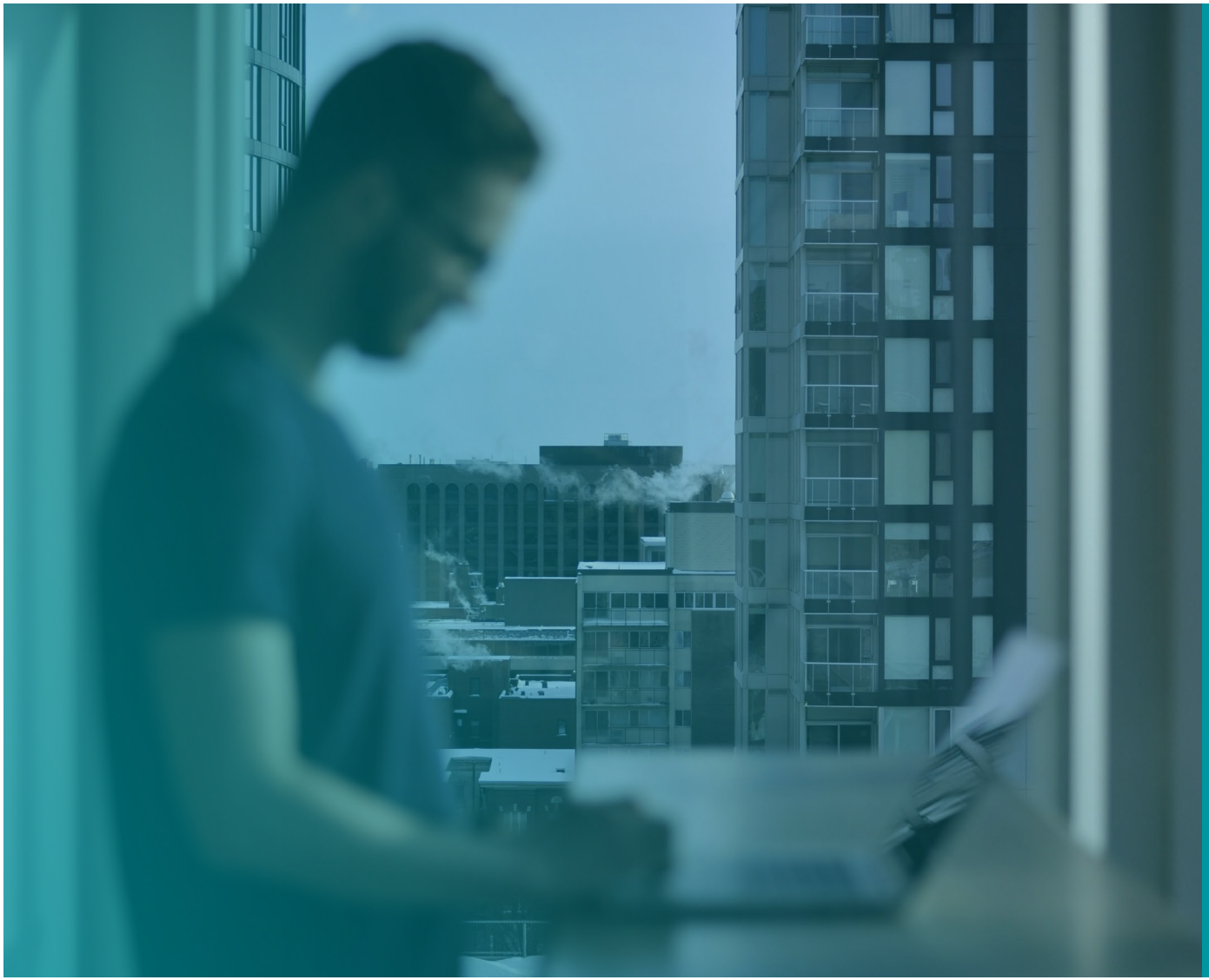
Wyniki te sugerują, że spora część pracowników firm działających w Polsce ma wątpliwości co do swoich umiejętności lub jest przekonanych o ich niedostatecznym poziomie. Szczególnie niepokojące jest to, że wielu badanych nie wierzy, że Polacy mają wystarczającą wiedzę na temat cyberbezpieczeństwa, co może wskazywać na potrzebę większej edukacji i świadomości w tym obszarze.

Co interesujące i warte podkreślenia, pracownicy większych firm zazwyczaj lepiej oceniają swoje umiejętności i wiedzę na temat cyberbezpieczeństwa. 43% badanych zatrudnionych w firmach liczących do 50 osób twierdzi, że potrafi w odpowiednim momencie zareagować na zagrożenie cyberatakiem. Odsetek ten rośnie wraz ze wzrostem wielkości firmy, osiągając 56% w firmach powyżej 1000 pracowników. Podobna tendencja jest widoczna w przypadku oceny posiadania wysokich kompetencji w obszarze cyberbezpieczeństwa. 26% pracowników z najmniejszych firm ocenia się w ten sposób. W największych firmach odsetek ten wynosi już 37%.

Opinie pracowników o kompetencjach w zakresie cyberbezpieczeństwa. Zgadzający się ze stwierdzeniami według rozmiaru firmy (liczba pracowników)

Stwierdzenie	do 50	51–250	251–500	501–1000	>1000
Potrafię w odpowiednim momencie zareagować na zagrożenie atakiem hakerskim	43%	48%	47%	48%	56%
Posiadam wysokie kompetencje w obszarze cyberbezpieczeństwa	26%	27%	29%	35%	37%
Jestem na bieżąco z informacjami na temat nowych form cyberataków	39%	41%	43%	52%	48%

PYT. B2 Zaznacz w jakim stopniu zgadzasz się z poniższymi zdaniami. "W mojej firmie..." N=1032



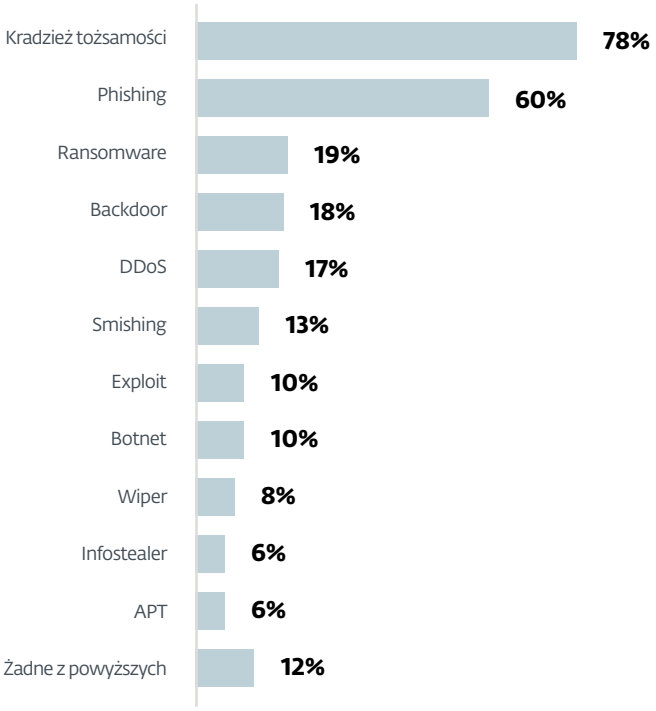
PAWEŁ JUREK
Business Development Director,
DAGMA Bezpieczeństwo IT

A co o zasadach myślą pracownicy w Twojej firmie? W naszym badaniu co czwarty pracownik przyznał, że zasady dotyczące cyberbezpieczeństwa utrudniają mu pracę, a co piąty uznał, że są one po prostu bez sensu. Możemy więc z dużym prawdopodobieństwem założyć, że potencjalnie co piąty pracownik będzie próbował łamać lub obchodzić firmowe zasady. Oznacza to, że każdy taki pracownik jest potencjalnie wewnętrznym zagrożeniem dla organizacji!

To bardzo ważna informacja. Pokazuje lukę i niezrozumienie między tym, co jako standardy wyznaczają specjaliści, a co uznają za potrzebne pracownicy. To napięcie zmniejsza znacząco skuteczność nawet najlepszych zasad. Niestety często to specjaliści mają problem z prostym wytłumaczeniem pracownikom, jaki jest cel wprowadzenia określonych regulacji. A skoro komunikacja z otoczeniem idzie im nie najlepiej, to proponowane przez nich zasady są przez zewnętrzne zespoły kwestionowane.

Dostrzegamy również, że pracownicy z większych przedsiębiorstw są bardziej na bieżąco z informacjami na temat nowych form cyberataków. W firmach do 50 pracowników 39% osób twierdzi, że śledzi takie informacje. W firmach zatrudniających od 501 do 1000 pracowników, odsetek ten wzrasta do 52%, a w tych powyżej 1000 pracowników - nieco spada, bo do 48%, ale nadal przewyższa znacząco wynik dla najmniejszych przedsiębiorstw. Warto zauważyć, że większe firmy prawdopodobnie mają zwykle więcej zasobów na edukację i szkolenia w obszarze cyberbezpieczeństwa, co może tłumaczyć wyższą samoocenę ich pracowników.

Odsetek pracowników znających wskazane terminy z zakresu cyberbezpieczeństwa



PRACOWNICY: UBOGI SŁOWNIK CYBERATAKÓW

Przyglądając się zrozumieniu pojęć dotyczących cyberzagrożeń wśród pracowników, można zauważyć znaczną dysproporcję w znajomości poszczególnych terminów. Największa część respondentów, bo aż 78%, rozumie termin „kradzież tożsamości". Drugim najczęściej rozpoznawanym terminem jest „phishing", który zna 60% badanych. Według danych CERT Polska, w 2023 roku był to najczęściej spotykany rodzaj cyberzagrożenia w kraju (blisko 96 tysięcy zgłoszeń). W kontekście tych danych znajomość tego terminu okazuje się stosunkowo niska.

Jednakże, dalsze wyniki wskazują na znacznie mniejsze zrozumienie innych pojęć związanych z cyberzagrożeniami. Tylko 19% badanych pracowników zna termin „ransomware", a 18% „backdoor". Jeszcze mniej, bo 17%, rozumie pojęcie „DDoS". Termin „smishing" jest znany 13% pracowników, a „exploit" oraz „botnet" po 10%. Co istotne, 12% przyznało, że nie zna żadnego z wymienionych terminów. Oznacza to więc, że w przypadku większości terminów z obszaru bezpieczeństwa cybernetycznego, udział osób znających ich znaczenie w całej populacji nie przekracza 20%.

Kradzież tożsamości

to pojęcie, które zna największy odsetek badanych (78%). Na drugim miejscu jest phishing, jasny dla 60% respondentów. Znajomość pozostałych terminów z zakresu cyberbezpieczeństwa deklaruje nie więcej niż 2 na 10 osób.

Wyniki te wskazują więc na dużą potrzebę większej edukacji i podnoszenia świadomości na temat różnorodnych cyberzagrożeń, poza najbardziej rozpoznawalnymi terminami. Koncentracja na dwóch głównych zagrożeniach sugeruje, że wiele osób może być nieświadomych innych, równie istotnych ryzyk, co może prowadzić do większej podatności na cyberataki.

PRACOWNICY: ZASADY I PROCEDURY

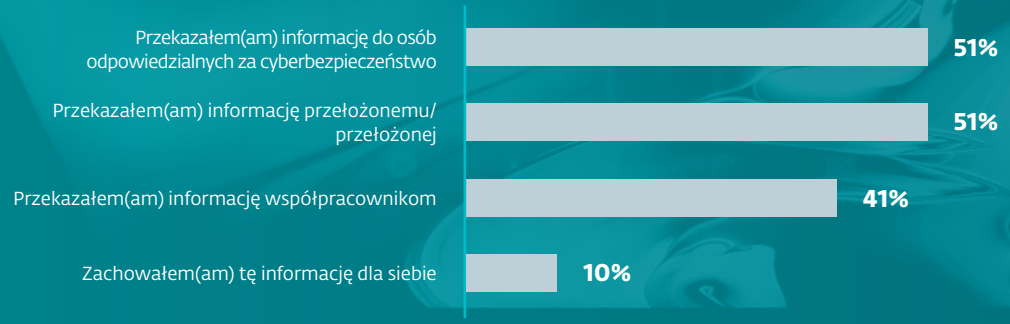
Aż 72% spośród pracowników (nie będących ekspertami w tej dziedzinie) doświadczyło incydentu naruszenia cyberbezpieczeństwa. Analizując dane dotyczące działań podjętych przez pracowników po takim doświadczeniu, można zauważyć, że większość zdecydowała się na przekazanie informacji do osób odpowiedzialnych za ten obszar w organizacji lub swoim przełożonym. Obie te opcje zostały wybrane przez połowę (51%) badanych pracowników. 41% badanych z kolei poinformowało swoich współpracowników o zaistniałej sytuacji.

Stosunkowo pozytywną kwestią jest fakt, że zaledwie 10% pracowników postanowiło zachować informację o incydencie dla siebie - czyli po prostu ją zataić - nie informując nikogo.

PRACOWNICY: WIĘKSZA ŚWIADOMOŚĆ, MNIEJSZE ZROZUMIENIE ZASAD

Większość badanych pracowników ma pewną świadomość procedur związanych z cyberbezpieczeństwem i czuje się współodpowiedzialna za bezpieczeństwo w firmie. Niemniej jednak, istnieje znaczny odsetek osób uważających, że niektóre zasady są zbyt restrykcyjne lub niepraktyczne, co może prowadzić do frustracji i niechęci do ich przestrzegania.

Działania podjęte po doświadczeniu incydentu bezpieczeństwa



10%

Taki odsetek respondentów zachował dla siebie informację o incydencie naruszenia bezpieczeństwa firmy. To niewiele, choć oznacza to, że nadal istnieje pilna potrzeba edukacji w tym zakresie.

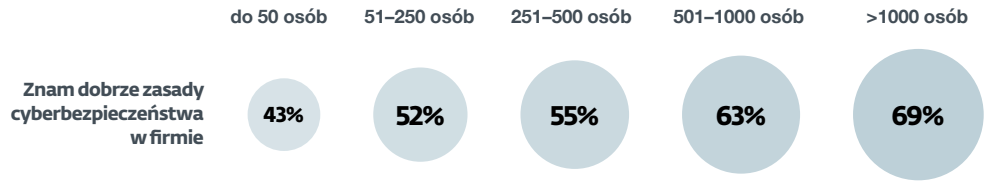
Ocena zasad cyberbezpieczeństwa - pracownicy zgadzający się ze zdaniami

54%

badanych z grupy ogólnej zna zasady cyberbezpieczeństwa wyznaczone przez firmę.

Analizując postrzeganie zasad cyberbezpieczeństwa przez pracowników, którzy nie są ekspertami w tej dziedzinie, można zauważyć kilka istotnych trendów. Po pierwsze, niemal 7 na 10 wie, komu powinno zgłosić cyberatak w swojej firmie, jeśli taki atak nastąpi. Jednakże aż 2 na 10 badanych osób nie posiada takiej wiedzy. Jeśli chodzi o znajomość zasad cyberbezpieczeństwa wyznaczonych w firmie, to zaledwie niewiele ponad połowa respondentów twierdzi, że dobrze je zna.

Pracownicy deklarujący dobrą znajomość firmowych zasad cyberbezpieczeństwa. Odsetek według rozmiaru firmy (liczba pracowników)



Wraz ze wzrostem rozmiaru firmy

rośnie także deklarowany przez jej pracowników poziom znajomości obowiązujących w organizacji zasad cyberbezpieczeństwa.

Około połowa badanych pracowników czuje się współodpowiedzialnych za cyberbezpieczeństwo w swojej firmie. Jednocześnie aż 40% uważa, iż cyberbezpieczeństwo w firmie to głównie sprawa osób, które się na tym znają i odpowiadają za ten obszar. Ponad jedna czwarta (26%) pracowników przyznaje, że niektóre zasady cyberbezpieczeństwa utrudniają im pracę, a 19% uważa, że są one bez sensu.

Warto przy tym podkreślić, że odsetek pracowników, którzy deklarują, że dobrze znają zasady w zakresie cyberbezpieczeństwa stosowane w ich organizacji, rośnie wraz z jej rozmiarem. O ile w firmach zatrudniających do 50 osób odsetek takich badanych wynosi 43%, o tyle w największych przedsiębiorstwach (powyżej tysiąca pracowników) jest to niemal 70%.

