BADANIE RYNKU CYBERBEZPIECZEŃSTWA W POLSCE 2017

W DUŻYCH I ŚREDNICH FIRMACH

PRZEPROWADZONE PRZEZ PMR

LIFE IS FOR SHARING.

WPROWADZENIE

Artur Ostrowski
Członek Zarządu, Dyrektor ds. Rynku Biznesowego, T-Mobile Polska S.A.

Szanowni Państwo, w maju 2018 roku w życie wejdzie Rozporządzenie o Ochronie Danych Osobowych (RODO, eng. GDPR), które dotyczy wszystkich firm działających na obszarze Unii Europejskiej. Zostaną one zobowiązane m.in. do zgłaszania każdego incydentu naruszenia zabezpieczeń infrastruktury, nawet jeśli dotyczy ono działalności podwykonawcy. Takie restrykcyjne podejście wcześniej dotyczyło tylko nielicznych branż, a nowe wymogi mogą stanowić dla wielu organizacji prawdziwe wyzwanie. W związku z tym oddajemy w Państwa ręce przygotowany w tym szczególnym momencie raport „Badanie rynku cyberbezpieczeństwa w Polsce 2017".

Postanowiliśmy, jeszcze przed wejściem RODO w życie, sprawdzić podejście do zagadnień związanych z cyberbezpieczeństwem w polskich firmach. Badanie obejmowało przeprowadzenie niemal 700 wywiadów zarówno w dużych spółkach, jak i średnich firmach. Położyliśmy w nich nacisk na zagrożenia cyberatakami, rozwiązania zapewniające bezpieczeństwo IT, wydatki ponoszone na budowę i utrzymanie infrastruktury ICT oraz znaczenie firm zewnętrznych i własnych specjalistów w zakresie ochrony zasobów przedsiębiorstwa. Zgromadzone dane uzupełniają komentarze naszych ekspertów, którzy analizują uzyskane wyniki oraz przedstawiają ich interpretację.

Podczas zapoznawania się z raportem powinni Państwo pamiętać, że obok przygotowań do zmian legislacyjnych, na pozycję cyberbezpieczeństwa w przedsiębiorstwach wpływa także rosnąca liczba oraz różnorodność zagrożeń IT. Często ich rozwiązanie wykracza poza wewnętrzne możliwości i kompetencje przedsiębiorstwa, które korzysta w takich przypadkach z wyspecjalizowanych ekspertów zewnętrznych. Wyniki tego badania stanowią swoistą diagnozę potrzeb firm w obszarze outsourcingu usług cyberbezpieczeństwa. Jako firma specjalizująca się od lat w monitorowaniu ataków i ochronie danych partnerów biznesowych, zwracamy na to szczególną uwagę, przygotowując produkty i usługi dla przedsiębiorców.

Obraz, który udało nam się uchwycić, mówi wiele o postrzeganiu cyberbezpieczeństwa przez polskie firmy. Z przyjemnością przekazujemy go w Państwa ręce.

ZNACZENIE BEZPIECZEŃSTWA DANYCH W FIRMIE

Włodzimierz Nowak
Członek Zarządu, Dyrektor
ds. Prawnych, Bezpieczeństwa
i Zarządzania Zgodnością,
T-Mobile Polska S.A.

Szanowni Państwo, mamy przyjemność oddać w Państwa ręce raport, który stanowi nasz wkład w debatę na temat aktualnego stanu cyberbezpieczeństwa w Polsce. Ataki na systemy informatyczne nie są już przedmiotem zainteresowania wyłącznie specjalistów ds. bezpieczeństwa informacji i IT. Ich konsekwencje są odczuwalne zarówno dla zarządów firm i innych interesariuszy, jak również klientów. Cyberbezpieczeństwo stało się zatem koniecznością dla biznesu, a nie jedynie opcją.

Co więcej, pojawienie się nowych regulacji unijnych w obszarze danych osobowych (RODO) niejako wymusza dostosowanie się firm i potencjalne inwestycje w cyberbezpieczeństwo. Tymczasem jak pokazują dane zebrane w raporcie, nieświadome zagrożenia przedsiębiorstwa inwestują jedynie w proste i często przestarzałe rozwiązania, które uznają za wystarczające. Przyglądając się opracowanym materiałom, należy pamiętać, że na funkcjonowanie cyberbezpieczeństwa wpływa także intensywny rozwój cyberzagrożeń, które charakteryzują się coraz wyższym stopniem zaawansowania. Wszyscy możemy więc na co dzień obserwować wpływ tych niebezpiecznych przemian na działalność biznesową wielu firm – 51% firm stało się ofiarami cyberataków, a 93% dużych przedsiębiorstw zostało zaatakowanych tylko w 2016 roku. Straty z tym związane szacowane są łącznie na 200 mld euro w Europie, a w skali świata na 450 mld euro. Co więcej, jeśli nie wprowadzimy odpowiednich narzędzi prewencyjnych skala tego zjawiska będzie nadal rosła.

Przedmiotem niniejszego badania jest diagnoza istniejącej sytuacji w Polsce w dziedzinie ochrony cyberprzestrzeni na poziomie średnich i dużych firm. Raport stanowi także punkt wyjścia do zaproponowania podmiotom biznesowym jeszcze lepiej dopasowanych i kompleksowych rozwiązań ICT. Jako firma specjalizująca się od lat w monitorowaniu ataków i ochronie danych partnerów biznesowych przykuwamy do tego aspektu szczególną uwagę. Zdajemy sobie także sprawę z tego jak ważne są działania mające na celu budowanie świadomości polskich przedsiębiorców na temat zagrożeń związanych z cyberbezpieczeństwem. Reagowanie i podnoszenie zabezpieczeń tylko przez część podmiotów lub grupy dostawców sprawia, że taka selektywna ochrona nie jest realnie skuteczna. Dlatego należy dążyć do podnoszenia standardów i wspólnego dbania o bezpieczeństwo – zarówno na poziomie biznesowym, państwowym czy międzynarodowym.

Mamy nadzieję, że niniejszy raport pozwoli na zwiększenie świadomości polskich przedsiębiorców w zakresie cyberbezpieczeństwa i wpłynie na polepszenie kondycji bezpieczeństwa danych w przedsiębiorstwach.

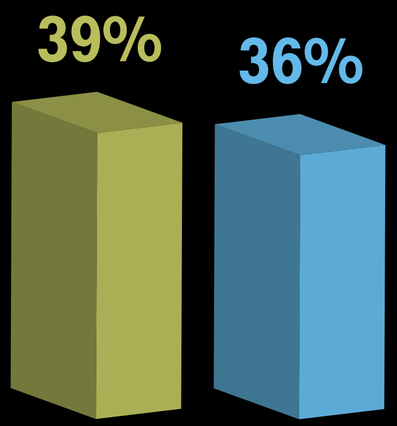
BADANE OBSZARY

1. Dostosowanie firm do Rozporządzenia o Ochronie Danych Osobowych 6
2. Zagrożenia związane z cyberatakami 13
3. Rozwiązania z zakresu cyberbezpieczeństwa 18
4. Wydatki na cyberbezpieczeństwo 34
5. Znaczenie firm zewnętrznych i własnych specjalistów w zakresie cyberbezpieczeństwa 45

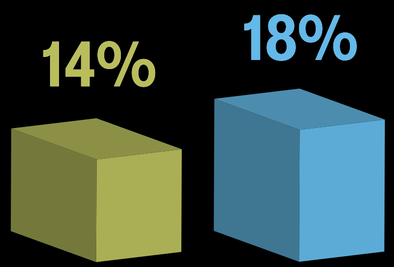
1. DOSTOSOWANIE FIRM DO RODO

ETAPY DOSTOSOWYWANIA SIĘ W FIRMACH DO WYMOGÓW RODO

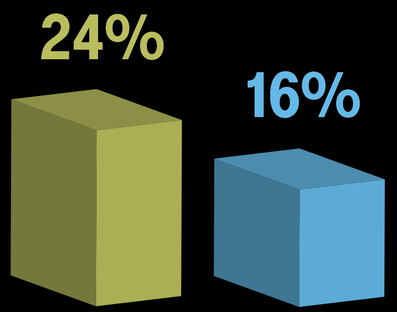
ŚREDNIE I DUŻE FIRMY W POLSCE (2017)



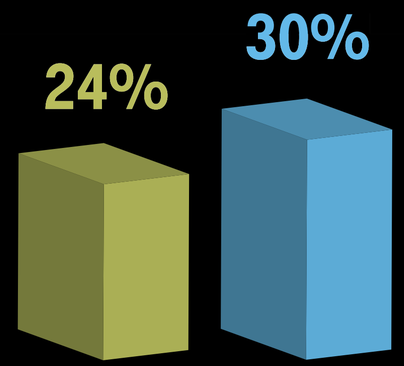
Wiemy, że musimy się dostosować i **rozpoczęliśmy już ten proces**



Wiemy, że musimy się dostosować i **planujemy rozpocząć ten proces**



RODO/GDPR **nie ma wpływu na moją firmę.** Nie sądzę, że trzeba się dostosować



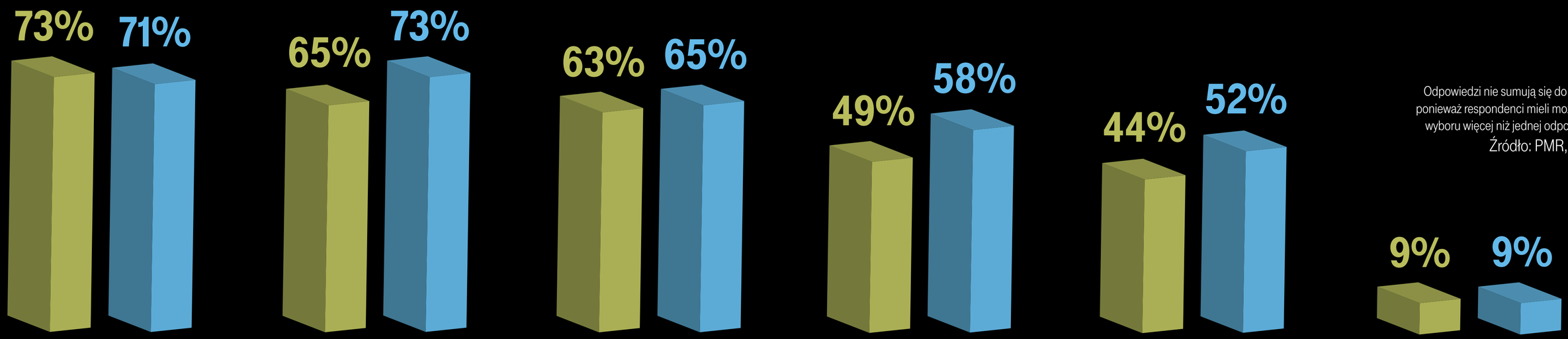
Nigdy **nie spotkałem się z określeniem** RODO/GDPR

ETAPY DOSTOSOWYWANIA SIĘ W FIRMACH DO WYMOGÓW RODO
ŚREDNIE I DUŻE FIRMY W POLSCE W PODZIALE NA BRANŻE (2017)

BRANŻE ▶	Produkcja dóbr szybko zbywalnych (żywności, napojów i chemii gospodarczej)	Handel hurtowy i detaliczny	ICT & media	Produkcja maszyn i urządzeń gotowych	Transport i logistyka	Przedsiębiorstwa użyteczności publicznej	Ochrona zdrowia	Pozostałe
Wiemy, że musimy się dostosować i rozpoczęliśmy już ten proces	34%	35%	39%	30%	30%	46%	46%	37%
Wiemy, że musimy się dostosować i planujemy rozpocząć ten proces	11%	7%	16%	14%	23%	18%	24%	17%
Nigdy nie spotkałem się z określeniem RODO/GDPR	34%	35%	21%	27%	24%	25%	20%	21%
RODO/GDPR nie ma wpływu na moją firmę/Nie sądzę, że trzeba się dostosować	21%	23%	24%	29%	22%	11%	10%	25%

DZIAŁANIA PODJĘTE LUB PLANOWANE W ZWIĄZKU Z DOSTOSOWANIEM SIĘ DO WYMOGÓW RODO

ŚREDNIE I DUŻE FIRMY W POLSCE (2017)



Odpowiedzi nie sumują się do 100%, ponieważ respondenci mieli możliwość wyboru więcej niż jednej odpowiedzi.

Źródło: PMR, 2017

Okresowe szkolenia dla pracowników dot. ochrony danych osobowych	**Uwzględnienie mechanizmów** ochrony danych osobowych w systemach IT	**Wdrożenie zabezpieczeń** w zakresie ochrony danych osobowych oraz audyt obszaru ochrony danych przez firmę zewnętrzną	**Utworzenie lub aktualizacja rejestru operacji** przetwarzania danych osobowych	**Ocena skutków operacji** przetwarzania danych	**Inne**

DZIAŁANIA PODJĘTE LUB PLANOWANE W ZWIĄZKU Z DOSTOSOWANIEM SIĘ DO WYMOGÓW RODO

ŚREDNIE I DUŻE FIRMY W POLSCE W PODZIALE NA BRANŻE (2017)

BRANŻE ▶	Produkcja dóbr szybko zbywalnych (żywności, napojów i chemii gospodarczej)	Handel hurtowy i detaliczny	ICT & media	Produkcja maszyn i urządzeń gotowych	Transport i logistyka	Przedsiębiorstwa użyteczności publicznej	Ochrona zdrowia	Pozostałe
Okresowe szkolenia dla pracowników dotyczące ochrony danych osobowych	70%	71%	73%	67%	78%	78%	67%	84%
Uwzględnienie mechanizmów ochrony danych osobowych w systemach IT	79%	79%	87%	58%	65%	59%	70%	64%
Wdrożenie zabezpieczeń w zakresie ochrony danych osobowych oraz audyt obszaru ochrony danych przez firmę zewnętrzną	63%	50%	73%	57%	79%	65%	74%	44%
Utworzenie lub aktualizacja rejestru operacji przetwarzania danych osobowych	58%	40%	73%	48%	50%	56%	63%	16%
Ocena skutków operacji przetwarzania danych	63%	33%	87%	34%	43%	49%	51%	28%
Inne	12%	4%	13%	9%	7%	13%	5%	8%

DOSTOSOWANIE FIRM DO RODO
NAJWAŻNIEJSZE WNIOSKI

Ponad połowa z przebadanych firm (53%) rozpoczęła lub planuje rozpocząć proces dostosowania się do ogólnego rozporządzenia o ochronie danych osobowych.

Przedstawiciel **co piątej** dużej i średniej firmy działającej w Polsce (20%) uważa, że rozporządzenie RODO nie ma wpływu na jego firmę i nie będzie trzeba się do niego dostosowywać. Warto również zaznaczyć, że **co czwarta** badana firma nie spotkała się nigdy wcześniej z określeniem RODO/GDPR.

Wśród wielu działań, mających na celu dostosowanie się do wymogów RODO/GDPR, badani przedstawiciele dużych i średnich firm zadeklarowali, że ich firma **przeprowadza lub dopiero planuje realizację okresowych szkoleń** dla pracowników z zakresu ochrony danych osobowych.

Firmy planują także uwzględnić mechanizmy związane z ochroną danych osobowych w swoich systemach IT (69%). Działania tego typu nieco częściej deklarowali przedstawiciele dużych firm (73%).

DOSTOSOWANIE FIRM DO RODO – OPINIA EKSPERTA T-MOBILE

Daniel Ślęzak
Kierownik Działu Ochrony Danych
i Zarządzania Ryzykiem
Radca Prawny, T-Mobile Polska S.A.

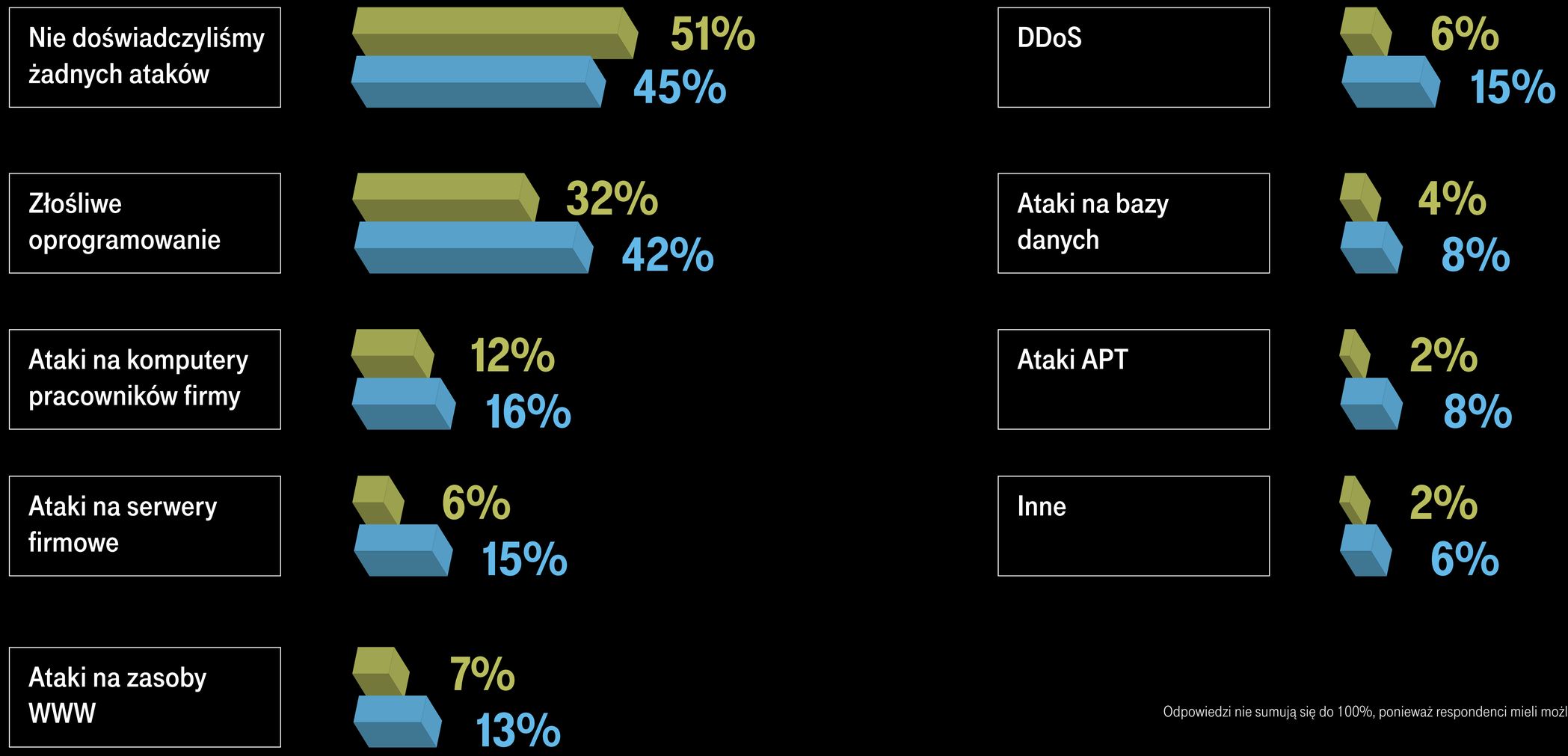
Celem zbliżających się zmian legislacyjnych w obszarze ochrony danych osobowych – RODO (ang. GDPR) – jest wzmocnienie tej ochrony. Jednym z instrumentów mających wspomóc realizację wskazanego celu jest obowiązek świadomego zarządzania ryzykiem związanym z przetwarzaniem danych, a co za tym idzie, dopasowania poziomu ochrony do stopnia ryzyka występującego przy operacjach przetwarzania. W obecnych regulacjach obowiązek ten nie jest eksponowany tak wyraźnie jak w RODO.