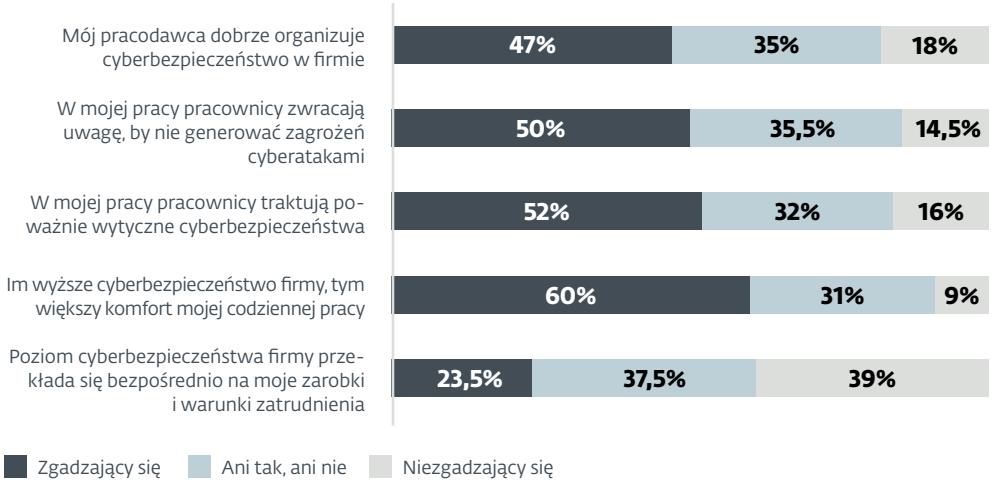
PRACOWNICY: CYBERBEZPIECZEŃSTWO W CODZIENNEJ PRACY

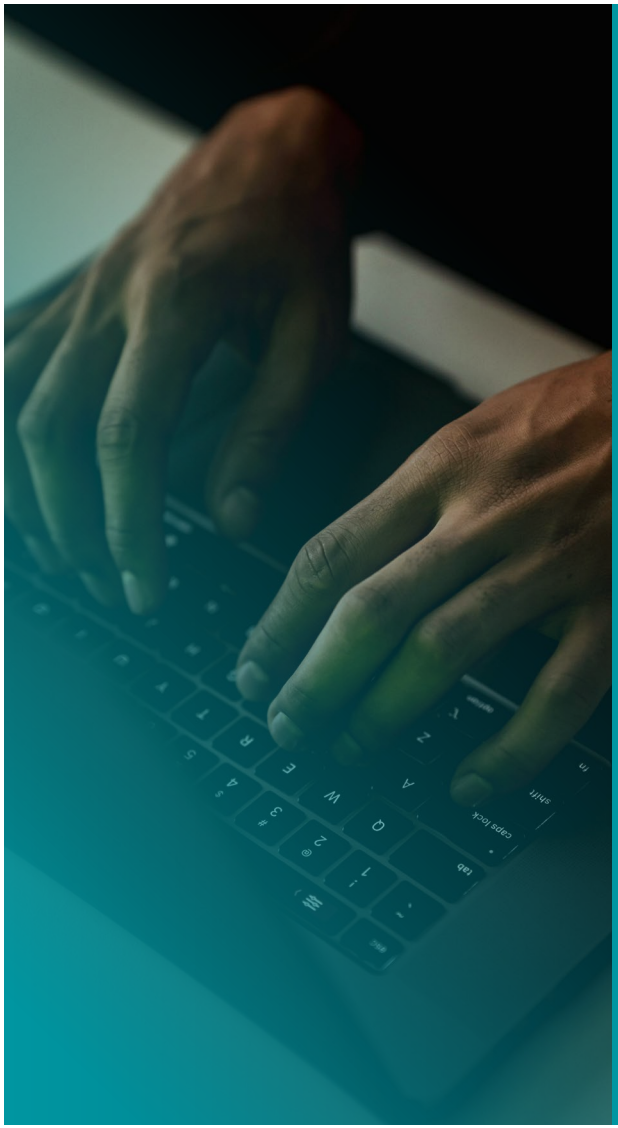
Dane wskazują, że chociaż pracownicy doceniają znaczenie cyberbezpieczeństwa i jego wpływ na komfort codziennej pracy, to jednak istnieją obszary, które wymagają dalszej uwagi. 47% pracowników uważa, że ich pracodawca dobrze organizuje cyberbezpieczeństwo w firmie. Jednakże aż 35% jest niezdecydowanych, co oznacza, że być może osoby te nie są w stanie dokonać stosownej oceny działań podejmowanych przez ich organizację.

Połowa respondentów twierdzi, że w ich firmie zespół zwraca uwagę, by nie stwarzać zagrożeń cyberatakami. 52% stwierdza, że w ich pracy pracownicy traktują poważnie wytyczne dotyczące cyberbezpieczeństwa. Tym bardziej więc firmy powinny opracowywać zasady w tym zakresie i jasno komunikować je swoim zespołom.

Najwyższy odsetek osób zgadzających się dotyczy stwierdzenia, że im wyższy poziom cyberbezpieczeństwa firmy, tym większy jest komfort codziennej pracy. To wyraźnie pokazuje, że pracownicy dostrzegają bezpośredni wpływ cyberbezpieczeństwa na wykonywane przez siebie każdego dnia zadania. Większość pracowników nie widzi jednak bezpośredniego związku między cyberbezpieczeństwem a ich wynagrodzeniem i warunkami zatrudnienia.

Opinie pracowników o znaczeniu cyberbezpieczeństwa w codziennej pracy





BENIAMIN SZCZEPANKIEWICZ
Analityk laboratorium antywirusowego, ESET

Cyberprzestępcy kierują swoje działania coraz celniej, chcąc dotrzeć do kluczowych z ich punktu widzenia zasobów firm: finansów, informacji czy wizerunku. W tym celu próbują wykorzystać najsłabszy element każdego systemu, czyli człowieka. Dlatego często w atakach na pracowników upatrują potencjalnego źródła zysków. Szantaże, kradzież danych, szpiegostwo przemysłowe przynoszą im wymierne korzyści. Odpowiednio przygotowana ochrona systemowa, ale też stosowanie się do zasad bezpieczeństwa informatycznego są kluczowe z punktu widzenia prewencji.

Absolutną podstawą cyberbezpieczeństwa jest świadomość najbardziej typowych zagrożeń oraz sposobów ich uniknięcia. 85% procent spośród badanych osób zadeklarowało, że publiczne sieci Wi-Fi mogą stanowić zagrożenie, a przesyłanie w ten sposób poufnych dokumentów może doprowadzić do ich wycieku. Również korzystanie z ogólnodostępnego sprzętu może zrodzić potencjalne kryzysowe sytuacje, a jest to spotykana praktyka w przypadku osób, które chcą pilnie (często pod presją czasu) zalogować się do firmowych zasobów lub wysłać dokument np. podczas swojego urlopu. Nagłe, kryzysowe sytuacje, mogą prowadzić do obniżenia poziomu procedur bezpieczeństwa przez pracowników. W tym przypadku świadomość potencjalnych kłopotów jest równie wysoka i wynosi 81%. Regularną aktualizację oprogramowania służbowego komputera aż 88% badanych uznaje za sposób zapobiegania cyberatakom. Te liczby mogą napawać optymizmem.

Obok świadomości na poziomie poszczególnych pracowników, bardzo istotnym czynnikiem w sferze cyberbezpieczeństwa firmy jest jednak testowanie procedur i symulacja realnego ataku. Sprawdzenie w praktyce w sytuacji kryzysowej zachowań pracowników i przetestowanie procedur może dać bardzo wiele informacji zwrotnych np. dotyczących tego, gdzie należy szukać usprawnień i czy teoria pokrywa się z praktyką. Z ankiet wynika, że w dużych firmach bezpieczeństwo jest na wyższym poziomie niż w mniejszych, ale to czemu również powinniśmy się przyglądać, to poziom bezpieczeństwa partnerów biznesowych. Kontrahenci z którymi współpracujemy od lat i im ufamy, mogą stać się obiektem ataku, co z kolei może zaburzyć bezpieczeństwo naszej firmy. Warto zachować czujność.

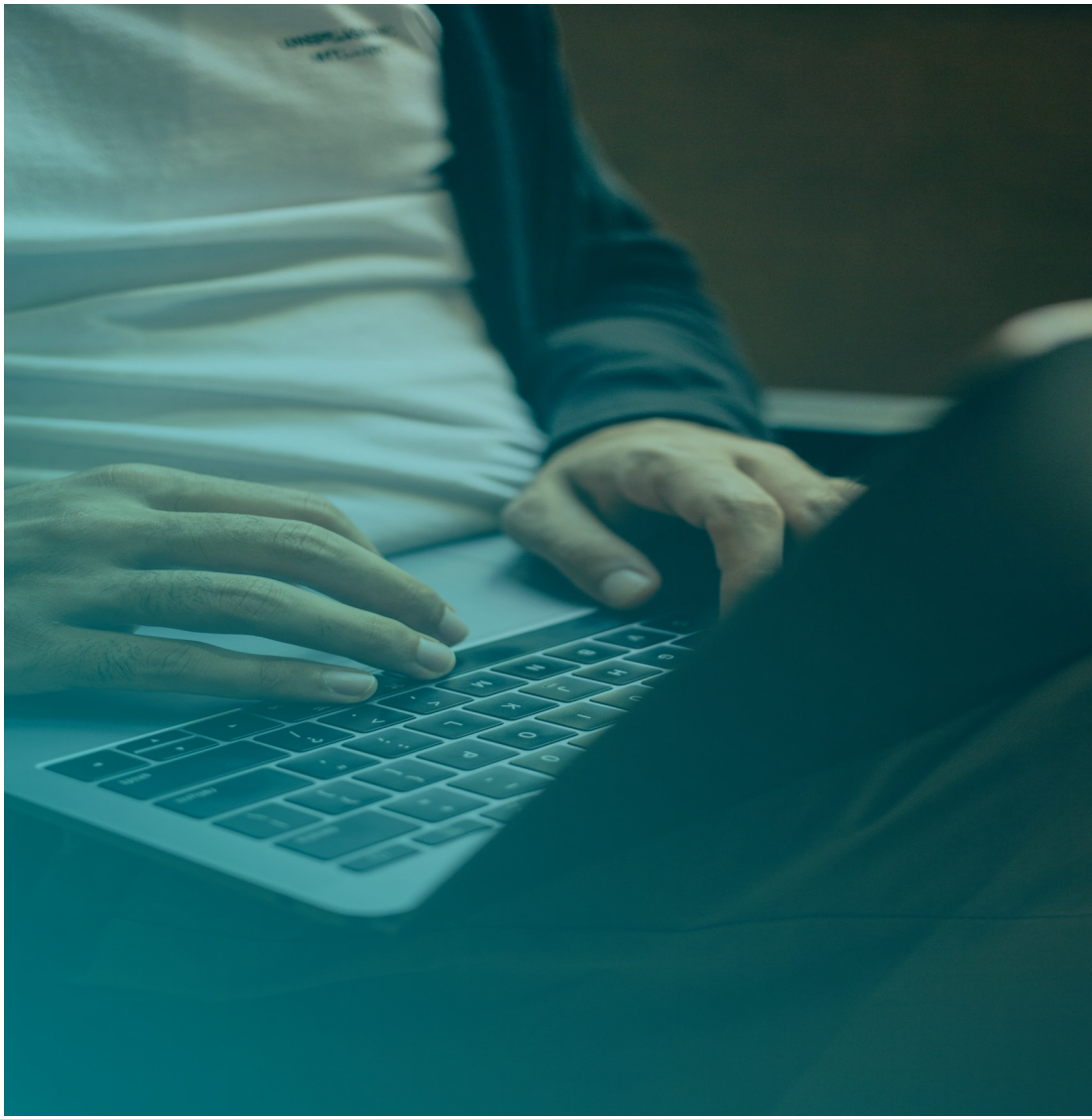
EKSPERCI: WIĘKSZA WIARA W ZABEZPIECZENIA

Analiza opinii ekspertów ds. cyberbezpieczeństwa na temat znaczenia bezpieczeństwa cybernetycznego w organizacji pozwala dojść do wniosku, że konsekwentnie nieco mocniej niż ogół badanych wierzą oni w jakość zabezpieczeń i zasad w ich firmie.

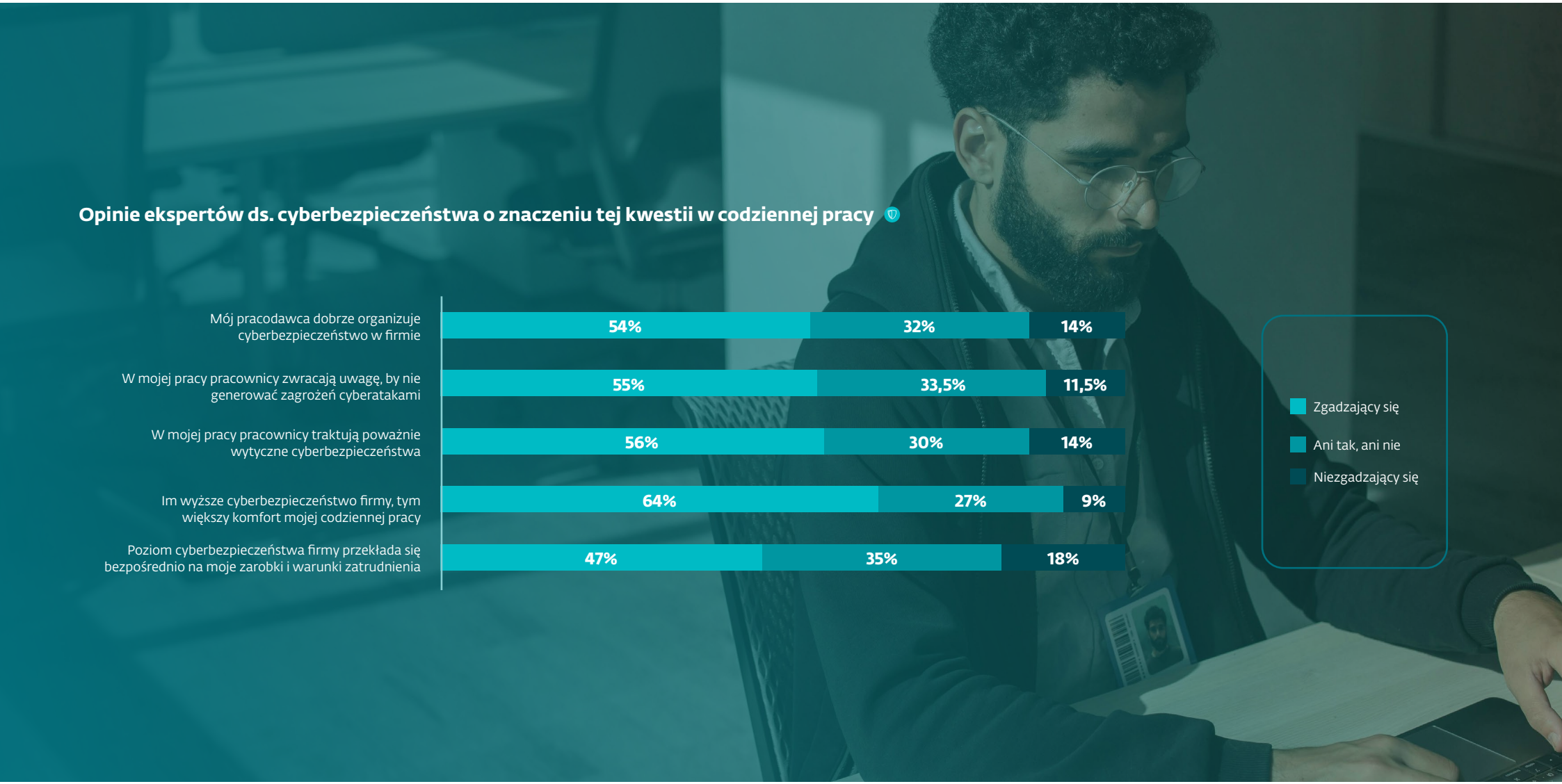
54% ekspertów uważa, że ich pracodawca dobrze organizuje cyberbezpieczeństwo w firmie, co jest nieco wyższym wynikiem niż wśród pozostałych pracowników, z których 47% wyraziło taką opinię. Najwyższy odsetek zgody (64%) dotyczy stwierdzenia, że im wyższe cyberbezpieczeństwo firmy, tym większy komfort codziennej pracy. Tu także wynik jest wyższy niż wśród pozostałych badanych (60%).

Najbardziej zwraca jednak uwagę to, że aż 47% badanych z grupy ekspertów uważa, iż poziom cyberbezpieczeństwa firmy przekłada się bezpośrednio na ich zarobki i warunki zatrudnienia. Jest to znacznie wyższy odsetek w porównaniu do 23,5% reszty badanych, co jednak wydaje się dość zrozumiałe - to nikt inny, ale właśnie badani z tej grupy odpowiadają za bezpieczeństwo w swojej organizacji i jego poziom może mieć istotne przełożenie na wyzwania, z którymi się mierzą, i które mogą przekładać się na finanse.

Wyniki sugerują więc, że eksperci mają bardziej pozytywne postrzeganie działań związanych z cyberbezpieczeństwem w swoich firmach, co może wynikać z ich większej wiedzy i zaangażowania w ten obszar.



Opinie ekspertów ds. cyberbezpieczeństwa o znaczeniu tej kwestii w codziennej pracy



05

Edukacja i luki kompetencyjne

SZKOLENIA W FIRMACH ORAZ ICH PERCEPCJA ZE STRONY PRACOWNIKÓW

52% pracowników w Polsce badanych przez ESET i DAGMA Bezpieczeństwo IT nie przeszło w ciągu ostatnich 5 lat ani jednego szkolenia z cyberbezpieczeństwa w miejscu pracy.

Ochrona przed cyberatakami zaczyna się już na poziomie pracowników, którzy z tą tematyką nie mają teoretycznie nic wspólnego. Kształtowanie wiedzy kadry o cyberbezpieczeństwie powinno być więc wpisane na stałe w politykę firm. Czy tak jednak faktycznie jest?

Edukacja i luki kompetencyjne

Dobrze wyszkoleni pracownicy mogą stanowić skuteczną, pierwszą linię obrony firmy przed cyberatakami. To na ich poziomie może zacząć się, ale też i skończyć wiele prób zainfekowania firmowych urządzeń czy wykradania poufnych danych. Tym ważniejsze jest, by ich szkolić. Jak sobie radzą z tym firmy w praktyce? Szkolenia z cyberbezpieczeństwa zdają się nadal nie być integralnym elementem życia firm, a jeśli się odbywają - zazwyczaj są organizowane rzadko. Widoczne jest, że na pewne ożywienie w tym względzie miały wpływ m.in. przepisy o ochronie danych osobowych. Co ciekawe, zwiększenie intensywności szkoleń powinno interesować firmy z dodatkowego, mniej oczywistego powodu - rosnącej satysfakcji z pracy u osób, które z nich skorzystały.