Niepokoi brak świadomości nadchodzących zmian prawa wśród przedsiębiorstw. Ponad połowa firm biorących udział w badaniu nie podjęła jeszcze kroków, by ocenić wpływ RODO na swoją działalność lub działań w celu dostosowania się do regulacji. W grupie tej znalazło się 62% średnich i 64% dużych spośród badanych firm. Przedsiębiorstwa te nie mają wiedzy o zmianach wprowadzanych przez RODO, uznają, że regulacja ich w ogóle nie dotyczy (!) albo zwlekają z podjęciem niezbędnych działań.

Wśród podjętych lub planowanych działań implementujących nowe regulacje ankietowane firmy najczęściej wskazują na konieczność podniesienia świadomości w zakresie ochrony danych osobowych u pracowników oraz zastosowanie mechanizmów ochrony danych w infrastrukturze IT. Budowanie świadomości oraz zmiany w IT są procesami długotrwałymi, a czasu jest coraz mniej. Firmy, które jeszcze nie rozpoczęły procesu dostosowania się do nowych regulacji, ryzykują tym, że mogą nie zdążyć wprowadzić zmian do wejścia RODO w życie.

2. ZAGROŻENIA ZWIĄZANE Z CYBERATAKAMI

RODZAJE CYBERATAKÓW
ŚREDNIE I DUŻE FIRMY W POLSCE (2017)



Odpowiedzi nie sumują się do 100%, ponieważ respondenci mieli możliwość wyboru więcej niż jednej odpowiedzi.

Źródło: PMR, 2017

RODZAJE CYBERATAKÓW
ŚREDNIE I DUŻE FIRMY W POLSCE W PODZIALE NA BRANŻE (2017)

BRANŻE ▶	Produkcja dóbr szybko zbywalnych (żywności, napojów i chemii gospodarczej)	Handel hurtowy i detaliczny	ICT & media	Produkcja maszyn i urządzeń gotowych	Transport i logistyka	Przedsiębiorstwa użyteczności publicznej	Ochrona zdrowia	Pozostałe
Nie doświadczyliśmy żadnych ataków	50%	41%	37%	50%	35%	47%	59%	54%
Złośliwe oprogramowanie (wirusy, konie trojańskie itp.)	39%	38%	59%	35%	48%	36%	26%	30%
Ataki na komputery pracowników firmy	10%	18%	24%	11%	26%	13%	10%	17%
Ataki na serwery firmowe	5%	9%	28%	5%	14%	20%	7%	6%
Ataki na zasoby WWW	6%	7%	28%	5%	12%	15%	7%	14%
DDoS	8%	14%	28%	6%	12%	14%	4%	8%
Ataki na bazy danych	4%	4%	24%	5%	2%	10%	3%	3%
Ataki APT (Advanced Persistent Threats)	2%	3%	24%	1%	5%	8%	2%	5%
Inne	3%	5%	7%	3%	2%	4%	2%	9%

ZAGROŻENIA ZWIĄZANE Z CYBERATAKAMI
NAJWAŻNIEJSZE WNIOSKI

Co druga badana firma z segmentu dużych i średnich firm zadeklarowała, że do tej pory nigdy nie doświadczyła żadnych cyberataków (48%).

Nieco częściej na brak ataków wskazywały firmy zatrudniające poniżej 250 pracowników (51%).

Głównym celem cyberataku jest użytkownik. Najczęstszym wektorem ataków jest złośliwe oprogramowanie, któremu uległo łącznie 37% respondentów. Ataków na komputery pracowników doświadczyło ogółem 14% badanych firm.

Duże firmy, z racji skali swojej działalności, znacznie częściej niż średnie przedsiębiorstwa bywają celem bezpośrednich ataków, takich jak: ataki na serwery firmowe (15%), zasoby WWW (13%) czy bazy danych (8%).

ZAGROŻENIA ZWIĄZANE Z CYBERATAKAMI – OPINIA EKSPERTA T-MOBILE

Arkadiusz Buczek
Główny Specjalista
ds. Cyberbezpieczeństwa,
T-Mobile Polska S.A.

W sumie 48% firm (w tym 51% respondentów z sektora średnich przedsiębiorstw i 45% dużych spółek) zadeklarowało, że nie padło ofiarą cyberataku. Taki wynik świadczy o niskiej kondycji cyberbezpieczeństwa w Polsce. Obserwacje prowadzone na całym świecie wskazują, że praktycznie każda infrastruktura dostępna w Internecie poddawana jest atakom. Czas wykrycia poważnego incydentu często zajmuje miesiące, a nawet lata. Dane te odzwierciedlają zatem niską jakość stosowanych metod monitorowania i rejestracji incydentów w polskich firmach, które ignorują nadzorowanie stanu bezpieczeństwa swoich zasobów i opóźniają wykrycie udanych ataków cybernetycznych.

Rodzaje ataków wskazywane najczęściej przez respondentów to złośliwe oprogramowanie – 37% oraz ataki na komputery – 14%. Popularność tego typu ataków związana jest z najsłabszym ogniwem w łańcuchu zabezpieczeń, czyli aktywnością człowieka. O wiele łatwiej jest uśpić czujność użytkownika niż przełamać techniczne zabezpieczenia, co potwierdzają dane zgromadzone w badaniu.

Szerokim echem odbiły się ostatnio dwie duże kampanie malware – WannaCry i NotPetya. Ta druga dotknęła polskie firmy współpracujące z Ukrainą i została dobrze zapamiętana przez przedsiębiorców. W wynikach badań potwierdza to wysoki procent ataków na firmy związane z transportem i logistyką.

Branże, które są najbardziej świadome zagrożeń cybernetycznych, a zarazem pozostają najaktywniejsze w cyberprzestrzeni, to ICT i media. Tylko 37% ich przedstawicieli twierdzi, że nie zaobserwowało ataków.

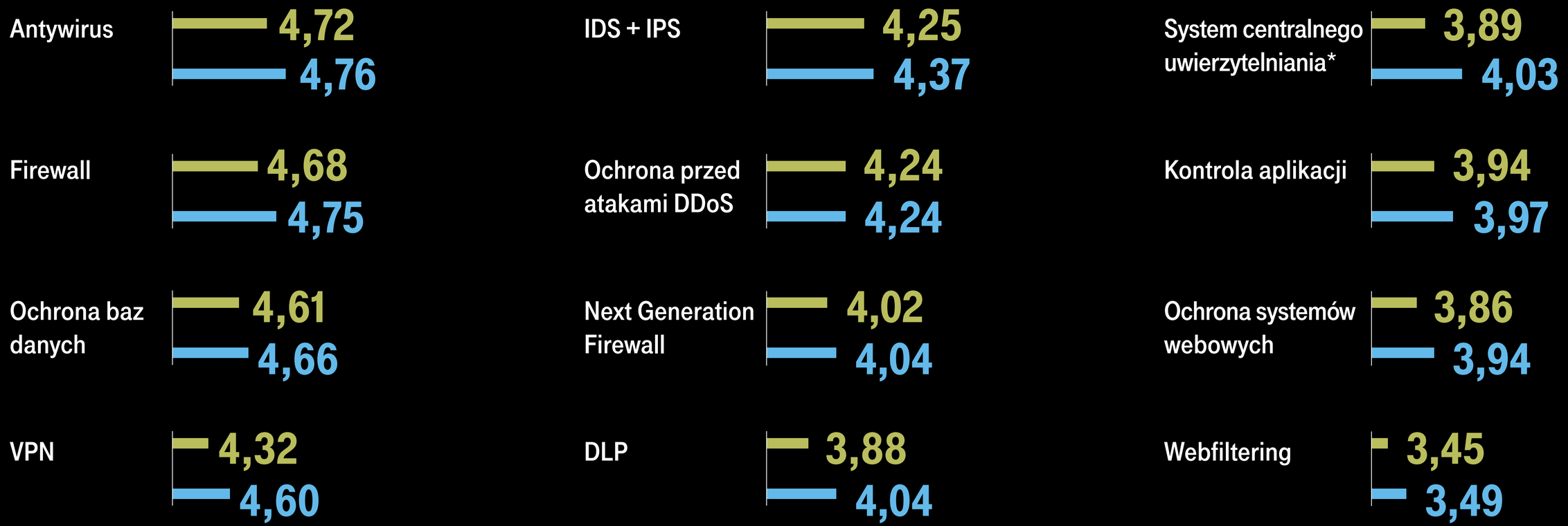
Odpowiedzi uzyskane na pytania postawione w sekcji „Zagrożenia związane z cyberatakami” nie przedstawiają w pełni sytuacji rzeczywistej, a raczej sposób postrzegania zagrożeń. To natomiast przekłada się na inicjatywy dotyczące bezpieczeństwa i wydatki firm w tym obszarze. Ponieważ poczucie zagrożenia jest niskie, nakłady finansowe na cyberochronę są proporcjonalnie niewysokie, a działania prewencyjne nie są traktowane priorytetowo.

3. ROZWIĄZANIA Z ZAKRESU CYBERBEZPIECZEŃSTWA

ZNACZENIE ROZWIĄZAŃ WPŁYWAJĄCYCH NA CYBERBEZPIECZEŃSTWO

ŚREDNIE I DUŻE FIRMY W POLSCE (2017)

Średnia ocena respondentów w skali 1-5.



* System centralnego uwierzytelniania/uwierzytelnianie dwuskładnikowe/zarządzanie certyfikatami.

Źródło: PMR, 2017

ZNACZENIE ROZWIĄZAŃ WPŁYWAJĄCYCH NA CYBERBEZPIECZEŃSTWO
ŚREDNIE I DUŻE FIRMY W POLSCE W PODZIALE NA BRANŻE (2017) (CZĘŚĆ I)

Średnia ocena respondentów w skali 1-5.

BRANŻE ▶	Produkcja dóbr szybko zbywalnych (żywności, napojów i chemii gospodarczej)	Handel hurtowy i detaliczny	ICT & media	Produkcja maszyn i urządzeń gotowych	Transport i logistyka	Przedsiębiorstwa użyteczności publicznej	Ochrona zdrowia	Pozostałe
Antywirus	4,65	4,81	4,73	4,76	4,86	4,66	4,74	4,79
Firewall	4,70	4,66	4,85	4,67	4,71	4,76	4,75	4,69
Ochrona baz danych	4,59	4,76	4,90	4,59	4,55	4,53	4,72	4,48
Router	4,53	4,59	4,71	4,56	4,61	4,51	4,49	4,55
VPN	4,71	4,53	4,83	4,44	4,45	4,21	4,28	4,35
Ochrona końcówek – urządzeń użytkowników/ pracowników	4,36	4,44	4,46	4,39	4,49	4,44	4,45	4,42
IDS + IPS (system ochrony przed włamaniami)	4,16	4,34	4,31	4,32	4,23	4,53	4,38	4,01
Ochrona przed atakami (D)DoS (ataki odmowy usługi)	4,30	4,34	4,40	4,08	4,27	4,25	4,32	3,95
Antyspyware	4,25	4,16	4,51	4,07	4,39	4,28	4,05	4,12

ZNACZENIE ROZWIĄZAŃ WPŁYWAJĄCYCH NA CYBERBEZPIECZEŃSTWO
ŚREDNIE I DUŻE FIRMY W POLSCE W PODZIALE NA BRANŻE (2017) (CZĘŚĆ II)

BRANŻE ▶	Produkcja dóbr szybko zbywalnych (żywności, napojów i chemii gospodarczej)	Handel hurtowy i detaliczny	ICT & media	Produkcja maszyn i urządzeń gotowych	Transport i logistyka	Przedsiębiorstwa użyteczności publicznej	Ochrona zdrowia	Pozostałe
Bezpieczne Wi-Fi (łączność bezprzewodowa)	4,29	4,23	4,26	4,24	4,31	3,75	3,65	3,86
Antyspam	4,15	4,15	4,29	3,96	4,27	4,08	3,72	4,15
Next Generation Firewall	4,13	4,07	4,09	3,91	3,89	4,08	4,12	3,91
DLP (system ochrony przed wyciekiem danych)	3,95	4,07	4,41	3,85	4,10	4,04	3,93	3,40
System centralnego uwierzytelniania/ uwierzytelnianie dwuskładnikowe/zarządzanie certyfikatami	4,07	3,90	4,44	3,87	3,80	3,97	3,93	3,82
Kontrola aplikacji	3,97	3,82	4,16	3,87	4,10	4,01	4,04	3,79
Ochrona systemów webowych (WWW)	3,87	4,05	4,50	3,68	4,03	3,98	3,80	3,64
Webfiltering (kategoryzacja stron WWW)	3,43	3,40	3,78	3,46	3,46	3,44	3,62	3,16
Rozwiązania typu sandbox	3,23	3,48	3,96	3,26	3,08	3,33	3,35	3,08

ROZWIĄZANIA WPŁYWAJĄCE NA CYBERBEZPIECZEŃSTWO, KTÓRE BĘDĄ PRIORYTETEM W CIĄGU 1-2 LAT

ŚREDNIE I DUŻE FIRMY W POLSCE (2017)

Respondenci mogli wybrać maks. 3 odpowiedzi.

	ŚREDNIE	DUŻE
Firewall	42%	44%
Antywirus	41%	36%
Ochrona baz danych	36%	34%
VPN	21%	30%
UTM	17%	22%
Ochrona końcówek urządzeń użytkowników/pracowników	18%	16%
Antyspam	13%	13%
Router	8%	9%
Antyspyware	7%	8%
Bezpieczne Wi-Fi (łączność bezprzewodowa)	5%	6%
IDS + IPS (system ochrony przed włamaniami)	7%	6%
Ochrona przed atakami (D)DoS	6%	6%
DLP (system ochrony przed wyciekiem danych)	4%	7%
Next Generation Firewall	5%	6%
System centralnego uwierzytelniania/ uwierzytelnianie dwuskładnikowe/zarządzanie certyfikatami	4%	5%
Ochrona systemów webowych	3%	3%
Webfiltering	3%	3%
Kontrola aplikacji	1%	2%
Rozwiązania typu sandbox	1%	2%
Inne	2%	1%

Źródło: PMR, 2017

ROZWIĄZANIA WPŁYWAJĄCE NA CYBERBEZPIECZEŃSTWO, KTÓRE BĘDĄ PRIORYTETEM W CIĄGU 1-2 LAT

ŚREDNIE I DUŻE FIRMY W POLSCE W PODZIALE NA BRANŻE (2017) (CZĘŚĆ I)

BRANŻE ▶	Produkcja dóbr szybko zbywalnych (żywności, napojów i chemii gospodarczej)	Handel hurtowy i detaliczny	ICT & media	Produkcja maszyn i urządzeń gotowych	Transport i logistyka	Przedsiębiorstwa użyteczności publicznej	Ochrona zdrowia	Pozostałe
Firewall	32%	44%	63%	43%	47%	49%	47%	28%
Antywirus	35%	44%	38%	46%	43%	37%	34%	28%
Ochrona baz danych	32%	33%	53%	31%	36%	30%	39%	37%
VPN	31%	32%	33%	28%	23%	15%	19%	25%
UTM	26%	14%	10%	14%	8%	24%	29%	22%
Ochrona końcówek – urządzeń użytkowników/ pracowników	17%	13%	20%	16%	17%	21%	14%	25%
Antyspam	8%	16%	13%	14%	21%	17%	8%	13%
Router	13%	7%	5%	11%	9%	8%	5%	9%
Antyspyware	11%	11%	5%	4%	8%	2%	7%	15%

ROZWIĄZANIA WPŁYWAJĄCE NA CYBERBEZPIECZEŃSTWO, KTÓRE BĘDĄ PRIORYTETEM W CIĄGU 1-2 LAT

ŚREDNIE I DUŻE FIRMY W POLSCE W PODZIALE NA BRANŻE (2017) (CZĘŚĆ II)

BRANŻE ▶	Produkcja dóbr szybko zbywalnych (żywności, napojów i chemii gospodarczej)	Handel hurtowy i detaliczny	ICT & media	Produkcja maszyn i urządzeń gotowych	Transport i logistyka	Przedsiębiorstwa użyteczności publicznej	Ochrona zdrowia	Pozostałe
Bezpieczne Wi-Fi (łączność bezprzewodowa)	2%	9%	0%	9%	6%	4%	7%	0%
IDS + IPS (system ochrony przed włamaniami)	10%	5%	8%	6%	8%	6%	2%	12%
Ochrona przed atakami (D)DoS (ataki odmowy usługi)	8%	6%	10%	2%	4%	4%	5%	9%
DLP (system ochrony przed wyciekiem danych)	4%	6%	8%	2%	6%	10%	7%	0%
Next Generation Firewall	6%	5%	10%	5%	4%	2%	7%	7%
System centralnego uwierzytelniania/ uwierzytelnianie dwuskładnikowe/zarządzanie certyfikatami	5%	3%	8%	4%	4%	1%	7%	6%

ROZWIĄZANIA WPŁYWAJĄCE NA CYBERBEZPIECZEŃSTWO, KTÓRE BĘDĄ PRIORYTETEM W CIĄGU 1-2 LAT

ŚREDNIE I DUŻE FIRMY W POLSCE W PODZIALE NA BRANŻE (2017) (CZĘŚĆ III)

BRANŻE ▶	Produkcja dóbr szybko zbywalnych (żywności, napojów i chemii gospodarczej)	Handel hurtowy i detaliczny	ICT & media	Produkcja maszyn i urządzeń gotowych	Transport i logistyka	Przedsiębiorstwa użyteczności publicznej	Ochrona zdrowia	Pozostałe
Ochrona systemów webowych (WWW)	2%	2%	0%	4%	2%	4%	3%	0%
Webfiltering (kategoryzacja stron WWW)	6%	4%	5%	2%	2%	2%	3%	0%
Kontrola aplikacji	4%	0%	0%	1%	4%	0%	2%	2%
Rozwiązania typu sandbox	0%	1%	0%	0%	2%	4%	1%	3%
Inne	2%	1%	0%	2%	0%	3%	1%	0%

ROZWIĄZANIA Z ZAKRESU CYBERBEZPIECZEŃSTWA – OPINIA EKSPERTA T-MOBILE

Sebastian Pióro
Główny Specjalista ds. Produktu ICT,
T-Mobile Polska S.A.