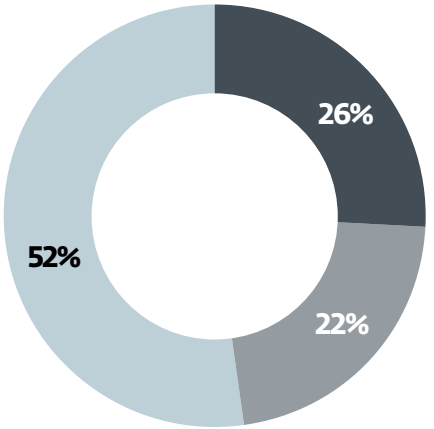
PRACOWNICY: PONAD POŁOWA BEZ SZKOLENIA

Jak wykazało badanie ESET i DAGMA Bezpieczeństwo IT, podejmowanie działań i inwestycji w obszarze edukacji dotyczącej cyberbezpieczeństwa pokrywa się zarówno z oczekiwaniami samych pracowników, jak i ekspertów ds. cyberbezpieczeństwa. Co ważne, w kontekście postępującej cyfryzacji pracy przechodzić je powinni zatrudnieni w niemal wszystkich typach organizacji, niezależnie od ich specjalizacji czy rozmiaru.

W praktyce bywa z tym różnie, a ocena stanu faktycznego zależy od skali oczekiwań. Z jednej strony - według badania szkolenia z cyberbezpieczeństwa stały się ważnym elementem życia wielu zatrudnionych. Z drugiej - nadal stanowią oni mniej, niż połowę pracujących z cyfrowym sprzętem służbowym. Aż 52% badanych pracowników nie wzięło udziału w takim szkoleniu w ciągu ostatnich 5 lat. Kolejne 22% wzięło w nich udział tylko jednokrotnie.

W efekcie okazuje się, że niewiele ponad 1 na 4, bo tylko 26% pracowników zaangażowanych było w naukę cyberbezpieczeństwa w swoim miejscu zatrudnienia więcej, niż raz. Biorąc pod uwagę tempo zmian w cyfrowych środowiskach pracy oraz powstawania nowych zagrożeń cyberbezpieczeństwa, na które narażony jest biznes - to zdecydowanie zbyt niski odsetek. W ciągu ostatnich 5 lat krajobraz cyberzagrożeń znacznie się urozmaicił. Brak możliwie aktualnej wiedzy wśród członków zespołów może narażać firmy na straty finansowe i organizacyjne o bezprecedensowej skali. Dlatego inwestycje w ten obszar w najbliższych latach muszą rosnąć.

Czy uczestniczyłeś(aś) w szkoleniach z cyberbezpieczeństwa w pracy w ostatnich 5 latach?



26%

tylko taki odsetek badanych polskich pracowników w ciągu ostatnich 5 lat przeszedł więcej, niż jedno szkolenie z cyberbezpieczeństwa w swoim miejscu pracy.

Więcej o znaczeniu szkoleń z cyberbezpieczeństwa w planach inwestycyjnych firm przeczytasz w rozdziale "Inwestycja w cyfrowe bezpieczeństwo"

Dane nasuwają wniosek, że skoro ponad połowa pracowników w ogóle się nie szkoli, to w ich postawach tkwić może ryzyko, o czym w badaniu wprost mówią eksperci. Istnieje prawdopodobieństwo, że nieprzeszkolony pracownik może posiadać jedno, wspólne hasło do swoich systemów służbowych i prywatnych. Nie można wykluczyć także, że w ryzykowny sposób korzysta z Internetu lub nawet miesza dwa światy: służbowy i prywatny. Dane pokazują więc, że szkolenia są konieczne, a miernikiem ich skuteczności powinna być następująca po nich zmiana nawyków i lepsze zrozumienie zasad panujących w firmie.

PRACOWNICY: SKALA FIRMY SPRZYJA NABYWANIU WIEDZY

Co ważne, wpływ na dostęp pracowników do szkoleń ma skala biznesu. Duże przedsiębiorstwa zazwyczaj dysponują większymi budżetami na cyberbezpieczeństwo, czyli zarówno na zaawansowane narzędzia, jak i na edukację zespołu. Przekłada się to z kolei na dostępność szerzej zakrojonych programów szkoleniowych obejmujących różne poziomy organizacji.

Wśród pracowników firm w Polsce liczących powyżej 500 osób aż ¾ uczestniczyło w ciągu ostatnich 5 lat w przynajmniej jednym szkoleniu z cyberbezpieczeństwa. Dla porównania, w przedsiębiorstwach małych jest to aż o ponad 30 punktów procentowych mniej, a w przedsiębiorstwach średnich - o około 20 p.p. Odsetek mających możliwość wziąć udział w szkoleniu rośnie więc wraz z rozmiarem firmy do progu 500 pracowników - następnie się stabilizując.

Takie różnice budują kompetencyjne przepaści w dziedzinie cyberbezpieczeństwa między mniejszymi a większymi organizacjami. Rozdźwięk okazuje się głębszy, gdy przyjrzymy się pracownikom uczestniczącym w seriach wydarzeń z zakresu edukacji cyberbezpieczeństwa. Wśród pracowników firm w Polsce liczących powyżej 1000 osób aż 49% brało udział w co najmniej kilku takich szkoleniach na przestrzeni ostatnich lat. Dla porównania, w małych przedsiębiorstwach takich osób było dwukrotnie mniej (24%).

To zrozumiałe, że większe firmy - będąc często narażonymi na większą skalę i różnorodność cyberataków, a także dysponując dużymi budżetami czy zasobami ludzkimi - mają większy potencjał szkoleniowy w zakresie cyberbezpieczeństwa. Jednak w obliczu zróżnicowanej oferty szkoleń dostępnych na rynku, dopasowanej do różnych typów przedsiębiorstw, tak duże dysproporcje w szkoleniu pracowników zaskakują. Wskazują też na bardzo dużą potrzebę edukacji sektora MŚP w zakresie zagrożeń dla biznesu, płynących z niskiego poziomu wiedzy pracowników o potencjalnych atakach i metodach radzenia sobie z nimi.

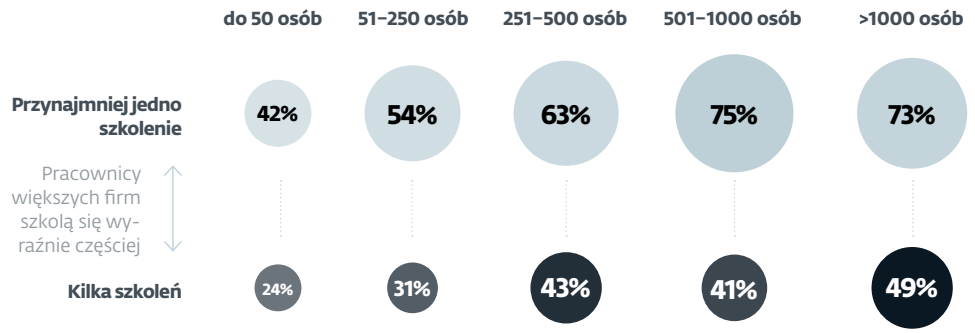
PRACOWNICY: SZKOLENIOWE ABC, CZYLI CZEGO SIĘ UCZY

Zagłębiając się w odpowiedzi osób uczestniczących w szkoleniach zauważyć można, że najczęściej w ich trakcie poruszano w ostatnich latach kilka kwestii. Na czele znajdują się szczegóły dotyczące firmowych zasad cyberbezpieczeństwa - wytycznych tworzonych przez security w organizacji oraz obowiązujących wszystkich pracowników. Brało w nich udział 63% badanych pracowników firm, którym pracodawca zapewnił szkolenie w ciągu ostatnich pięciu lat.

Drugą kategorię tworzą szkolenia dotyczące ochrony danych osobowych i zgodności z regulacjami w tym obszarze (odpowiednio 61% i 59%) - oczywiście związane głównie z obowiązkami wynikającymi z RODO. Trzecią grupę wśród popularnych szkoleń stanowią te związane z codzienną praktyką pracy w cyfrowym środowisku - rozpoznawaniem potencjalnych źródeł ataków phishingowych czy też zapobieganiem wyciekom danych.

Poza czołową piątką tematów szkoleń, w których uczestniczyli pracownicy, znalazły się między innymi zasady bezpiecznego korzystania z poczty elektronicznej, metody tworzenia haseł do kont, podstawy bezpiecznego korzystania z sieci - których uczono około połowę badanych zapraszanych przez pracodawcę na szkolenia. Z kolei około 1/3 miała okazję zapoznać się z zasadami korzystania z programów antywirusowych czy też z podstawami szyfrowania danych.

Pracownicy uczestniczący w szkoleniach z cyberbezpieczeństwa w ciągu ostatnich 5 lat. Odsetek według rozmiaru firmy (liczba pracowników)



PRACOWNICY: CO DOCENIAJĄ W SZKOLENIACH

Najważniejszym celem szkoleń oczywiście zawsze jest nabycie odpowiedniej wiedzy i aż 3 na 4 badanych pracowników zadeklarowało, że szkolenie z zakresu cyberbezpieczeństwa zwiększyło ich świadomość reguł w tym obszarze. Jednak nasze badanie wykazało także inne korzystne efekty dokształcania pracowników w sferze cyfrowej ochrony i profilaktyki. Są one wartościowe zarówno dla samych pracowników, jak i całej firmy.

Szkolenia te mają również wpływ na codzienne obowiązki pracowników. Około połowa przeszkolonych twierdzi, że szkolenie z cyberbezpieczeństwa wpłynęło pozytywnie na ich zadowolenie z pracy. Podobny odsetek zadeklarował większą szybkość wykonywania codziennych obowiązków. Połowa badanych dzięki szkoleniu osiąga lepsze wyniki w pracy. Co ciekawe, w wynikach widać również duży wpływ na wizerunek pracodawcy w oczach pracowników. Aż 63% z nich po szkoleniu z cyberbezpieczeństwa ma o swoim pracodawcy lepszą opinię. Dowodzi to, że wśród zatrudnionych istnieje silna potrzeba poszerzania wiedzy i pracodawcy, którzy na nią odpowiadają mogą liczyć na uznanie. Przy okazji notując u swoich pracowników lepsze wyniki i satysfakcję.

Top 5: Tematy poruszane na firmowych szkoleniach nt. cyberbezpieczeństwa

63%	61%	59%	53%	53%
Firmowe zasady cyberbezpieczeństwa	Ochrona danych osobowych i bezpieczeństwo informacji	Zgodność z regulacjami o ochronie danych	Zapobieganie wyciekom danych	Rozpoznawanie niebezpiecznych źródeł, linków czy kontaktów

Rolę cyberbezpieczeństwa w małych i średnich przedsiębiorstwach podkreślają wyniki badania ESET Digital Security Sentiment, przeprowadzonego w 2023 roku. Już wówczas 59% firm z Polski o tym profilu doświadczyło incydentu związanego z cyberbezpieczeństwem w ciągu 12 miesięcy od badania.

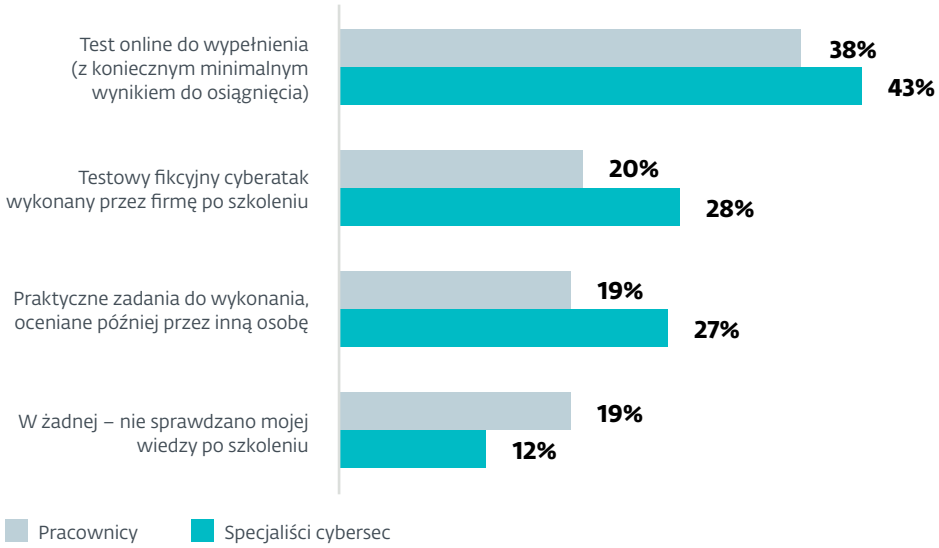
EKSPERCI I PRACOWNICY: UTRWALANIE WIEDZY

Po przyswojeniu wiedzy przychodzi czas na jej sprawdzenie. Zbadaliśmy w jaki sposób testowana jest wiedza z zakresu cyberbezpieczeństwa, po przebytym szkoleniu, zarówno u specjalistów w tej dziedzinie, jak i pozostałych pracowników. Eksperci są sprawdzani częściej pod kątem praktycznym.

Najpopularniejszą metodą jest test online z minimalnym koniecznym do osiągnięcia wynikiem. W ten sposób swoją wiedzę miało okazję przetestować około 4 na 10 (43%) specjalistów od cyberbezpieczeństwa i podobny odsetek pozostałych pracowników (38%).

Do najbardziej miarodajnych metod weryfikowania wiedzy należy zaaranżowanie fikcyjnego cyberataku. Na ten rodzaj testu zdecydowało się jednak stosunkowo mało firm – zaledwie 1 na 5 pracowników miało okazję sprawdzić się w ten sposób i niewiele więcej, bo 28% specjalistów od cyberbezpieczeństwa.

Sposoby testowania wiedzy z zakresu cyberbezpieczeństwa po szkoleniu. Doświadczenia pracowników oraz ekspertów



70%

pracowników oceniło, że szkolenie w zakresie cyberbezpieczeństwa pozytywnie wpłynęło na ich poczucie bezpieczeństwa.

19%

pracowników nie miało okazji sprawdzenia swojej wiedzy po szkoleniu z cyberbezpieczeństwa.

EKSPERCI: CYBERBEZPIECZEŃSTWO OCZAMI SPECJALISTY

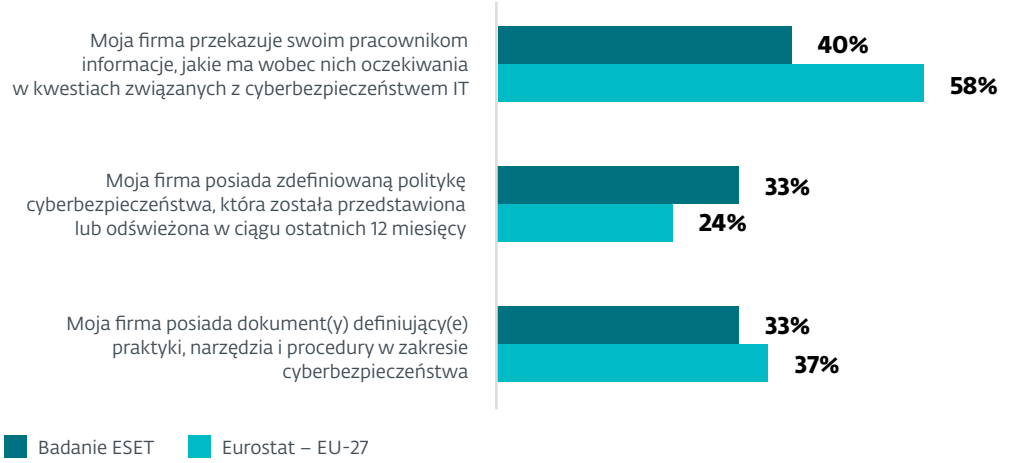
Zapytaliśmy specjalistów od cyberbezpieczeństwa jak oceniają działania ich pracodawców w tym obszarze. Z odpowiedzi wyłania się obraz, który jednoznacznie pokazuje, że pracodawcy mają przed sobą dużo pracy, aby w należyty sposób zadbać o własną kadrę i interesy. Poprawy wymaga zarówno kwestia dokumentacji, narzędzi i procedur, jak i ich dostępność dla zatrudnionych osób. Wyniki porównaliśmy z danymi Eurostatu z 2023 roku.