Mimo rozwoju technologii cyberzabezpieczeń, firmy wciąż ufają rozwiązaniom takim jak firewall i antywirus, które od pewnego czasu uznawane są za niewystarczające. Największą popularnością wśród badanych cieszą się produkty firm Cisco Systems, Fortinet i Eset.

Niepokojący jest fakt, że choć poziom zaawansowania cyberataków znacznie wzrósł, to sposoby zabezpieczeń mają się nie zmienić – te same rozwiązania znalazły się na liście priorytetów na najbliższe 1-2 lata. Wynika to z niewielkiej wciąż świadomości cyberzagrożeń w przedsiębiorstwach.

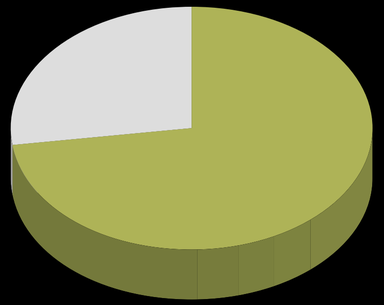
Rozwiązania w zakresie bezpieczeństwa powinny być implementowane według najlepszych praktyk, zaleceń z audytów, testów penetracyjnych poprzedzonych rzetelną analizą ryzyka – tu z pomocą mogą przyjść pewnego rodzaju drogowskazy, takie jak norma ISO 27001.

Podobnie jak przed kilku laty regulacja KNF (rekomendacja D) w sektorze finansowym, tak teraz RODO powinno wymusić na firmach przetwarzających dane osobowe wdrożenie odpowiednich rozwiązań w zakresie bezpieczeństwa. Wskazuje na to m.in. wzrost zainteresowania mechanizmami zabezpieczeń baz danych, w których często przechowywane są dane osobowe.

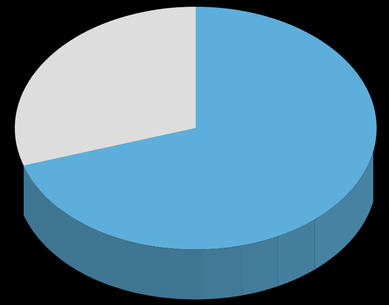
PRZEPROWADZENIE TESTÓW PENETRACYJNYCH/PENTESTÓW SIECI I SERWERÓW

ŚREDNIE I DUŻE FIRMY W POLSCE (2017)

TAK

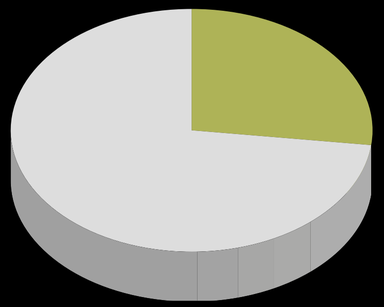


73%

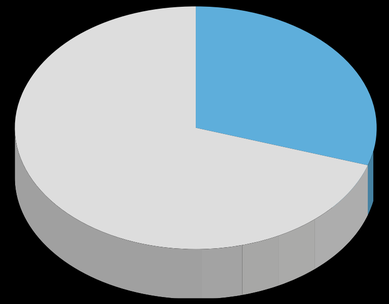


70%

NIE



27%



30%

Źródło PMR, 2017

PRZEPROWADZENIE TESTÓW PENETRACYJNYCH/PENTESTÓW SIECI I SERWERÓW

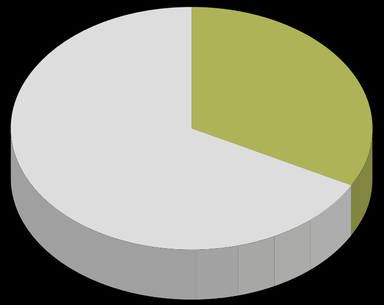
ŚREDNIE I DUŻE FIRMY W POLSCE W PODZIALE NA BRANŻE (2017)

BRANŻE ▶	Produkcja dóbr szybko zbywalnych (żywności, napojów i chemii gospodarczej)	Handel hurtowy i detaliczny	ICT & media	Produkcja maszyn i urządzeń gotowych	Transport i logistyka	Przedsiębiorstwa użyteczności publicznej	Ochrona zdrowia	Pozostałe
Tak	72%	68%	92%	68%	64%	69%	66%	62%
Nie	28%	32%	8%	32%	36%	31%	34%	38%

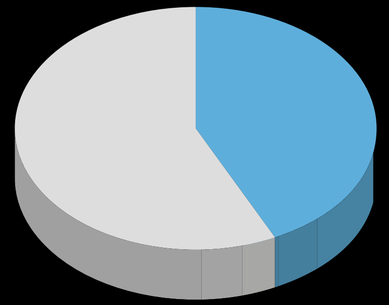
PRZEPROWADZENIE AUDYTU BEZPIECZEŃSTWA INFORMACJI, POD KĄTEM ZGODNOŚCI Z NORMĄ ISO 27001

ŚREDNIE I DUŻE FIRMY W POLSCE (2017)

TAK

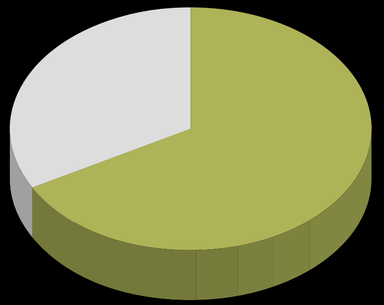


33%

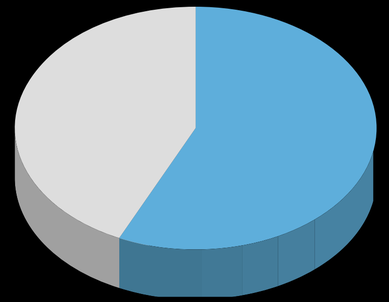


43%

NIE



67%



57%

Źródło PMR, 2017

PRZEPROWADZENIE AUDYTU BEZPIECZEŃSTWA INFORMACJI POD KĄTEM ZGODNOŚCI Z NORMĄ ISO 27001

ŚREDNIE I DUŻE FIRMY W POLSCE W PODZIALE NA BRANŻE (2017)

BRANŻE ▶	Produkcja dóbr szybko zbywalnych (żywności, napojów i chemii gospodarczej)	Handel hurtowy i detaliczny	ICT & media	Produkcja maszyn i urządzeń gotowych	Transport i logistyka	Przedsiębiorstwa użyteczności publicznej	Ochrona zdrowia	Pozostałe
Tak	34%	31%	66%	31%	35%	38%	44%	35%
Nie	66%	69%	34%	69%	65%	62%	56%	65%

ROZWIĄZANIA Z ZAKRESU CYBERBEZPIECZEŃSTWA
NAJWAŻNIEJSZE WNIOSKI

Zarówno w średnich, jak i w dużych firmach najważniejsze rozwiązania wpływające na bezpieczeństwo sieciowe to **program antywirusowy** oraz **zapora sieciowa**. Dla większości badanych firm stanowią one podstawę całego systemu bezpieczeństwa.

Siedem na dziesięć badanych przedsiębiorstw przeprowadziło testy penetracyjne sieci i serwerów.

W ciągu najbliższych 2 lat badane firmy z sektora dużych i średnich przedsiębiorstw nie planują większych zmian w działaniach związanych z cyberbezpieczeństwem. Podstawowe zabezpieczenia będą oparte na **oprogramowaniu antywirusowym** oraz **zaporach sieciowych**. Ponadto nadal dużą uwagę będą przywiązywać do rozwiązań, mających na celu **zapewnienie bezpieczeństwa baz danych**.

Tylko **jedna trzecia** średnich firm przeprowadziła audyt bezpieczeństwa informacji pod kątem zgodności z normą ISO 27001.

Częściej na przeprowadzenie audytu wskazywali przedstawiciele dużych firm (43% w stosunku do 33% w grupie średnich przedsiębiorstw).

AUDYTY BEZPIECZEŃSTWA I PENTESTY – OPINIA EKSPERTA T-MOBILE

Arkadiusz Buczek
Główny Specjalista
ds. Cyberbezpieczeństwa,
T-Mobile Polska S.A.

W zakresie proaktywnych działań, takich jak pentesty lub audyty, wyniki są zaskakujące. Ponad 70% ankietowanych firm potwierdza przeprowadzenie testów penetracyjnych w swojej firmie. Tak wysokie statystyki tłumaczyć mogą po części dane dotyczące poszczególnych branż, a także wynik 92% dla sektora ICT oraz mediów. Powstaje pytanie, co tak naprawdę rozumiane jest pod pojęciem „pentesty". Wiele przedsiębiorstw może traktować skanowanie podatności lub audyt reguł firewall na równi z testami penetracyjnymi, co sumarycznie wpłynęło na tak wysoki wynik.