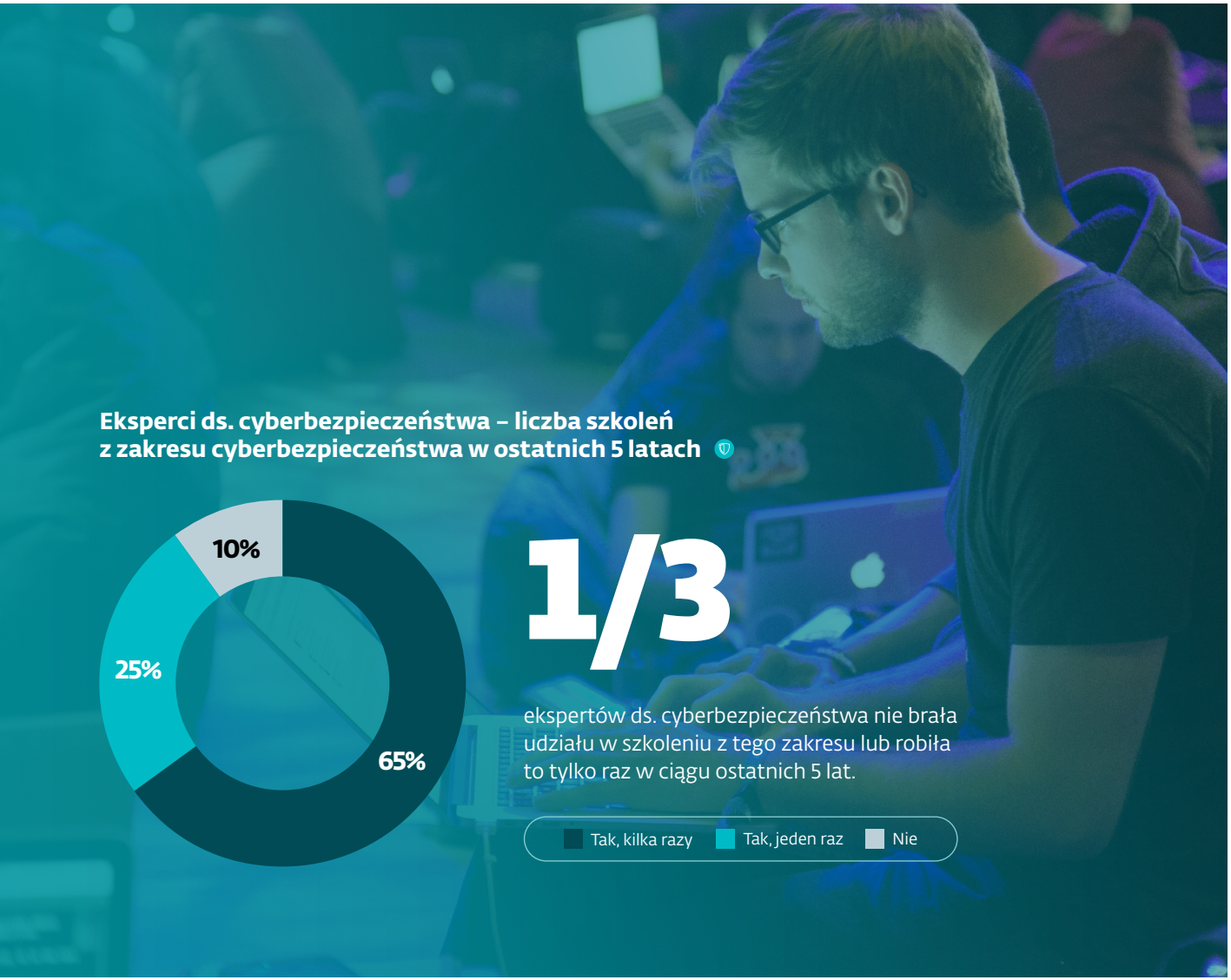
Zaledwie 40% ekspertów uważa, że ich firma przekazuje pracownikom, jakie ma wobec nich oczekiwania w kwestii cyberbezpieczeństwa – w porównaniu do średniej dla Unii Europejskiej (58%) jesteśmy daleko w tyle. Tylko co trzeci specjalista ocenia, że w ich miejscu zatrudnienia istnieje odpowiednia dokumentacja definiująca właściwe praktyki, narzędzia i procedury w tej sferze. Średnia unijna w tym zakresie jest nieco wyższa i wynosi 37%.

67%

specjalistów ds. cyberbezpieczeństwa twierdzi, że ich firma w ciągu ostatniego roku nie zdefiniowała lub nie zaktualizowała wewnętrznej polityki cyfrowego bezpieczeństwa.

Polityka cyberbezpieczeństwa w firmie. Odsetek firm realizujących wskazane praktyki





EKSPERCI: SZKOLENIA TO PODSTAWA

Na sam koniec rozdziału warto podkreślić, że równie ważną grupą szkolonych, co pracownicy z innych linii biznesu, są także sami... specjaliści ds. cyberbezpieczeństwa. Nowo powstające i zyskujące na znaczeniu zagadnienia związane z bezpieczeństwem firm, takie jak ransomware-as-a-service, wykorzystanie sztucznej inteligencji do kampanii phishingowych, ataki na usługi chmurowe czy łańcuchy dostaw wymagają stałej aktualizacji i poszerzania wiedzy.

Analiza wyników badania ESET i DAGMA Bezpieczeństwo IT wskazuje, że świadomi tego zdają się być zarówno sami eksperci ds. cyberbezpieczeństwa, jak i ich pracodawcy. 90% z badanych z tej grupy uczestniczyło w szkoleniach z cyberbezpieczeństwa w ostatnich latach. Warto podkreślić, żę dane te dotyczą tylko kursów w miejscu pracy, nie uwzględniając tych odbywanych w czasie prywatnym. Ponadto 2/3 ekspertów uczestniczyło w miejscu pracy w kilku takich szkoleniach.

Z jednej strony wyniki te wydają się być optymistyczne. Jednak biorąc pod uwagę szybkość rozwoju obszaru cyberbezpieczeństwa w Polsce i na świecie w ostatnich latach - można postrzegać je także inaczej. Wyniki sondażu wskazują bowiem, że nieco ponad 1/3 ekspertów, w obliczu tak dużych zmian, w ciągu 5 lat uczestniczyło w miejscu pracy w jednym szkoleniu - lub nie robiło tego nigdy. Nawet przy założeniu, że część tej grupy nadrabia braki "po godzinach", w czasie wolnym - luki w ich wiedzy mogą zwiększać ryzyko cyberataków w firmie.

KRYSTIAN PASZEK
Cybersecurity Services Manager, DAGMA Bezpieczeństwo IT

Szkolenia związane z cyberbezpieczeństwem powinny być traktowane jako obowiązkowe dla wszystkich pracowników, którzy korzystają z komputera lub rozwiązań cyfrowych i powinny być przeprowadzane cyklicznie. Niewykorzystywana wiedza lubi się ulatniać.

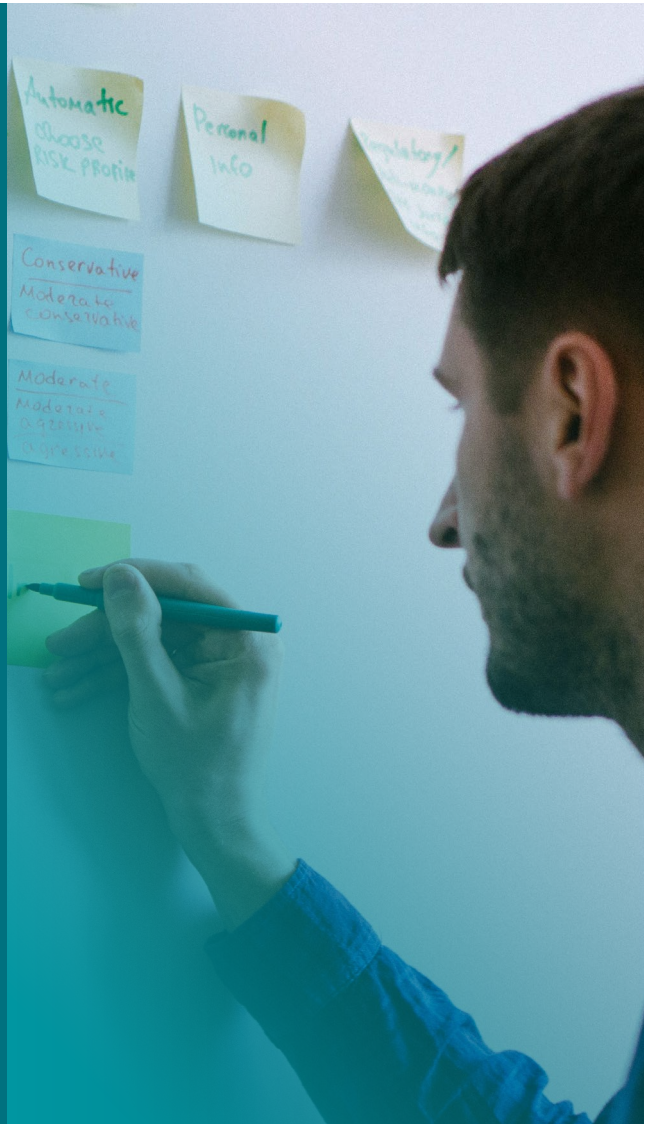
Wykonując różnego rodzaju testy socjotechniczne widzimy, że luki w wiedzy dotyczącej cyberzagrożeń są spore. Brak jakichkolwiek szkoleń z cyberbezpieczeństwa, to niestety jeden z najczęstszych problemów, z którym spotykamy się podczas audytów. Czasami zdarza się, że szkolenie prowadzone jest podczas przyjęcia nowego pracownika razem ze szkoleniem stanowiskowym, lecz zakres tego szkolenia obejmuje tylko podstawowe kwestie i nie jest odpowiednio dopasowany do wiedzy uczestnika, co nie pomaga w budowaniu cyberbezpieczeństwa. Sama edukacja to jednak nie wszystko. Widząc różny poziom wiedzy i zaangażowania osób w danej organizacji, szkolenia należy podzielić na 3 główne rodzaje:

1. Dla kadry zarządzającej – aby miała świadomość istniejących zagrożeń i wpływu na organizację oraz tego w jaki sposób można się chronić, a także co powinno wpłynąć na odpowiednie zrozumienie cyberochrony w zakresie funkcjonowania całego biznesu.

2. Dla wszystkich pracowników – każdy kto ma dostęp do komputera może być potencjalnie zagrożony. Zespół powinien wiedzieć jakie są rodzaje ataków skierowane wobec pracownika i na co zwracać uwagę. Ważną kwestią jest to, że szkolenie poza ciekawym prowadzeniem, powinno zawierać elementy, które dotyczą życia prywatnego, ponieważ w wielu przypadkach jeżeli dana osoba będzie odpowiednio postępować w życiu prywatnym, to adekwatnie zachowa się w sytuacjach służbowych.

3. Dla osób technicznych/zajmujących się zabezpieczeniem infrastruktury – bardziej zaawansowane szkolenia, dedykowane w danej dziedzinie czy to analizowania, projektowania czy też testowania, tak aby zdobytą wiedzę można było wdrożyć do organizacji poprzez realne działania.

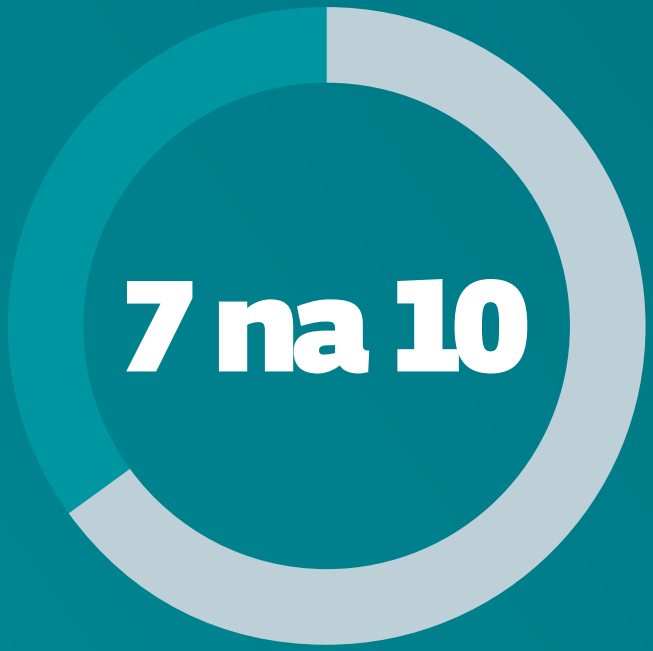
Z doświadczenia wiem, że nawet jeśli szkolenie z cyberbezpieczeństwa będzie ciekawe, a uczestnicy po szkoleniu pełni wiedzy, to po pewnym czasie tylko część z nich będzie się stosować do wytycznych, ponieważ każdy wróci do swoich obowiązków i zapomni o większości poruszanych kwestii. Dlatego warto w ramach regularnych szkoleń wykonywać testy socjotechniczne, które pozwolą uczestnikom spotkać się z realną sytuacją, która mogłaby ich dotknąć od strony hackera. Takie działanie pozwoli nie tylko na zdobycie cennej teoretycznej wiedzy, ale również na praktyczne obycie się z atakami i weryfikację w jakim stopniu jesteśmy podatni na ataki.



06

Narzędzia cyberbezpieczeństwa

ROZWIĄZANIA STOSOWANE W FIRMACH ORAZ MOTYWACJE PRACOWNIKÓW DO DBANIA O CYBERBEZPIECZEŃSTWO



7 na 10 firm w Polsce badanych przez ESET nie przeprowadza regularnie testów bezpieczeństwa teleinformatycznego.

Choć firmy w Polsce sięgają po różnorodne narzędzia cyberbezpieczeństwa - ich wykorzystanie wciąż jest zbyt niskie. Istnieją jednak narzędzia motywacji zespołów, które mogłyby się okazać szczególnie skuteczne w poszerzaniu zaangażowania zespołu w cyberbezpieczeństwo.

Narzędzia cyberbezpieczeństwa

Wyniki raportu "Cyberportret polskiego biznesu" dowodzą, że katalog możliwych zagrożeń cyberbezpieczeństwa dla firm stale się rozszerza. W tym kontekście zastosowanie odpowiednich rozwiązań staje się coraz bardziej palącą kwestią. Dlatego przyjrzeliśmy się zastosowaniu poszczególnych typów narzędzi kontroli cyberbezpieczeństwa. Sprawdziliśmy także jakie działania, podejmowane przez pracodawców, mogą zwiększać zaangażowanie w cyberbezpieczeństwo ze strony kadry pracowniczej.

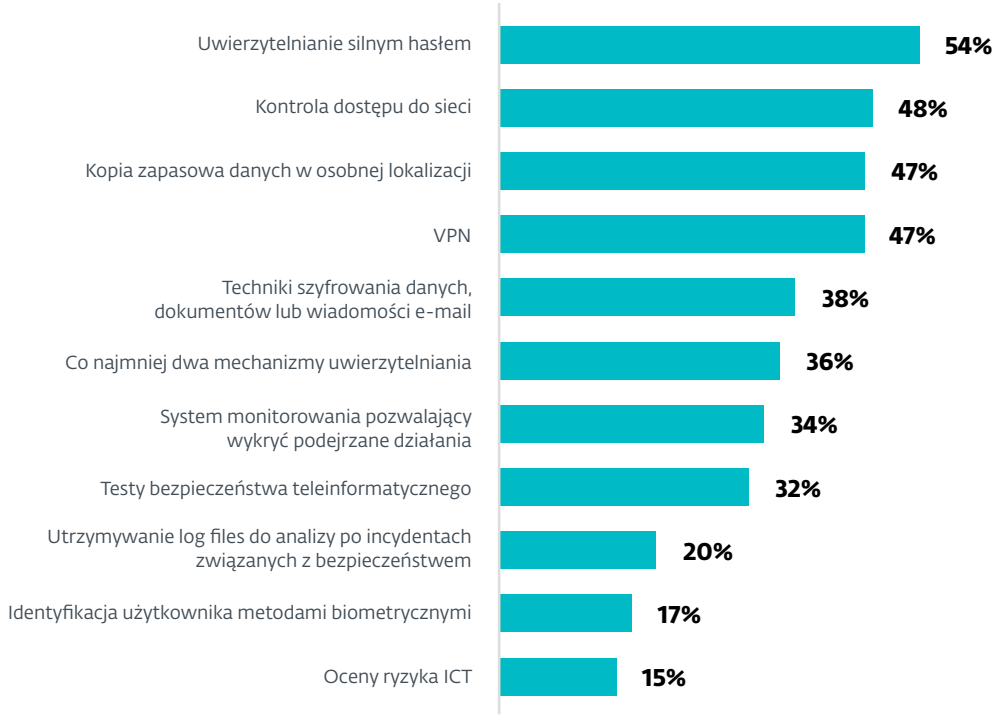
EKSPERCI: WIELE NARZĘDZI KONTROLI I... WIELE OBSZARÓW DO POPRAWY

Badane firmy sięgają po szereg różnorodnych rozwiązań związanych z cyberbezpieczeństwem, na co wskazuje dość równy rozkład popularności narzędzi. Jednocześnie jednak odpowiedzi wskazują, że często działania te skupiają się na firmowej polityce bezpieczeństwa czy ogólnie przyjętych zasadach, a rzadziej - na proaktywnym wykrywaniu i silnej kontroli.

Czołową trójkę narzędzi wspierających cyberbezpieczeństwo wykorzystywanych w firmach tworzą uwierzytelnianie silnym hasłem (54%), kontrola dostępu do sieci (48%) oraz tworzenie kopii zapasowych w osobnej lokalizacji i wykorzystanie sieci VPN (po 47%). Warto zauważyć jednak, że już tylko co trzecia spośród badanych firm sięga po co najmniej dwa mechanizmy uwierzytelniania czy po techniki szyfrowania danych. Również co trzecia organizacja przeprowadza regularne testy bezpieczeństwa teleinformatycznego.

Te wyniki są tym bardziej zaskakujące, że odpowiedzi pochodziły od firm zatrudniających ekspertów ds. cyberbezpieczeństwa - a więc mogących uchodzić za bardziej świadome w tym obszarze. To alarmująca statystyka zważywszy na fakt, że testy te są kluczowe dla proaktywnej identyfikacji luk w zabezpieczeniach. Brak regularnych testów może skutkować pozostawieniem niezidentyfikowanych podatności, które mogą być wykorzystane przez atakujących, prowadząc do kosztownych incydentów bezpieczeństwa. Co więcej, tylko 34% badanych przedsiębiorstw stosuje systemy monitorowania pozwalające wykryć podejrzane działania. Konsekwencje mogą obejmować nie tylko straty finansowe, ale także utratę zaufania klientów i reputacji firmy.

Narzędzia kontroli cyberbezpieczeństwa stosowane przez firmy



32%

zaledwie co trzecia firma badana przez ESET przeprowadza regularne testy bezpieczeństwa teleinformatycznego. Co więcej, tylko 34% z nich stosuje systemy monitorowania pozwalające wykryć proaktywnie podejrzane działania, jak na przykład rozwiązania XDR.

Analizując wyniki badań, eksperci DAGMA Bezpieczeństwo IT i ESET zwracają uwagę, że tylko 15% firm deklaruje dokonywanie oceny ryzyka. W dyrektywie NIS2, której przypisy zaczną obowiązywać w październiku 2024 roku, znalazł się wymóg dla podmiotów ważnych i kluczowych, by zarządzały ryzykiem. Tak niski odsetek wskazuje, że gotowość do dokonywania tego typu ocen może być bardzo niska w stosunku do oczekiwań w tym zakresie ze strony rynku i jego regulatorów.

PRACOWNICY: POZYTYWNA MOTYWACJA BARDZIEJ SKUTECZNA

Różnorodne formy mierzenia wiedzy i śledzenia aktywności są koniecznym oraz skutecznym komponentem polityki cyberbezpieczeństwa. Jednak w budowie świadomości wśród pracowników szczególnie skuteczne mogą być rozwiązania szkoleniowe wzmacniające ich na rynku pracy, a także gratyfikacje i grywalizacja, napędzające kulturę zaangażowania. Z kolei nadmiernie podkreślana kontrola lub mechanizmy karania mogą działać na zespół demotywująco.

Które kwestie miałyby realną szansę zwiększyć osobiste zaangażowanie pracowników w zachowanie cyberbezpieczeństwa w firmie? Jak się okazuje, kluczowymi motywatorami mogą być zarówno działania skierowane na rozwój kompetencji, jak też związane z benefitami finansowymi oraz pozapłacowymi. Innymi słowy można powiedzieć, że - parafrazując znane w Polsce powiedzenie - w zwiększeniu zaangażowania zespołu w cyberbezpieczeństwo pomocna może być zarówno wędka, jak i ryba. Natomiast z perspektywy pracowników jako znacznie mniej skuteczne prezentują się działania pracodawcy związane z kontrolą oraz wymiernymi karami.

Największy odsetek, bo blisko połowa (46%) pracowników badanych przez ESET i DAGMA Bezpieczeństwo IT, poczułoby się bardziej zmotywowanymi do zaangażowania w cyberbezpieczeństwo, jeśli otrzymaliby dostęp do większej liczby szkoleń. Tuż za nimi (z wynikiem 38%) znalazła się możliwość zdobycia przez pracowników certyfikatów potwierdzających nabytą wiedzę. Obie kwestie wpisują się w wyżej wymieniony wątek rozwoju kompetencji.

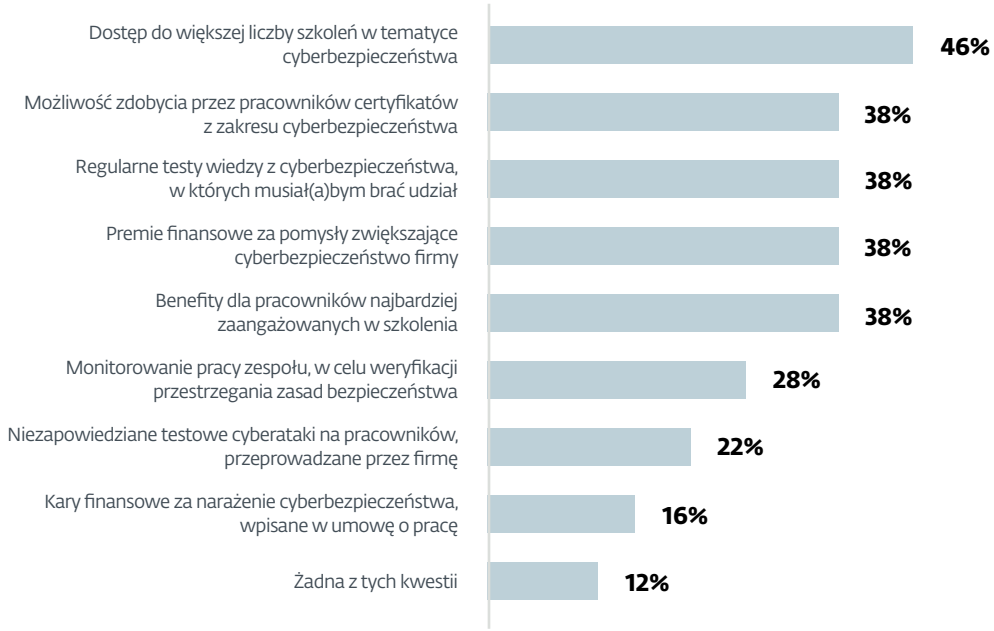
59%

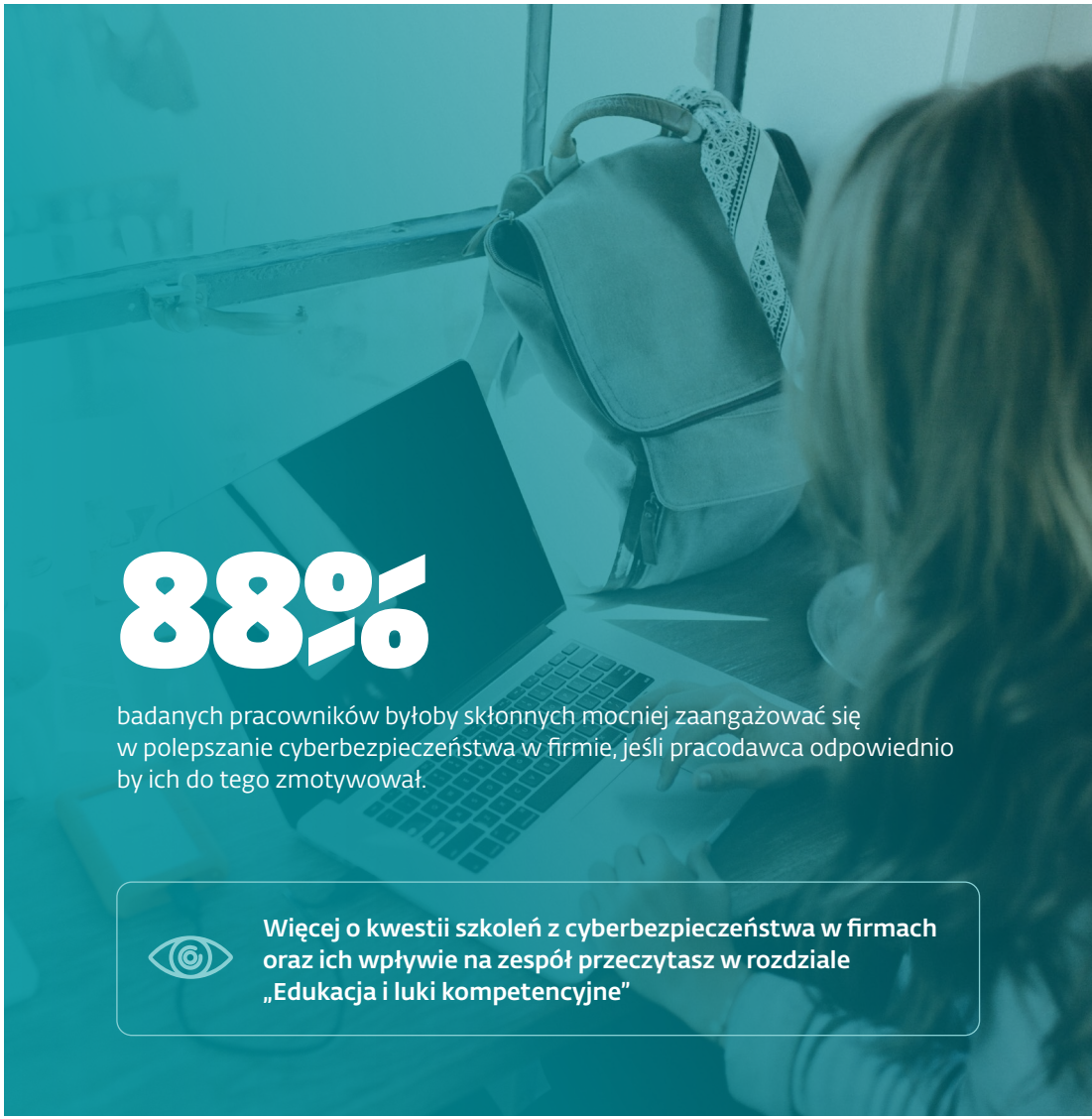
Tylko 59% badanych polskich firm deklaruje, że używa oprogramowania antywirusowego. Oznacza to duże zagrożenie dla ponad 1/3 przedsiębiorstw.

O znaczeniu kwestii finansowych i benefitów świadczy natomiast, że blisko 4 na 10 pracowników (38%) zmotywowałyby premie finansowe dla pomysłodawców inicjatyw, które realnie zwiększyłyby bezpieczeństwo cyfrowe firmy. Taki sam odsetek pracowników zmotywowany zostałby przez różnorodne benefity dla osób najbardziej zaangażowanych w szkolenia.

Natomiast jako mniej zachęcające zostały ocenione działania pracodawcy związane z kontrolą i karami, czyli monitorowanie pracy zespołu pod kątem cyberbezpieczeństwa (28%), niezapowiedziane testowe cyberataki na sprzęt pracowników (22%) czy kary finansowe wpisywane w umowy o pracę (16%). Na tym tle pozytywnie wyróżniają się regularne testy wiedzy z cyberbezpieczeństwa (38%) - czyli formy mierzenia wiedzy, które nie kojarzyły się badanym z zagrożeniem lub negatywnymi konsekwencjami.

Działania, które pracownicy określają jako motywujące do dbałości o cyberbezpieczeństwo firmy





88%

badanych pracowników byłoby skłonnych mocniej zaangażować się w polepszanie cyberbezpieczeństwa w firmie, jeśli pracodawca odpowiednio by ich do tego zmotywował.

Więcej o kwestii szkoleń z cyberbezpieczeństwa w firmach oraz ich wpływie na zespół przeczytasz w rozdziale „Edukacja i luki kompetencyjne”

KAMIL SADKOWSKI
Analityk laboratorium antywirusowego, ESET

Branża cyberbezpieczeństwa oferuje obecnie wachlarz różnego rodzaju narzędzi, eliminujących szereg ryzyk oraz zwiększających bezpieczeństwo firm i pracowników. Dane pokazują jednak, że tylko co trzecia firma deklaruje wykorzystywanie dwuskładnikowego uwierzytelniania – to katastrofalny wynik.

Hasła od wielu lat nie są uznawane za wystarczające zabezpieczenie dostępu do kont i usług. Nawet unikalne i silne hasła mogą wyciec, zostać wyłudzone lub wykradzione przez cyberprzestępców. Duże portale oraz popularne usługi internetowe umożliwiają włączenie, a niekiedy nawet wymuszają dwuskładnikowe uwierzytelnienie. Polskie firmy powinny wziąć z nich przykład.

Podobnie, jedynie co trzecia firma deklaruje wykorzystywanie systemów monitorowania, takich jak EDR, MDR, XDR, umożliwiających wykrywanie i zapobieganie podejrzanym zdarzeniom na urządzeniach firmowych. Takie systemy, w kontekście dynamicznie rozwijającego się krajobrazu cyberzagrożeń, powinny stanowić fundament wielowarstwowej ochrony organizacji, dając możliwość szybkiego wykrywania i reagowania na wszelką złośliwą aktywność, odnotowywaną w sieciach firmowych.

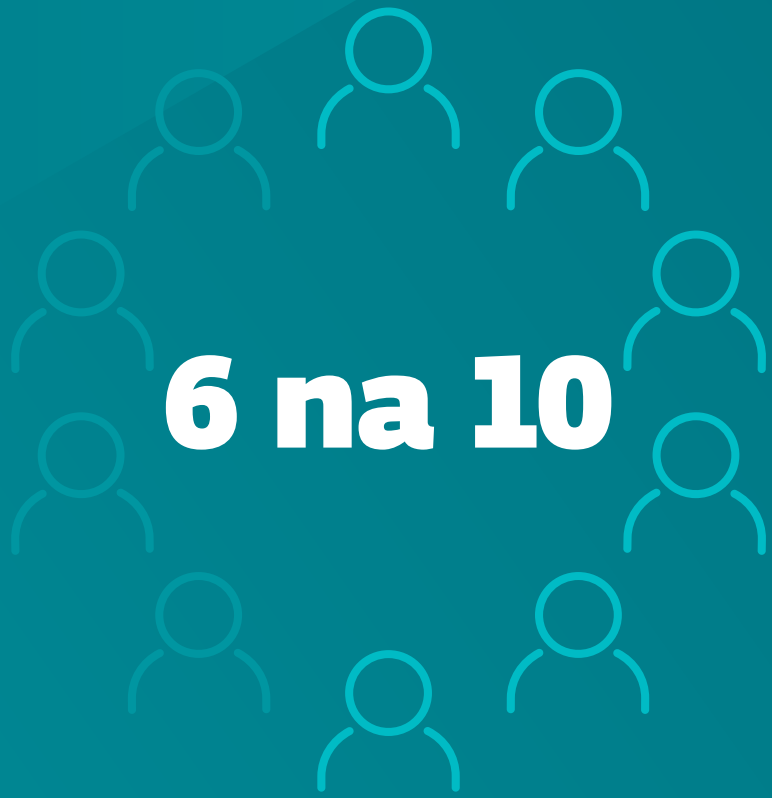
Jedynie około 30% firm deklaruje przeprowadzanie testów penetracyjnych, mających za zadanie odnaleźć ewentualne luki w zabezpieczeniach, które firmy powinny następnie załatać. To również słaby wynik.

Testy penetracyjne powinny być przeprowadzane regularnie w każdej dużej organizacji. W ramach takiego testu wykonywanych jest szereg czynności i etapów analogicznych do tych, stosowanych przez cyberprzestępców. Celem jest odnalezienie jak największej ilości dotkliwych słabości w systemach i sieciach firmowych, zanim zrobią to osoby o złych zamiarach. Nieprzeprowadzanie testów penetracyjnych można porównać do wychodzenia z domu przed nadciągającą burzą bez sprawdzenia, czy mamy zamknięte wszystkie okna.

07

Inwestycje w cyfrowe bezpieczeństwo

BUDŻETY I KLUCZOWE OBSZARY WYDATKÓW



6 na 10 ekspertów od cyberbezpieczeństwa spodziewa się, że firmy nieinwestujące w cyberbezpieczeństwo będą osiągać w bliskiej przyszłości gorsze wyniki finansowe.

W rywalizacji o firmowe budżety cyberbezpieczeństwo nie zawsze znajduje się na szczycie piramidy. Jednak zarządy powinny mieć świadomość, że obszar ten rzutuje nie tylko na odporność na zagrożenie cyfrowe, ale także na realną kondycję biznesową firmy. I faktycznie - nakłady na cyfrowe zabezpieczenia przed atakami zdają się realnie rosnąć, jednak wciąż jest wiele do zrobienia.

Inwestycje w cyfrowe bezpieczeństwo

W większości poruszanych przez nas obszarów około połowa firm (w opinii ekspertów) odnotowywała wzrosty wydatków na cyberbezpieczeństwo. Choć na rynku widoczne są dążenia do optymalizacji wydatków na IT, w obszarze cyberbezpieczeństwa spadki zaliczyła marginalna część firm. Pod kątem priorytetów inwestycyjnych wyróżniają się wydatki na zwiększanie kompetencji pracowników w tym obszarze. Mimo to wciąż są one uznawane jako za niskie przez blisko ⅓ badanych ekspertów. Ogółem wydatki na cyberbezpieczeństwo w 7 na 10 firm nie przekraczają 30% całego budżetu na IT, w blisko połowie - 20%. Jak zauważają sami eksperci w tej dziedzinie - zbyt niskie nakłady na cyfrowe zabezpieczenia mogą znacząco odbijać się na wizerunku i kondycji finansowej biznesu.

EKSPERCI: STABILNE NAKŁADY FINANSOWE

Wzrost nakładów na poszczególne cele związane z bezpieczeństwem w organizacjach w ostatnich dwóch latach był dość równomierny - na pierwszy rzut oka nie wyróżnia się żaden obszar, który otrzymałby szczególnie więcej lub mniej środków finansowych na rozwój.

Średnio około połowa respondentów z grupy ekspertów ds. cyberbezpieczeństwa zgadza się, że w większości obszarów w ciągu ostatnich 24 miesięcy odnotowano wzrost nakładów finansowych. Jednocześnie duży odsetek osób deklarował, że nie widział zmian. Spadki zgłaszali nieliczni respondenci.

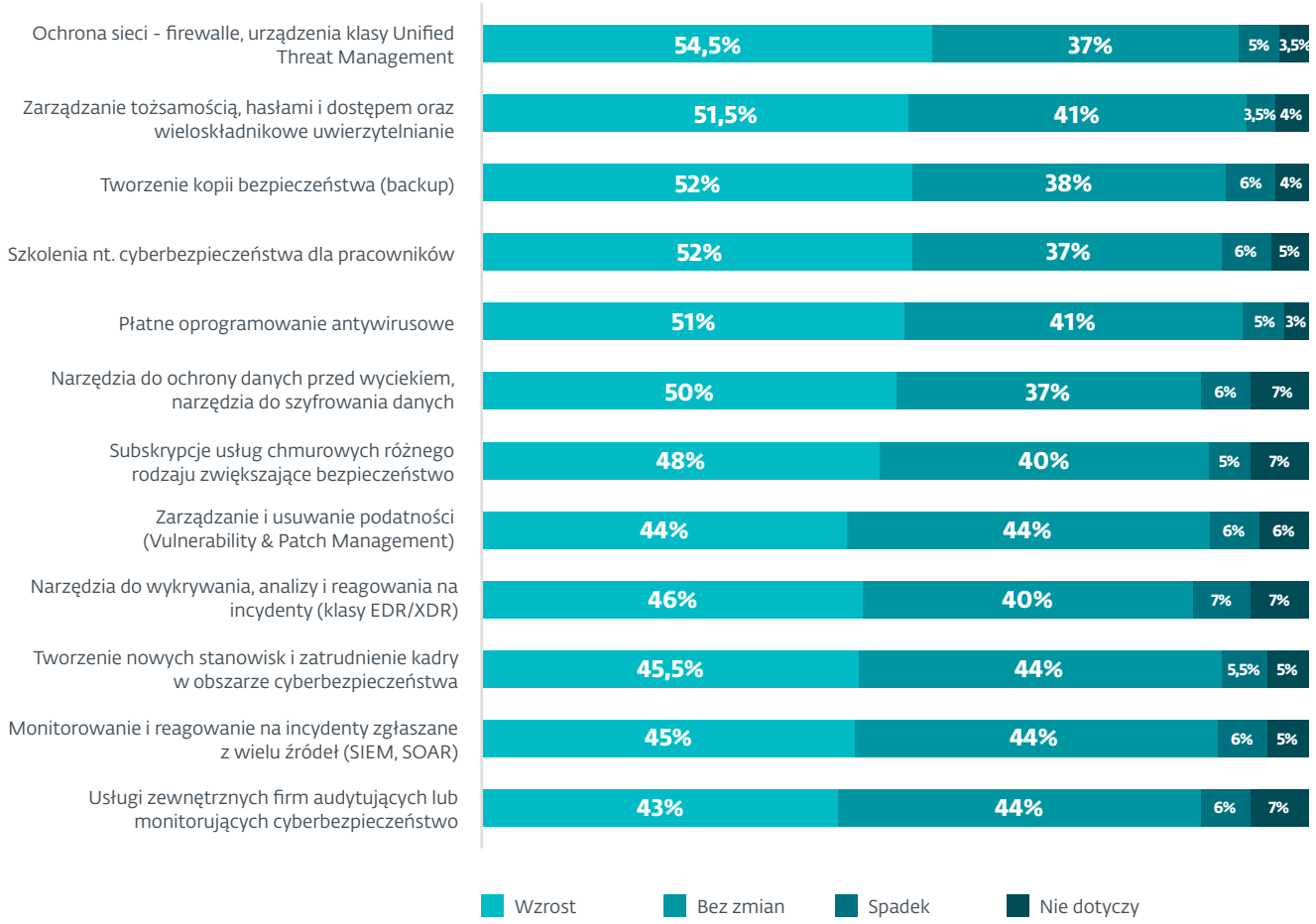
Inaczej było tylko w kilku obszarach (zarządzanie i usuwanie podatności, narzędzia do wykrywania, analizy i reagowania na incydenty (klasy EDR/XDR), tworzenie nowych stanowisk i zatrudnienie kadry w obszarze cyberbezpieczeństwa oraz monitorowanie i reagowanie na incydenty zgłaszane z wielu źródeł) - tam jednak nadal odsetek osób deklarujących wzrost nakładów finansowych oscylował w okolicach 40% na rzecz ekspertów, którzy zgłaszali brak zmian w budżecie. Odsetek osób twierdzących, że obserwują spadki, utrzymywał się na podobnym, bardzo niskim poziomie.