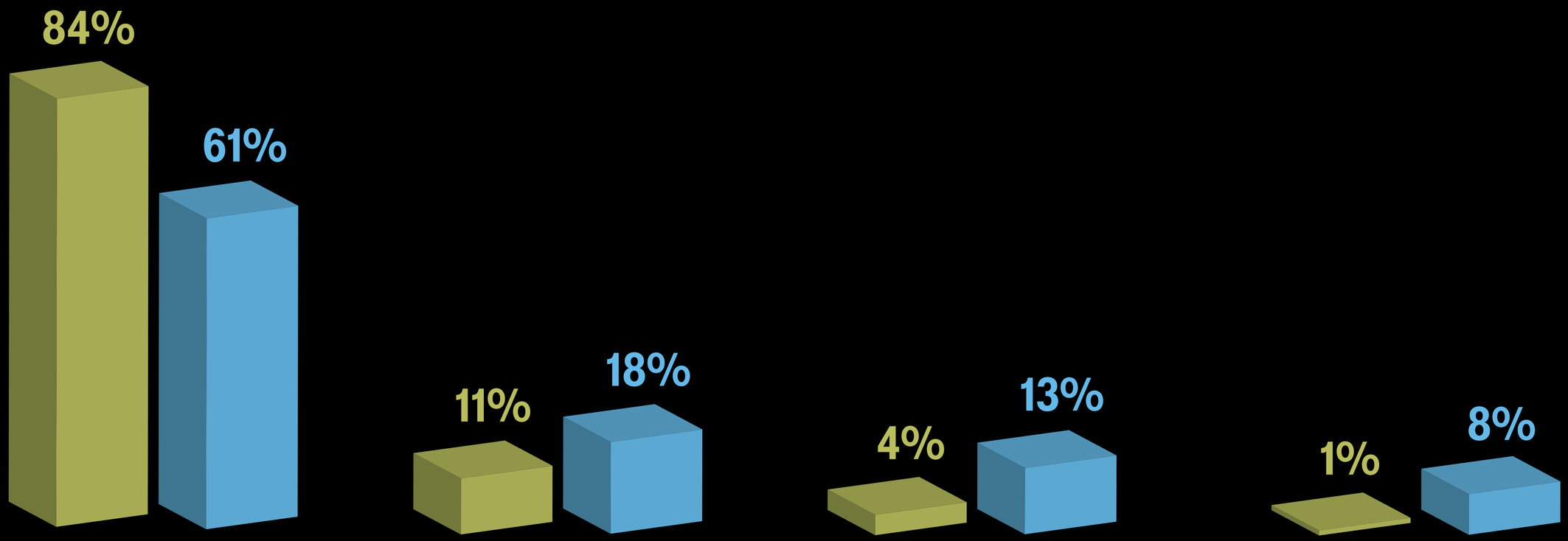
Z kolei tylko nieco ponad jedna trzecia firm przeprowadza audyty zgodności z normą ISO 27001. W wynikach pozytywnie wyróżnia się branża ICT i mediów, gdzie proporcje są odwrotne – dwie trzecie przedsiębiorstw poddaje się audytom. Dysproporcje powodują prawdopodobnie inne regulacje, którym podlega branża ICT, takie jak Prawo telekomunikacyjne, a w tej sytuacji norma ISO 27001 wydaje się dobrym punktem startowym tworzenia skutecznego systemu zarządzania bezpieczeństwem. Audyty są pomocne w określaniu dojrzałości firmy w zarządzaniu bezpieczeństwem i wskazywaniu słabych punktów w organizacji. Wyższy wskaźnik przeprowadzanych audytów w sektorze ICT i media świadczy zatem o większej świadomości zagrożeń i zabezpieczeń.

Należy także nadmienić, że aby testy penetracyjne przynosiły pozytywne efekty, muszą być powtarzane regularnie, a znalezione luki – odpowiednio zabezpieczone. Podobne stwierdzenie dotyczy także audytów zgodności. Sama wiedza o istniejących lukach to za mało, aby skutecznie ochronić organizację.

4. WYDATKI NA CYBERBEZPIECZEŃSTWO

WYSOKOŚĆ WYDATKÓW ZWIĄZANYCH Z CYBERBEZPIECZEŃSTWEM

ŚREDNIE I DUŻE FIRMY W POLSCE (2016)



Źródło PMR, 2017

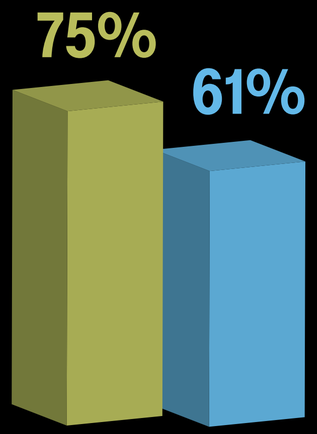
DO 50 TYS. ZŁ	51–100 TYS. ZŁ	101–250 TYS. ZŁ	POWYŻEJ 250 TYS. ZŁ

WYSOKOŚĆ WYDATKÓW ZWIĄZANYCH Z CYBERBEZPIECZEŃSTWEM
ŚREDNIE I DUŻE FIRMY W POLSCE W PODZIALE NA BRANŻE (2016)

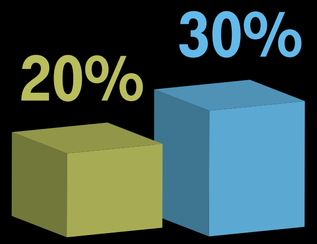
BRANŻE ▶	Produkcja dóbr szybko zbywalnych (żywności, napojów i chemii gospodarczej)	Handel hurtowy i detaliczny	ICT & media	Produkcja maszyn i urządzeń gotowych	Transport i logistyka	Przedsiębiorstwa użyteczności publicznej	Ochrona zdrowia	Pozostałe
Do 50 tys. zł	80%	67%	39%	70%	84%	77%	86%	77%
51–100 tys. zł	14%	14%	26%	18%	7%	11%	8%	13%
101–250 tys. zł	2%	13%	19%	10%	10%	3%	4%	5%
Powyżej 250 tys. zł	5%	6%	16%	3%	0%	9%	1%	5%

PLANOWANE ZMIANY BUDŻETU NA DZIAŁANIA ZWIĄZANE Z CYBERBEZPIECZEŃSTWEM

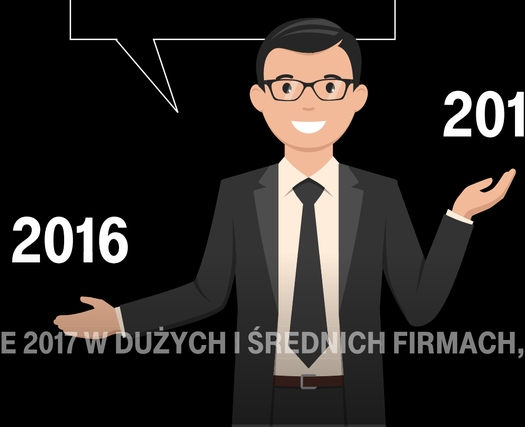
ŚREDNIE I DUŻE FIRMY W POLSCE (2017)

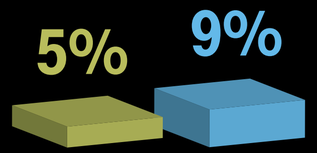


Porównywalny
do tego z 2016 r.

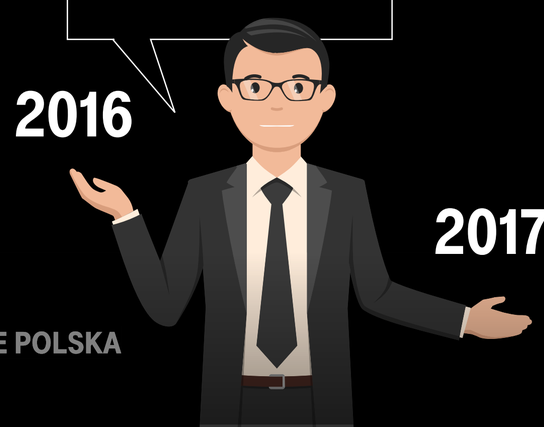


Większy
niż w 2016 r.

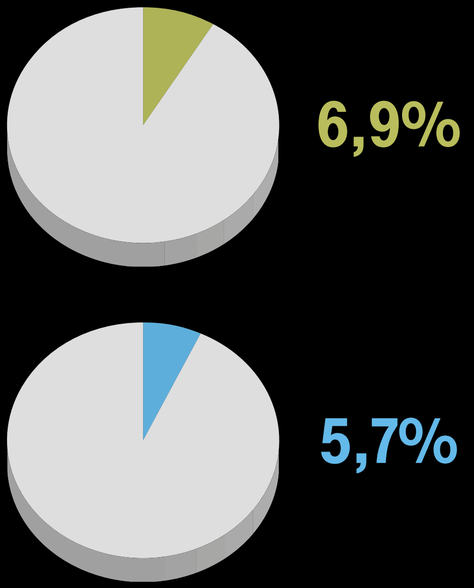




Mniejszy
niż w 2016 r.



DYNAMIKA



Źródło PMR, 2017

PLANOWANE ZMIANY BUDŻETU NA DZIAŁANIA ZWIĄZANE Z CYBERBEZPIECZEŃSTWEM

ŚREDNIE I DUŻE FIRMY W POLSCE W PODZIALE NA BRANŻE (2017)

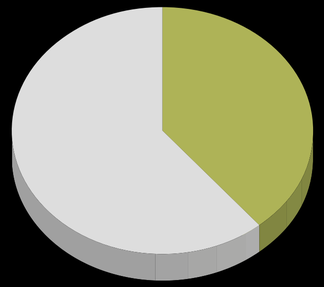
BRANŻE ▶	Produkcja dóbr szybko zbywalnych (żywności, napojów i chemii gospodarczej)	Handel hurtowy i detaliczny	ICT & media	Produkcja maszyn i urządzeń gotowych	Transport i logistyka	Przedsiębiorstwa użyteczności publicznej	Ochrona zdrowia	Pozostałe
Porównywalny do tego z 2016 r.	65%	70%	77%	63%	83%	75%	57%	76%
Większy niż w 2016 r.	28%	27%	23%	29%	12%	16%	29%	21%
Mniejszy niż w 2016 r.	7%	3%	0%	7%	5%	8%	14%	4%

PLANOWANA ZMIANA BUDŻETU ZWIĄZANEGO Z DZIAŁANIAMI W OBSZARZE CYBERBEZPIECZEŃSTWA W 2017 R.