Dane te wskazują na rosnące znaczenie i inwestycje w różne aspekty cyberbezpieczeństwa. Firmy zdają sobie sprawę z rosnących zagrożeń i zwiększają swoje wydatki, aby zapewnić odpowiednie zabezpieczenia i przygotowanie na ewentualne incydenty.

TOP 5 obszarów wymagających pilnych inwestycji i rozwoju według ekspertów ds. cyberbezpieczeństwa

48%	Szkolenia w zakresie cyberbezpieczeństwa
37%	Monitorowanie i reagowanie na incydenty zgłaszane z wielu źródeł (SIEM, SOAR)
36%	Ochrona sieci - firewalle, urządzenia klasy Unified Threat Management
34%	Tworzenie kopii bezpieczeństwa (backup)
33%	Narzędzia do wykrywania, analizy i reagowania na incydenty (klasy EDR/XDR)

Zmiana nakładów firm na cyberbezpieczeństwo w ostatnich dwóch latach



Obszary cyberbezpieczeństwa wymagające najbardziej pilnych inwestycji. Odsetek wskazań wśród ekspertów ds. cyberbezpieczeństwa

Analizując obszary wymagające pilnych inwestycji i rozwoju według ekspertów ds. cyberbezpieczeństwa, możemy zauważyć, że priorytetem są szkolenia nt. cyberbezpieczeństwa dla pracowników, wskazane przez niemal połowę respondentów. To pokazuje, jak istotna jest edukacja i podnoszenie świadomości w zakresie cyberzagrożeń.

Na drugim miejscu znalazło się monitorowanie i reagowanie na incydenty zgłaszane z wielu źródeł (SIEM, SOAR), które wymaga inwestycji według 37% ekspertów. Ochrona sieci, w tym firewalle i urządzenia klasy Unified Threat Management, została wskazana przez 36% badanych.

Tworzenie kopii bezpieczeństwa (backup) jest kolejnym istotnym obszarem, wymagającym inwestycji według 34% badanych. Listę top 5 obszarów zamykają narzędzia do wykrywania, analizy i reagowania na incydenty (klasy EDR/XDR).

Mniej pilne, ale nadal istotne, są subskrypcje usług chmurowych zwiększające bezpieczeństwo (22%), zarządzanie i usuwanie podatności (21%) oraz usługi zewnętrznych firm audytujących lub monitorujących cyberbezpieczeństwo (18%).

Wyniki te sugerują, że eksperci ds. cyberbezpieczeństwa kładą duży nacisk na edukację pracowników oraz na zaawansowane narzędzia i systemy do monitorowania i reagowania na incydenty, co podkreśla rosnące znaczenie kompleksowego podejścia do zarządzania cyberbezpieczeństwem w organizacjach.

Ciekawych wniosków dostarcza porównanie poszczególnych obszarów pod względem wzrostu nakładów na ich rozwój w ciągu ostatnich dwóch lat oraz tego, jaki procent badanych ekspertów ds. cyberbezpieczeństwa wskazał je wśród pięciu najpilniejszych priorytetów.

Blisko 1/2

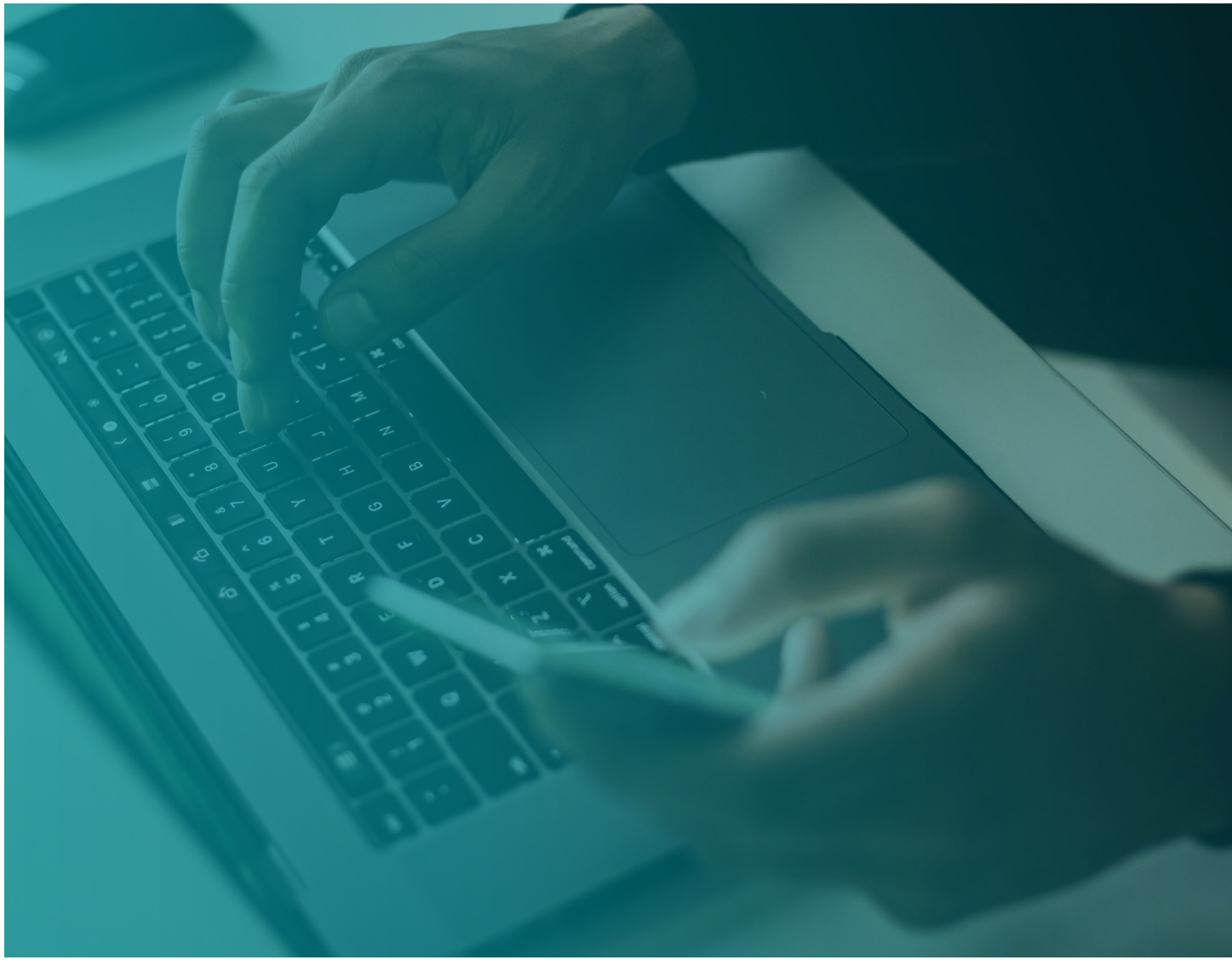
badanych ekspertów ds. cyberbezpieczeństwa wśród priorytetów wymagających nakładów finansowych wymienia szkolenia zespołu w zakresie bezpieczeństwa cybernetycznego.

Największa różnica widoczna jest w obszarze subskrypcji usług chmurowych zwiększających bezpieczeństwo. Niemal połowa ekspertów zgłasza w tym obszarze wzrost nakładów, mimo że tylko 23% uważa go za priorytetowy.

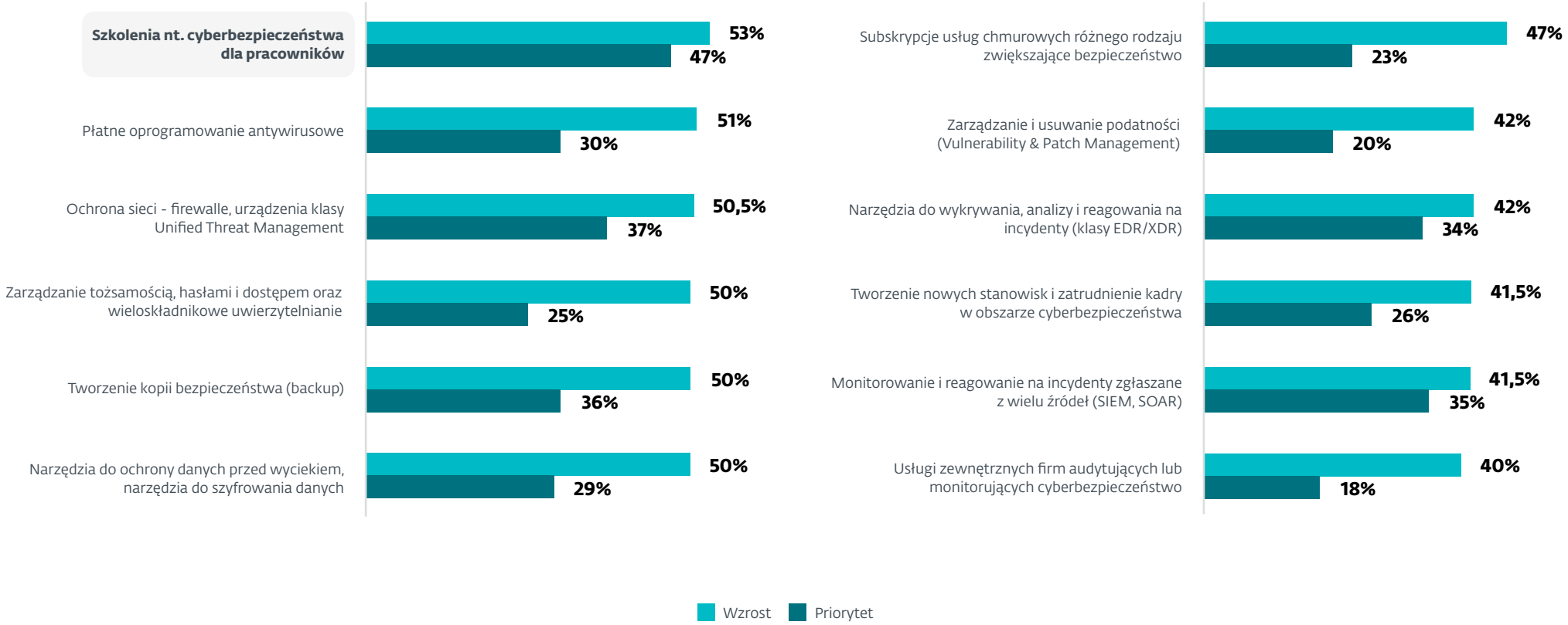
Podobną tendencję zauważyć można w przypadku zarządzania i usuwania podatności oraz usług zewnętrznych firm audytujących lub monitorujących cyberbezpieczeństwo (w obu przypadkach różnica wynosi 22 punkty procentowe).

Wyjątkowo mała różnica natomiast odnotowana została w przypadku szkoleń w zakresie cyberbezpieczeństwa dla pracowników - badani eksperci zgadzają się, że jest to jeden z głównych priorytetów, a firmy znacząco zwiększają nakłady na ten cel.

W większości przypadków widoczne są jednak pewne dysproporcje między deklarowanymi priorytetami a faktycznymi wzrostami nakładów finansowych w kluczowych obszarach cyberbezpieczeństwa, co sugeruje, że niektóre istotne aspekty mogą wymagać większej uwagi i inwestycji w przyszłości.



Inwestycje w cyberbezpieczeństwo. Odsetek firm wskazujących dany obszar jako priorytetowy oraz jako związany z większymi wydatkami w ostatnich latach

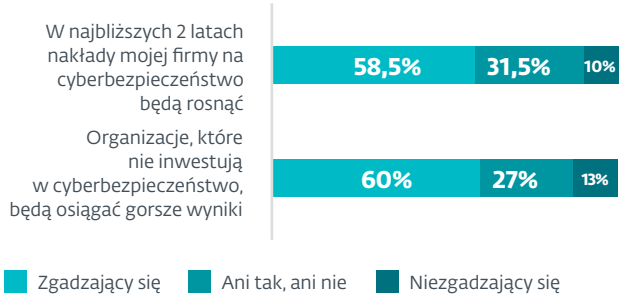


EKSPERCI: DLACZEGO WARTO INWESTOWAĆ

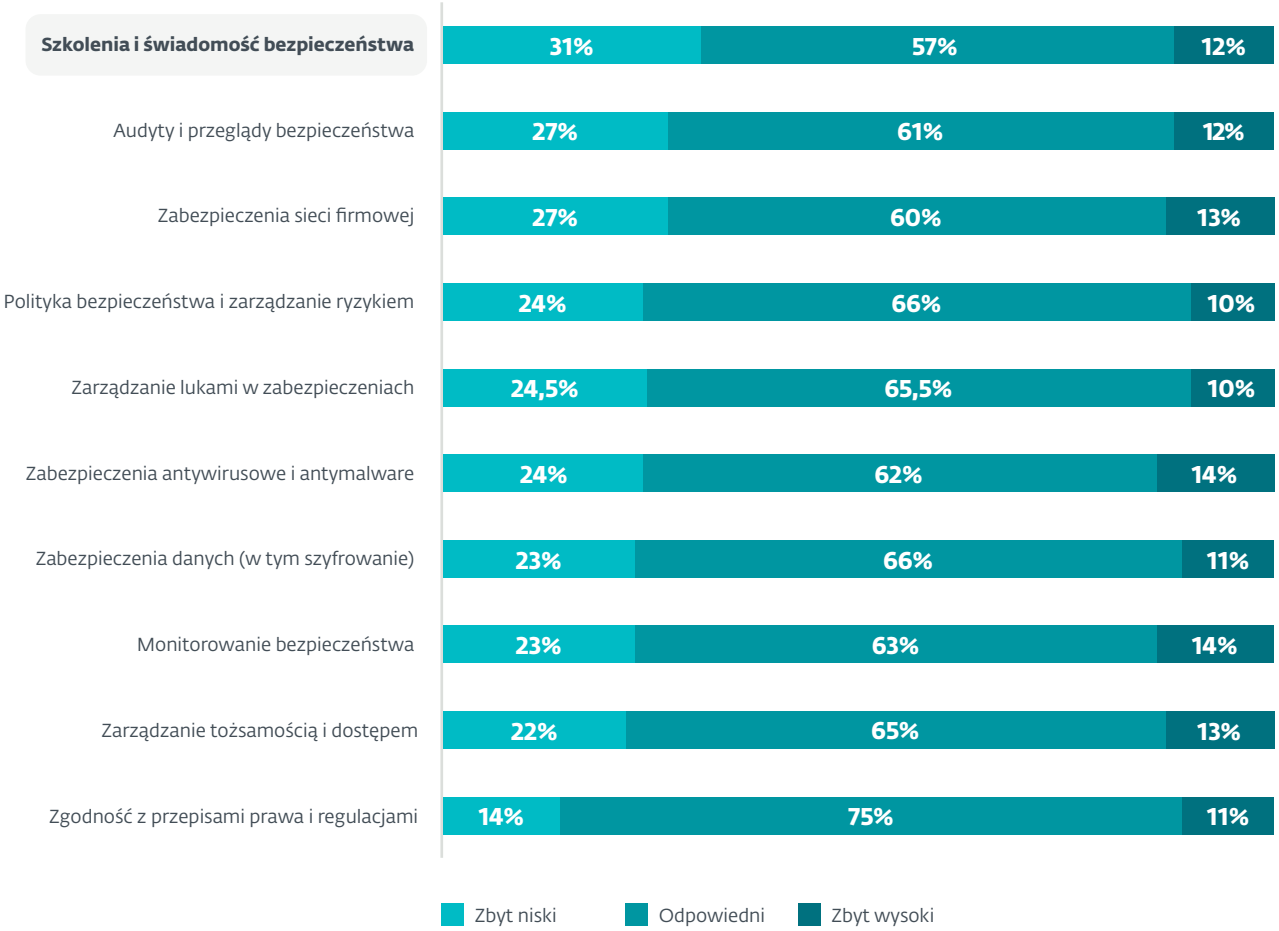
W zdecydowanej większości obszarów badani eksperci ds. cyberbezpieczeństwa uważają budżety przeznaczane na rozwój tych kwestii za istotne. I tutaj jednak znaleźć można pewne ciekawe dane. O ile szkolenia i działania podnoszące świadomość w zakresie cyberbezpieczeństwa wprawdzie otrzymały większe nakłady finansowe w minionych dwóch latach, to jednak w opinii niemal ⅓ badanych ekspertów nie jest to budżet wystarczający. Zdaniem 27% badanych firmy przeznaczają zbyt mało środków na audyty i przeglądy bezpieczeństwa oraz na zabezpieczenia sieci firmowej.

Kolejnymi obszarami, które wymagają uwagi, są: polityka bezpieczeństwa i zarządzanie ryzykiem, zarządzanie lukami w zabezpieczeniach oraz zabezpieczenia antywirusowe i antymalware (wszystkie po około 24%).

Opinie o nakładach firmy na cyberbezpieczeństwo. Odsetek ekspertów



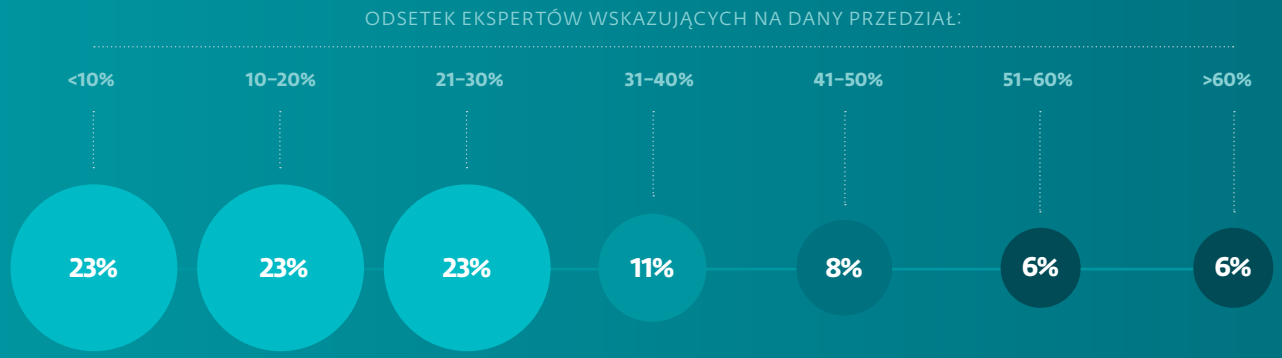
Ocena budżetu przeznaczanego przez firmę na wybrane obszary



31%

badanych ekspertów ds. cyberbezpieczeństwa sądzi, że ich firma wydaje zbyt mało środków na szkolenie zespołu i podnoszenie świadomości w zakresie cyberbezpieczeństwa.

Ocena udziału budżetu na cyberbezpieczeństwo w całkowitym budżecie IT firmy. Odsetek ekspertów wskazujących na dany przedział



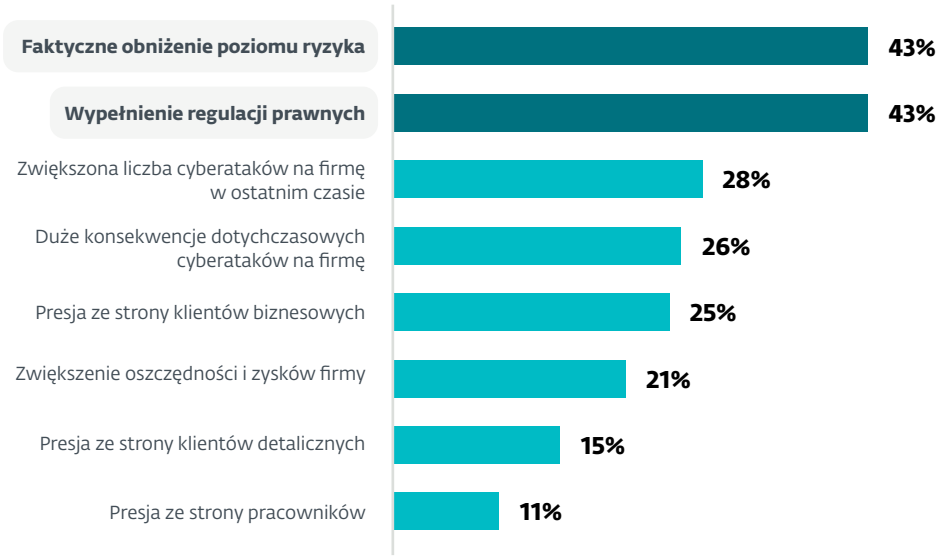
Aż 1 na 4 badanych ekspertów

ocenia, że jego firma przeznacza na cyberbezpieczeństwo mniej niż 10% budżetu IT. W sumie 7 na 10 respondentów sądzi, że odsetek ten wynosi 30% lub mniej.

Najważniejszymi motywacjami do inwestycji są m.in. faktyczne obniżenie poziomu ryzyka oraz wypełnienie regulacji prawnych - oba wskazane przez 43% respondentów. To sugeruje, że zarówno praktyczne, jak i regulacyjne aspekty są istotne przy podejmowaniu decyzji o inwestycjach w cyberbezpieczeństwo.

Kolejnym istotnym argumentem jest zwiększona liczba cyberataków na firmę w ostatnim czasie, wskazana przez 28% ekspertów. Duże konsekwencje dotychczasowych cyberataków na firmę są z kolei czynnikiem wskazanym przez 26% ekspertów ds. cyberbezpieczeństwa. Badanie sugeruje, że zarówno działania prewencyjne, jak i motywy reaktywne odgrywają kluczową rolę w decyzjach dotyczących cyberbezpieczeństwa.

Główne czynniki skłaniające firmy do inwestycji w obszar cyberbezpieczeństwa



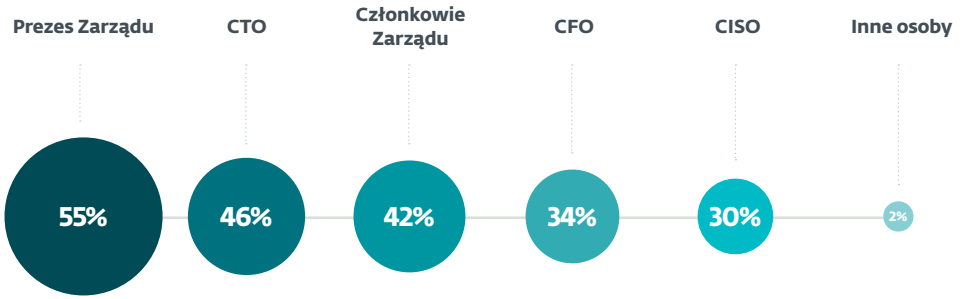
EKSPERCI: ZARZĄD CZY CISO? CZYLI KTO DECYDUJE O BUDŻETACH

A kto według ekspertów ds. cyberbezpieczeństwa ma największy wpływ na decyzje dotyczące budżetu na cyberbezpieczeństwo? Badanie pokazuje, że jest to prezes zarządu wskazany przez 55% respondentów. Na drugim miejscu znajduje się CTO (46%), a następnie członkowie zarządu (42%).

Co ciekawe, zdaniem ekspertów stosunkowo niski jest wpływ na te decyzje CISO (Chief Information Security Officer), który uzyskał tylko 30% wskazań - czyli mniej niż Dyrektor Finansowy (34%). To zaskakujące, biorąc pod uwagę, że CISO jest bezpośrednio odpowiedzialny za bezpieczeństwo informacji w organizacji i powinien odgrywać kluczową rolę w decyzjach budżetowych dotyczących tego obszaru. Prawdopodobnie nie jest to wynik lekceważenia osoby na tym stanowisku a faktu, że w wielu organizacjach takiego stanowiska w strukturach w ogóle nie ma. Może to być kolejny dowód na stosunkowo niski poziom świadomości w obszarze kształtowania procedur bezpieczeństwa i przywiązywania do nich odpowiedniej wagi.

Wyniki te sugerują więc, że decyzje dotyczące budżetu na cyberbezpieczeństwo są głównie w rękach najwyższego kierownictwa, a rola specjalistów bezpośrednio związanych z bezpieczeństwem, takich jak CISO, jest mniejsza niż można by się spodziewać.

Osoby mające największy wpływ na decyzje firmy dotyczące budżetu na cyberbezpieczeństwo. Wskazania ekspertów



EKSPERCI: KLUCZOWE BARIERY INWESTYCJI

Jeśli chodzi o przeszkody w dalszych inwestycjach w cyberbezpieczeństwo, według ekspertów, można zauważyć kilka kluczowych barier, takich jak ograniczenia budżetowe (szczególnie wobec innych priorytetów firm), a także opór ze strony pracowników i niska świadomość wśród personelu oraz liderów organizacji.

Badanie pokazało, że koncentracja firmy na innych wyzwaniach, co utrudnia skupienie się na cyberbezpieczeństwie, jest najczęściej wskazywaną przeszkodą - wybrało ją 33% respondentów. Zaraz za nią znajdują się zbyt wysokie koszty wdrożenia rozwiązań, które zostały wskazane przez 32%. Trzecią w kolejności istotną barierą jest zbyt niski budżet, co zgłosiło 31% specjalistów ds. cyberbezpieczeństwa.

Niechęć pracowników do ścisłych procedur cyberbezpieczeństwa stanowi przeszkodę w oczach 1/4 badanych ekspertów. Dochodzi do tego niska świadomość pracowników i liderów organizacji oraz brak odpowiednich kompetencji w zespole, wskazywane przez 23% respondentów każda. Zwraca to uwagę na potrzebę edukacji i rozwijania umiejętności w zakresie cyberbezpieczeństwa wśród pracowników i kierownictwa. Jedynie 9% ekspertów ds. cyberbezpieczeństwa stwierdziło, że ich firma nie napotyka żadnych z wymienionych przeszkód.

Przeszkody w inwestycjach w cyberbezpieczeństwo wskazywane przez firmy

DAWID ZIĘCINA
Technical Department Director, DAGMA Bezpieczeństwo IT

Budżetowanie i wydatkowanie w obszarze cyberbezpieczeństwa to temat często stymulowany czynnikami innymi niż strategia biznesowa. W odróżnieniu od wydatków na infrastrukturę IT, gdzie po latach cyfryzacji osoby zarządzające firmami widzą korelację pomiędzy rozwojem biznesu, a dobrze działającym środowiskiem informatycznym, tak inwestycje w cyberbezpieczeństwo zyskują na znaczeniu poprzez wpływ czynników zewnętrznych jak np. regulacje na poziomie państwa czy wymagania partnerów biznesowych. Wzrost wydatków na cyberbezpieczeństwo potwierdzają firmy, w których dochodzi do incydentów. Powyższe scenariusze pokazują, że decydentom z jednej strony brakuje nadal przekonania o wpływie cyberodporności na rozwój organizacji, a decyzje o podniesieniu wydatków w tym obszarze podejmują często na podstawie poniesionych strat w wyniku cyberataków. Jest to działanie responsywne, pokazujące niską świadomość o istotności cyberbezpieczeństwa dla danego przedsiębiorstwa czy organizacji.

Wpływ osób odpowiedzialnych za zarządzanie bezpieczeństwem informacji (np. CISO) jest marginalizowany w tworzeniu polityki wydatków firm. Decyzje o kształcie budżetu i priorytetach inwestycyjnych w obszarach bezpieczeństwa IT podejmują nadal głównie osoby zarządzające zespołami administratorów czy działów technicznych (np. CTO), które ukierunkowane są jednak na ciągłość działania i utrzymanie funkcjonujących procesów biznesowych, niż na działania wyprzedzające straty poniesione w wyniku cyberataków.

Co ciekawe w przeprowadzonym badaniu respondenci wskazali, że głównym czynnikiem skłaniającym firmy do inwestycji w obszarze cyberbezpieczeństwa jest chęć faktycznego obniżenia poziomu ryzyka. Wynika z tego, że firmy te mają na tyle wysoką dojrzałość procesów zarządzania w obszarze bezpieczeństwa IT, że realizują zadania związane z szacowaniem ryzyk w organizacji. Potwierdzeniem tego może być wskazanie przez ankietowanych, że obszar związany z nakładami na zgodność z przepisami prawa i regulacjami jest wysoko doinwestowany. Procesy związane z polityką bezpieczeństwa i zarządzaniem ryzyka są również wskazywane jako jeden z lepiej zaopiekowanych budżetowo obszarów.

Najpilniejszym a zarazem ciągle niewystarczająco doinwestowanym obszarem jest budowa świadomości bezpieczeństwa wśród pracowników i osób zarządzających. Dodatkowo obserwowany jest niski poziom wewnętrznej, oddolnej presji osób tworzących organizację na podnoszenie standardów cyberbezpieczeństwa. Zestawiając wszystkie powyższe wnioski można stwierdzić, że osoby odpowiedzialne za cyberbezpieczeństwo w swojej walce o podniesienie istotności tego obszaru w organizacji, powinny sukcesywnie budować mechanizmy ukazujące jaki wpływ ma cyberodporność na kondycję firmy, jej rozwój, jak i konkurencyjność. Budowanie cyberświadomości nie powinno ograniczać się tylko do szkoleń i treningów z rodzajów ataków i sposobów ich wykrywania oraz odpierania. Nacisk na budowanie świadomości o istotności cyberbezpieczeństwa w funkcjonowaniu biznesu i jego efektywności musi być równie mocny.

08

RODO w praktyce. Bilans przed NIS2

REAKCJE NA WYMOGI W OBSZARZE CYBERBEZPIECZEŃSTWA

32% firm badanych przez ESET i DAGMA Bezpieczeństwo IT nadal nie jest pewnych, czy odpowiednio dostosowały się do wymagań wynikających z przepisów RODO – sześć lat po ich wejściu w życie.

Regulacje prawne to istotny kontekst dla cyberbezpieczeństwa w Polsce i Europie. Przepisy wspierające ochronę danych i reakcje na cyberataki potrafią być trudne do implementacji. Można o tym się przekonać, śledząc jakość stosowania się firm do wymogów RODO. Wejście w życie dyrektywy NIS2 dla wielu objętych nią firm będzie stanowić jeszcze większą rewolucję.

RODO w praktyce. Bilans przed NIS2

RODO, a już wkrótce także NIS2, to regulacje stanowiące kluczowe elementy europejskiego krajobrazu prawnego w zakresie ochrony danych i cyberbezpieczeństwa w 2024 roku. Obowiązujące od lat RODO pokazuje, jak duże wyzwania wiążą się z realnym wdrażaniem praktyk cyberbezpieczeństwa w firmach o różnym rozmiarze. Z kolei NIS2 - choć dotyczy węższego grona firm - dobrze odzwierciedla poszerzającą się skalę obszarów, które są narażone na cyberataki. Badanie ESET i DAGMA Bezpieczeństwo IT pokazuje, że ochrona danych osobowych wciąż stanowi dla części firm wyzwanie, a z kolei nowe regulacje przynoszą sporą niepewność.

KRAJOBRAZ PO RODO. NIS2 NA HORYZONCIE

RODO (Rozporządzenie Ogólne o Ochronie Danych) jest stosowane od 25 maja 2018, nakładając na firmy obowiązki związane z przetwarzaniem i ochroną danych osobowych. Te regulacje przed sześcioma laty wzbudziły duże zamieszanie w firmach w Polsce. Proces dostosowania się do nich wymagał znacznych zmian organizacyjnych, technologicznych i proceduralnych, co stanowiło wyzwanie, zwłaszcza dla mniejszych podmiotów.

Z kolei NIS2 (Network and Information Systems Directive) zacznie obowiązywać w Unii Europejskiej w październiku 2024 - kiedy to wszystkie kraje członkowskie UE powinny zaimplementować tę dyrektywę w swoim systemie prawnym. Obecne dyskusje o NIS2 przypominają w dużym stopniu te, które toczyły się kontekście RODO - cechując się dużą niepewnością firm co do poziomu dostosowania, a także obawami o łamanie nowych przepisów. Dyrektywa rozszerzy wymagania dotyczące cyberbezpieczeństwa w wielu firmach, w tym związane z odpowiednimi środkami technicznymi czy zgłaszaniem incydentów bezpieczeństwa.

NIS2 obejmie m.in. operatorów usług kluczowych (m.in. energetyka, transport, bankowość, infrastruktura rynków finansowych, zdrowie, wodociągi), sklepy online i wiele innych firm działających w sektorze usług cyfrowych. Zmiany dotyczą również firm z sektora MSP, które wcześniej były wyłączone z regulacji NIS1. Będą musiały je wprowadzić przedsiębiorstwa, które zatrudniają ponad 50 pracowników lub osiągają roczny obrót przekraczający 10 milionów euro.

Pojawienie się NIS2 to kolejny krok w kierunku ujednolicenia zasad cyberbezpieczeństwa w różnych krajach Unii Europejskiej. Liczby związane z regulacjami robią wrażenie. Kary za naruszenie przepisów NIS2 sięgać mogą w przypadku podmiotów kluczowych nawet do 10 mln euro lub 2% łącznego światowego obrotu. To oczywiście tylko liczby, a podobnie jak w przypadku RODO - kary mogą okazać się znacznie mniejsze i dotyczyć najbardziej znaczących naruszeń. Nie zmienia to jednak faktu, że wiele z organizacji czeka rewolucja, a część wciąż nie jest w pełni świadoma czekających je wyzwań.