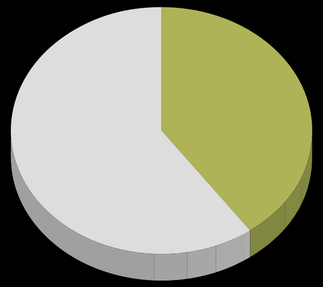
ŚREDNIE I DUŻE FIRMY W POLSCE W PODZIALE NA BRANŻE (2017)

BRANŻE ▶	Produkcja dóbr szybko zbywalnych (żywności, napojów i chemii gospodarczej)	Handel hurtowy i detaliczny	ICT & media	Produkcja maszyn i urządzeń gotowych	Transport i logistyka	Przedsiębiorstwa użyteczności publicznej	Ochrona zdrowia	Pozostałe
Cyberbezpieczeństwo	9,9%	3,5%	1,0%	7,1%	0,7%	0,0%	16,4%	0,1%

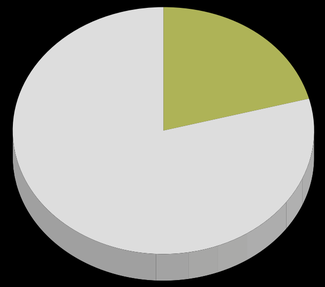
UDZIAŁ WYDATKÓW NA CYBERBEZPIECZEŃSTWO
ŚREDNIE I DUŻE FIRMY W POLSCE (2016)



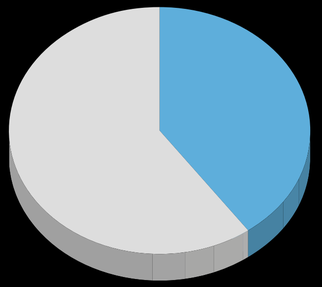
39%



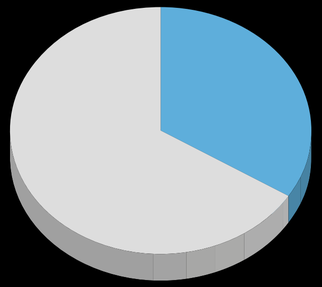
40%



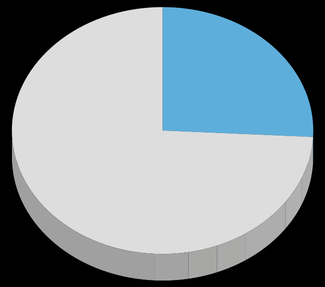
21%



40%



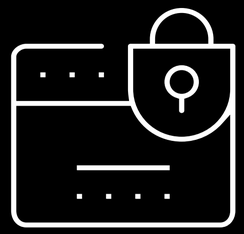
34%



26%

SPRZĘT

APLIKACJE
PROGRAMOWANIE I SYSTEMY



USŁUGI*

*W tym zakup dostępu do rozwiązań sprzętowych i aplikacyjnych w modelu usługowym.

Źródło PMR, 2017

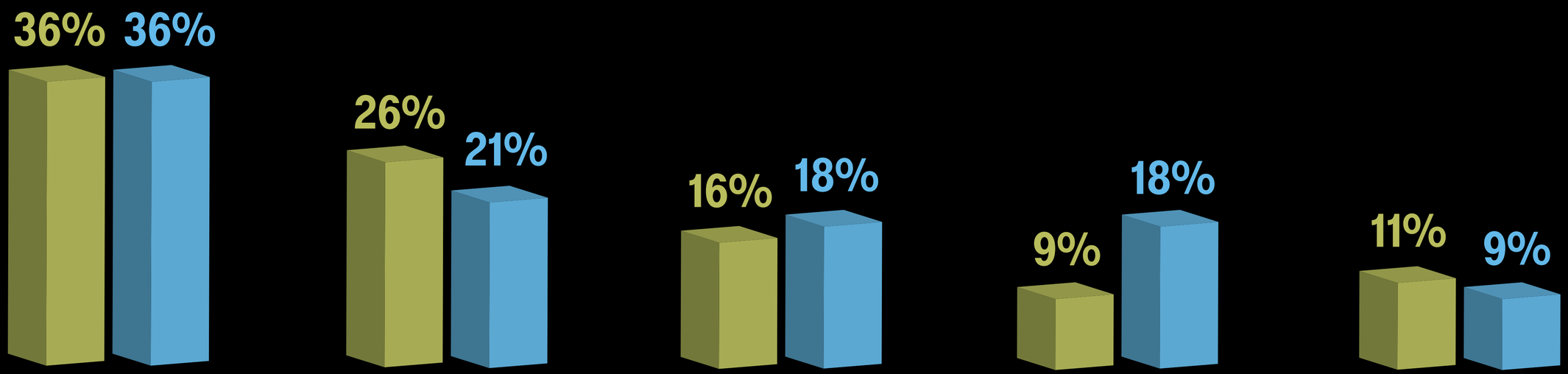
UDZIAŁ WYDATKÓW NA CYBERBEZPIECZEŃSTWO
ŚREDNIE I DUŻE FIRMY W POLSCE W PODZIALE NA BRANŻE (2016)

BRANŻE ▶	Produkcja dóbr szybko zbywalnych (żywności, napojów i chemii gospodarczej)	Handel hurtowy i detaliczny	ICT & media	Produkcja maszyn i urządzeń gotowych	Transport i logistyka	Przedsiębiorstwa użyteczności publicznej	Ochrona zdrowia	Pozostałe
Sprzęt	38%	40%	33%	42%	37%	38%	38%	43%
Aplikacje, oprogramowanie i systemy	45%	37%	36%	4%	39%	37%	40%	31%
Usługi*	17%	23%	31%	16%	26%	25%	22%	27%

*W tym zakup dostępu do rozwiązań sprzętowych i aplikacyjnych w modelu usługowym.

PROCENT WYDATKÓW PRZEZNACZONYCH NA DZIAŁANIA ZWIĄZANE Z CYBERBEZPIECZEŃSTWEM

ŚREDNIE I DUŻE FIRMY W POLSCE (2017)



Operacyjne centrum bezpieczeństwa

Ocena ryzyka
– skanery pasywne (hostowe), skanery aktywne (sieciowe)

Ład organizacyjny

Inteligentny wywiad
– mechanizmy zaawansowanego AI, pozwalające na identyfikację ukrytych ataków

Pozostałe

Źródło PMR, 2017

WYDATKI NA CYBERBEZPIECZEŃSTWO
NAJWAŻNIEJSZE WNIOSKI

Wydatki dużych i średnich przedsiębiorstw poniesione z tytułu działań w obszarze cyberbezpieczeństwa kształtują się na relatywnie niskim poziomie. **Trzy czwarte** badanych firm zadeklarowało, że na ten cel w 2016 r. przeznaczyło mniej niż **50 tys. zł**.

Warto też zwrócić uwagę na fakt, że ok. **7%** dużych firm działających w Polsce przeznaczyło w ubiegłym roku ponad **1 mln zł** na działania w obszarze cyberbezpieczeństwa.

Nie jest zaskakujące, że **duże firmy przeznaczały w 2016 r. większe kwoty na cyberbezpieczeństwo** niż średnie przedsiębiorstwa. Wyższe koszty były związane z większymi przychodami, które na ogół wypracowują duże podmioty, oraz z większymi zasobami IT do zabezpieczenia.

Struktura wydatków na działania w obszarze cyberbezpieczeństwa w dużych i średnich firmach nieznacznie się różni. O ile **średnie firmy wydają mniej więcej tyle samo na sprzęt** oraz oprogramowanie, to **duże firmy nieco większe kwoty przeznaczają na sprzęt**.

Zwiększenie budżetu na działania w obszarze cyberbezpieczeństwa w 2017 r. rozważa jedynie **co piąta** średnia i **co trzecia** duża firma.

WYDATKI NA CYBERBEZPIECZEŃSTWO – OPINIA EKSPERTA T-MOBILE

Arkadiusz Buczek
Główny Specjalista
ds. Cyberbezpieczeństwa,
T-Mobile Polska S.A.

Zgodnie z najlepszymi praktykami budżet przeznaczany na cyberbezpieczeństwo powinien stanowić nie mniej niż 10% budżetu IT. Dlatego wydatki do 50 tys. odnotowane u 84% średnich przedsiębiorstw mogą odzwierciedlać racjonalny poziom kosztów ponoszonych przez firmy, choć wydają się one nieproporcjonalnie małe w stosunku do kar, które będą obowiązywały w ramach RODO/GDPR.

Większość respondentów nie planuje podniesienia wydatków na bezpieczeństwo – dynamika zmian na poziomie 6–7% wskazuje raczej na wzrost inflacyjny niż inwestycję w nowe rozwiązania. Stagnacja w obszarze zabezpieczeń jest niepokojąca i wynika z braku świadomości zagrożeń. W przypadku, gdy firmy nie widzą skutków ataków, konsekwencją jest zaniechanie inwestycji w dodatkowe zabezpieczenia. Równocześnie korzystanie z usług pentestów wzmacnia przeświadczenie o byciu twierdzą nie do zdobycia, co powoduje, że w rezultacie przedsiębiorstwa pozostają w tym samym miejscu – z zabezpieczeniami w postaci firewalla, antywirusa, bez procedur zarządzania bezpieczeństwem.