Raport ESET i DAGMA Bezpieczeństwo IT publikowany jest na kilka tygodni przed 17 października 2024 roku - czyli datą wyznaczającą termin wdrożenia NIS2 w krajowym porządku prawnym Państw UE. Temat dostosowania się przez firmy w Polsce do dyrektywy będziemy śledzić w kolejnych publikacjach – przyglądając się faktycznemu przebiegowi implementacji nowych przepisów. W niniejszym raporcie weryfikujemy natomiast poziom realnego wdrożenia RODO – poprzedniej, jeszcze większej regulacji, wpływającej na funkcjonowanie firm, instytucji i całego społeczeństwa. Wnioski dotyczące tych przepisów kilka lat po ich wdrożeniu pokazują, że implementacja nowych rozwiązań zwiększających bezpieczeństwo danych to bardzo trudny proces.

Wyzwania i inwestycje związane z NIS2

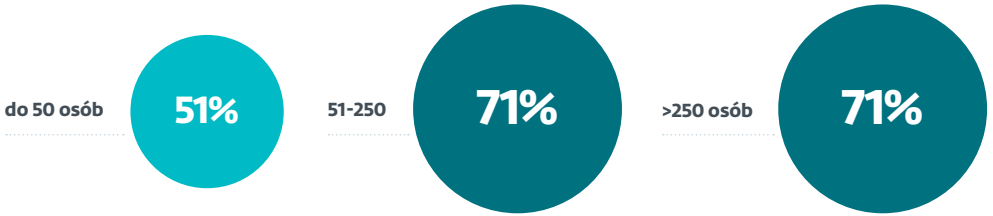
Według analiz przedstawionych w raporcie EY "The Future of Cybersecurity in Europe", regulacja NIS (poprzedniczka NIS2) spowodowała szereg inwestycji w cyberbezpieczeństwo w sektorach objętych tymi przepisami. Największe średnie wydatki na ten cel dotyczyły sektorów bankowości, energii, służby zdrowia i transportu, a także internetowych platform handlowych. Eksperci spodziewają się podobnej fali inwestycji w obliczu NIS2. Wśród trzech obszarów, które uważane są za kluczowe w tym kontekście, zidentyfikowane zostały: odpowiednie zarządzanie, wdrożenie systemów ochrony i testowania systemów IT, a także wykrywanie i reagowanie na incydenty cyberbezpieczeństwa.

Źródło: EY, The future of cybersecurity in Europe. Challenges related to the NIS2 Directive, 2023

EKSPERCI: RODO Z (UMIARKOWANYM) OPTYMIZMEM

Blisko 7 na 10 firm badanych przez ESET i DAGMA Bezpieczeństwo IT uważa, że w skuteczny sposób dostosowały się do wymogów przepisów RODO. Natomiast tylko 7% z nich nie zgadza się z tym stwierdzeniem, a 25% - nie ma na ten temat precyzyjnej opinii. Biorąc pod uwagę poruszenie i niejasność związaną z wchodzeniem i implementacją tych przepisów przez firmy w minionych latach, wynik ten zdaje się być stosunkowo optymistyczny. Przedsiębiorstwa wypracowały w większości odpowiednie procedury związane z ochroną danych osobowych oraz ich przechowywaniem. Stosunkowo niska realna skala spraw związanych z naruszeniem przepisów RODO w Polsce zdaje się też zmniejszać obawy biznesu o konsekwencje obowiązywania tych przepisów dla firmy.

Pozytywna ocena dostosowania się do wymogów RODO - odsetek firm



Warto zauważyć, że podobnie, jak w wielu innych częściach badania ESET, zarysowuje się wyraźna różnica między większymi firmami, a mniejszymi podmiotami. Zarówno w przypadku firm liczących ponad 50 pracowników, jak i tych z ponad 250 osób w kadrze dobre wdrożenie rozwiązań związanych z RODO deklaruje 71% badanych. Natomiast w segmencie małych przedsiębiorstw odsetek ten spada do blisko połowy (51%).

Firmy oceniające się jako przestrzegające wskazanych kwestii związanych z RODO

68% Przechowywanie danych osobowych klientów i kontrahentów w sposób zgodny z prawem

64% Transparentność w zbieraniu i przetwarzaniu danych osobowych klientów i kontrahentów

63% Zastosowanie różnorodnych i skutecznych zabezpieczeń logowania pracowników do firmowych systemów / zasobów zawierających dane szczególnej kategorii

60% Ograniczenie czasu przechowywania danych szczególnej kategorii i zwykłych do koniecznego minimum

EKSPERCI: RODO TKWI W SZCZEGÓŁACH

Jednak ogólna ocena dostosowania do RODO to jedno, a opinie na temat bardziej szczegółowych wymogów - to drugie. Zapytani o nie eksperci ds. cyberbezepieczeństwa wykazują się dość wysokim, ale jednak niższym poziomem pewności. Największy odsetek badanych z tej grupy (68%) jest przekonany, że ich firma dobrze dostosowała się do przechowywania danych osobowych klientów i kontrahentów w sposób zgodny z prawem. Jednocześnie 10% jest odwrotnego zdania. To teoretycznie dość niska wartość, ale z drugiej strony może wskazywać, że co dziesiąta firma z zatrudnionym ekspertem ds. cyberbezpieczeństwa może mieć trudności z przestrzeganiem przepisów obowiązujących już od kilku lat.

Nieco mniejszym zdecydowaniem wykazują się w ocenie transparentności w zbieraniu i przetwarzaniu danych osobowych, a także zastosowania różnorodnych i skutecznych zabezpieczeń logowania pracowników do systemów/zasobów zawierających dane. Przestrzeganie tych kwestii z pełnym przekonaniem deklaruje nieco mniej, niż 2/3 z nich.

Jeszcze mniejszy odsetek jest pewny, że ogranicza czas przechowywania danych szczególnej kategorii i zwykłych do koniecznego minimum. W każdej z czterech kwestii przytaczanych powyżej odsetek przekonanych o braku przygotowania firmy nie przekraczał kilkunastu procent, a nie mających pewności w tym względzie - oscylował między 1/4 a 1/5 badanych ekspertów ds. cyberbezpieczeństwa. Zwraca więc uwagę, że na poziomie szczegółów, w blisko 1/3 badanych przedsiębiorstw kwestie związane z wymogami RODO nie okazały się być zorganizowane w sposób niebudzący wątpliwości ekspertów - wciąż jest więc wiele do zrobienia.

09

O raporcie

METODOLOGIA
BADANIA ILOŚCIOWEGO

Metodologia badania ilościowego oraz cele badania

Raport "Cyberportret polskiego biznesu" przygotowany został przez marki ESET i DAGMA Bezpieczeństwo IT. Celem raportu było zweryfikowanie relacji między inwestycjami firm w cyberbezpieczeństwo oraz ich dojrzałością w tym zakresie, a faktycznymi postawami przyjmowanymi przez szeregowych pracowników.

Tezy i informacje zawarte w raporcie oparte zostały na badaniu opinii, przeprowadzonym w terminie 23.05 - 10.06 2024 r. Pomiar zrealizowano metodą CAWI za pomocą profesjonalnej ankiety online przy wsparciu instytutu ARC Rynek i Opinia. Pomiar przeprowadzono na próbie 1032 Polaków wykonujących obowiązki służbowe przy komputerze minimum przez 3 dni w tygodniu. Zdecydowana większość badanych (88%) wykonywała swoje zadania służbowe codziennie przy wykorzystaniu sprzętu elektronicznego od pracodawcy.

Próba objęła także tzw. boost n=256 osób zaangażowanych w działania z zakresu cyberbezpieczeństwa w swoim miejscu zatrudnienia. Analizy w raporcie dotyczą badanych ekspertów ds. cyberbezpieczeństwa z firm liczących przynajmniej 10 pracowników (n=227).

Na grono ekspertów ds. cyberbezpieczeństwa składała się różnorodna grupa respondentów, od praktyków monitorujących, zabezpieczających i audytujących firmowe systemy bezpieczeństwa, przez osoby wpływające na budżety na ten cel i menedżerów zespołów cybersecurity, aż po szkoleniowców w tym zakresie.

ESET

Jeden z globalnych liderów cyberbezpieczeństwa, którego rozwiązania zabezpieczają ponad 100 mln użytkowników i 400 tys. klientów biznesowych na całym świecie. Technologia ESET obejmuje wykrywanie i reakcję na zagrożenia, ultra-bezpieczne szyfrowanie oraz uwierzytelnianie wieloskładnikowe. Dzięki całodobowej ochronie w czasie rzeczywistym i silnemu wsparciu lokalnemu, zapewnia bezpieczeństwo użytkowników i ciągłość działania organizacji bez zakłóceń.

DAGMA Bezpieczeństwo IT

Od blisko 40 lat specjalizuje się w rozwiązaniach i usługach z zakresu cyberbezpieczeństwa, pomagając chronić ponad 150 tys. firm i instytucji w Polsce oraz Europie. Od 2023 roku Partner Ministerstwa Cyfryzacji w ramach programu „PWCyber", skupiającego największe firmy IT w kraju i którego celem jest poprawa szeroko rozumianego cyberbezpieczeństwa Państwa i firm w Polsce.

Cyberportret polskiego biznesu. Podstawowe informacje o badaniu

1032

Polaków pracujących przy komputerze min. 3 dni w tygodniu (firmy dowolnego rozmiaru)

227

Zaangażowanych w cybersecurity w firmach z min. 10 pracownikami (w całym badaniu 257 ekspertów cybersec)

244

specjalistów IT

Najczęstsze branże firmy

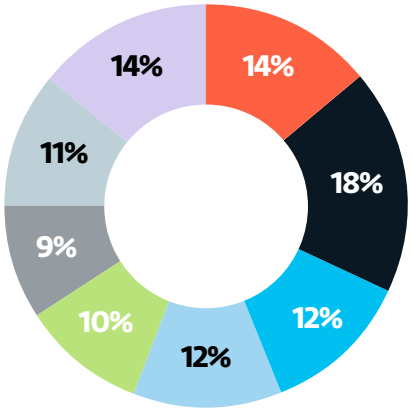
GRUPA OGÓLNA

1	IT / telco	15%
2	Handel	12%
3	Adm. publiczna	11%
4	Usługi	10%
5	Przemysł	8%
6	Nauka i szkolnictwo	7%
7	Transport i logistyka	6%
8	Finanse i bankowość	6%
9	Budownictwo	6%
10	Opieka zdrowotna	6%

EKSPERCI CYBERSEC

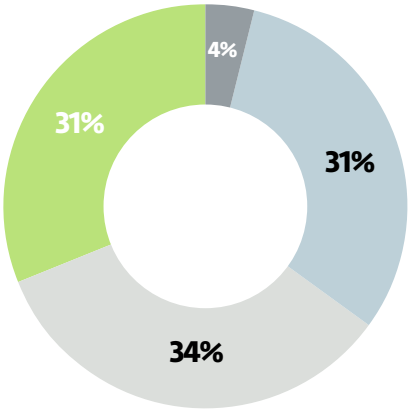
1	IT / telco	37%
2	Adm. publiczna	13%
3	Finanse i bankowość	9%
4	Usługi	8%
5	Transport i logistyka	6%
6	Przemysł	5%
7	Budownictwo	5%
8	Opieka zdrowotna	5%
9	Handel	4%
10	Nauka i szkolnictwo	2%

Struktura próby – pracownicy (ogół)



ROZMIAR FIRMY

- <10 osób
- 10 do 50
- 51 do 100
- 101 do 250
- 251 do 500
- 501 do 1000
- 1001 do 5000
- powyżej 5000



WIEK

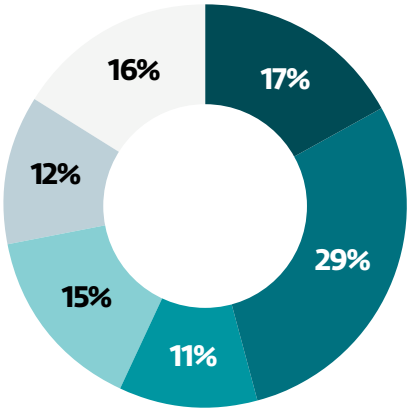
- 18-24
- 25-34
- 35-44
- 45-65

88%
respondentów pracuje przy komputerze przez 5 dni w tygodniu lub więcej

7%
przez 4 dni w tygodniu

5%
przez 3 dni w tygodniu

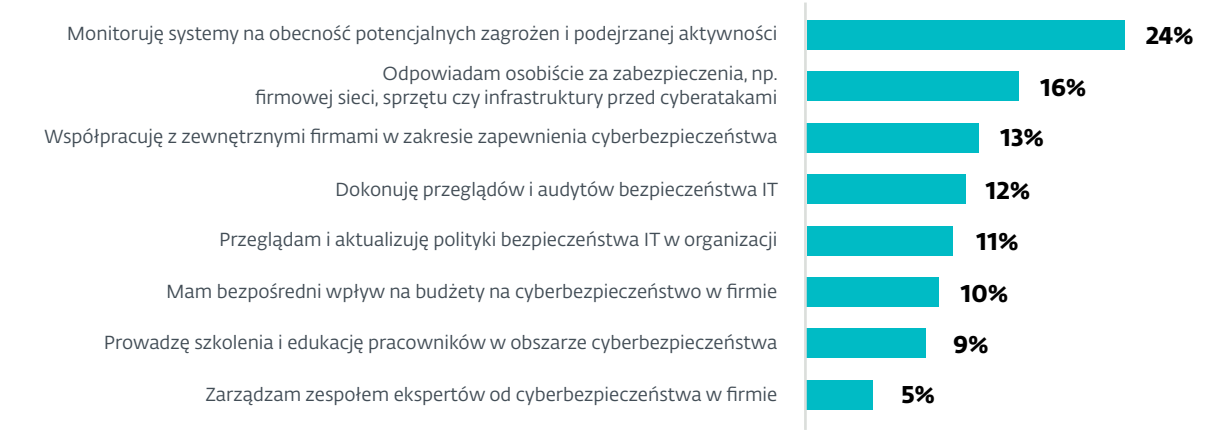
Struktura próby – eksperci cybersec

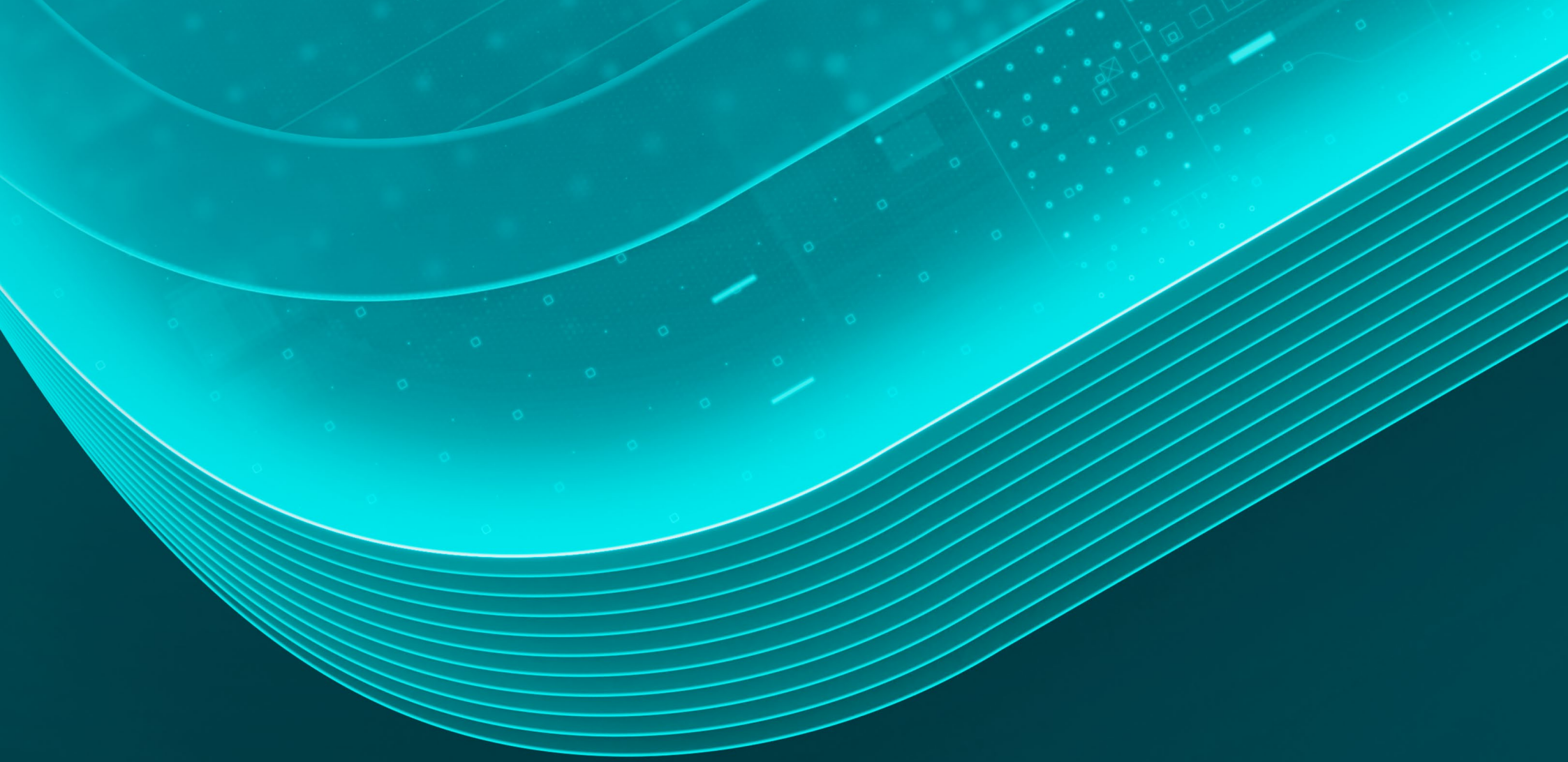


ROZMIAR FIRMY

- 10 do 50
- 51 do 250
- 251 do 500
- 501 do 1000
- 1001 do 5000
- powyżej 5000

Główny charakter zaangażowania w cyberbezpieczeństwo (możliwość wyboru tylko 1 odpowiedzi)





ESET Digital Security
Progress. Protected.

Raport powstał we współpracy z

DAGMA
BEZPIECZEŃSTWO IT