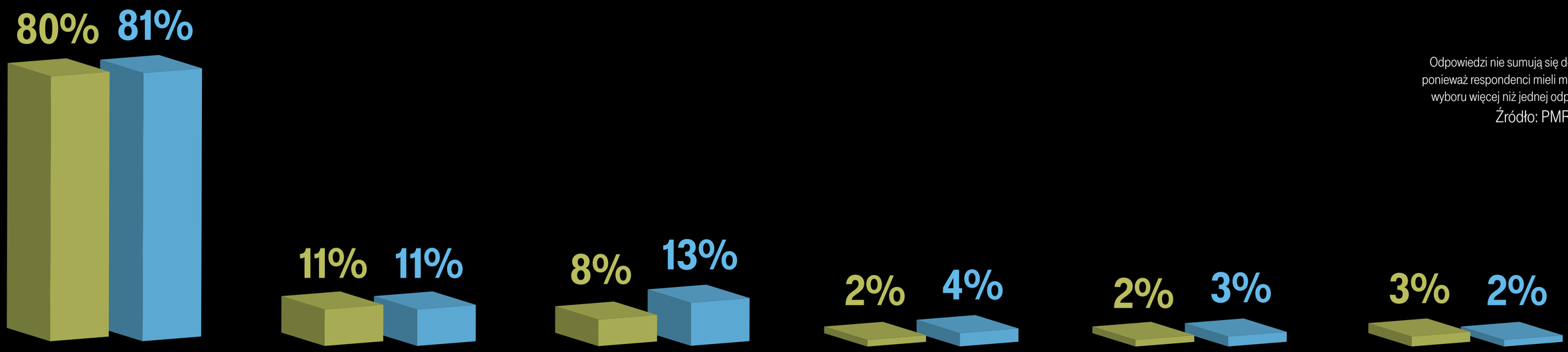
Ciekawe jest, że w tym roku tylko branża ICT i media nie planuje zmniejszyć wydatków na cyberbezpieczeństwo. Jest to również sektor, w którym wydatki na bezpieczeństwo przekraczają 250 tys. zł, podczas gdy w pozostałych branżach inwestuje praktycznie co dziesiąta firma. Choć spadek wydatków w większości branż względem roku poprzedniego jest niepokojący, może wynikać z wyższych kosztów z tytułu inwestycji w sprzęt lub ludzi w 2016 roku, które jednak nie są ponoszone co roku.

Średnie firmy – ze względu na ograniczone zasoby ludzkie – najwięcej środków inwestują w zautomatyzowane rozwiązania, tj. systemy i aplikacje (40%). W dużych przedsiębiorstwach, gdzie infrastruktura może być bardziej rozległa, koszt sprzętu stanowi główny wydatek (40%). Ze zgromadzonych danych jednoznacznie wynika, że spółki najchętniej inwestują we własną infrastrukturę, nie w usługi.
Tu znów wiedzie prym branża ICT i media, choć można założyć, że korzysta ona z własnych usług i traktuje je jako inwestycje. Działania zamykające się w granicach firmy mogą wprawdzie podnosić jej wartość, jednocześnie wskazują one jednak na pewną stagnację i brak korzystania z zaawansowanych rozwiązań, których głównym kosztem są zatrudnione zespoły, takie jak threat intelligence, centra monitoringu czy zespoły reagowania na incydenty.

5. ZNACZENIE FIRM ZEWNĘTRZNYCH I WŁASNYCH SPECJALISTÓW W ZAKRESIE CYBERBEZPIECZEŃSTWA

MODEL WDRAŻANIA PRODUKTÓW I USŁUG Z ZAKRESU CYBERBEZPIECZEŃSTWA

ŚREDNIE I DUŻE FIRMY W POLSCE (2017)



Odpowiedzi nie sumują się do 100%, ponieważ respondenci mieli możliwość wyboru więcej niż jednej odpowiedzi.

Źródło: PMR, 2017

Sami kupujemy i wdrażamy rozwiązania oraz zarządzamy usługami we własnym zakresie	Zakupem sprzętu, wdrożeniem rozwiązań i serwisem zajmuje się integrator natomiast sami zarządzamy usługami końcowymi	Zakupem sprzętu, wdrożeniem rozwiązań, serwisem i zarządzaniem usługami końcowymi zajmuje się integrator	Usługi dostarcza operator telekomunikacyjny, ale zarządzamy nimi we własnym zakresie	Usługi dostarcza i zarządza nimi operator telekomunikacyjny	Inny model

MODEL WDRAŻANIA PRODUKTÓW I USŁUG Z ZAKRESU CYBERBEZPIECZEŃSTWA

ŚREDNIE I DUŻE FIRMY W POLSCE W PODZIALE NA BRANŻE (2017) (CZĘŚĆ I)

BRANŻE ▶	Produkcja dóbr szybko zbywalnych (żywności, napojów i chemii gospodarczej)	Handel hurtowy i detaliczny	ICT & media	Produkcja maszyn i urządzeń gotowych	Transport i logistyka	Przedsiębiorstwa użyteczności publicznej	Ochrona zdrowia	Pozostałe
Sami kupujemy i wdrażamy rozwiązania oraz zarządzamy usługami we własnym zakresie	80%	78%	91%	74%	74%	86%	82%	87%
Zakupem sprzętu, wdrożeniem rozwiązań i serwisem zajmuje się integrator (zewnętrzny dostawca usług IT) – natomiast sami zarządzamy usługami końcowymi	11%	10%	9%	14%	15%	10%	12%	4%
Zakupem sprzętu, wdrożeniem rozwiązań, serwisem i zarządzaniem usługami końcowymi zajmuje się integrator	14%	13%	14%	12%	10%	9%	5%	10%

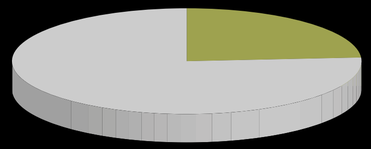
MODEL WDRAŻANIA PRODUKTÓW I USŁUG Z ZAKRESU CYBERBEZPIECZEŃSTWA

ŚREDNIE I DUŻE FIRMY W POLSCE W PODZIALE NA BRANŻE (2017) (CZĘŚĆ II)

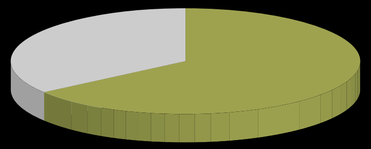
BRANŻE ▶	Produkcja dóbr szybko zbywalnych (żywności, napojów i chemii gospodarczej)	Handel hurtowy i detaliczny	ICT & media	Produkcja maszyn i urządzeń gotowych	Transport i logistyka	Przedsiębiorstwa użyteczności publicznej	Ochrona zdrowia	Pozostałe
Usługi dostarcza operator telekomunikacyjny, ale zarządzamy nimi we własnym zakresie	0%	7%	0%	3%	4%	3%	3%	0%
Inny model	7%	2%	0%	1%	2%	1%	1%	7%
Usługi dostarcza i zarządza nimi operator telekomunikacyjny	2%	2%	0%	4%	0%	2%	3%	3%

ZATRUDNIANIE SPECJALISTY Z OBSZARU CYBERBEZPIECZEŃSTWA

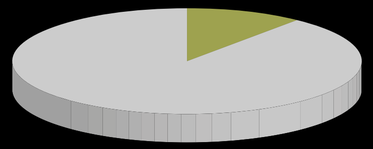
ŚREDNIE I DUŻE FIRMY W POLSCE (2017)



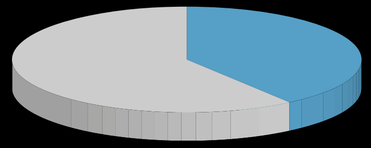
24%



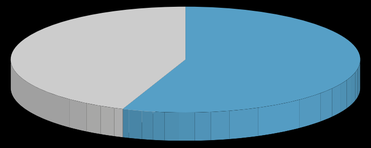
65%



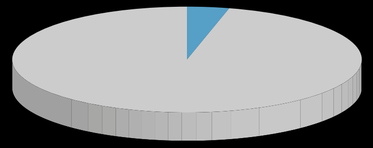
11%



40%



56%



4%

TAK

NIE
i nie planujemy zatrudnienia

NIE
ale planujemy zatrudnienie

Źródło: PMR, 2017

ZATRUDNIANIE SPECJALISTY Z OBSZARU CYBERBEZPIECZEŃSTWA
ŚREDNIE I DUŻE FIRMY W POLSCE W PODZIALE NA BRANŻE (2017)

BRANŻE ▶	Produkcja dóbr szybko zbywalnych (żywności, napojów i chemii gospodarczej)	Handel hurtowy i detaliczny	ICT & media	Produkcja maszyn i urządzeń gotowych	Transport i logistyka	Przedsiębiorstwa użyteczności publicznej	Ochrona zdrowia	Pozostałe
Nie i nie planujemy zatrudnienia	66%	65%	39%	64%	68%	61%	61%	46%
Tak	26%	31%	61%	28%	26%	29%	29%	40%
Nie, ale planujemy zatrudnienie	9%	3%	0%	8%	6%	10%	10%	13%

PLANY KORZYSTANIA Z USŁUG ZEWNĘTRZNYCH FIRM I WŁASNYCH SPECJALISTÓW W ZAKRESIE CYBERBEZPIECZEŃSTWA

NAJWAŻNIEJSZE WNIOSKI

Przedstawiciele 80% badanych firm z sektora dużych i średnich przedsiębiorstw zadeklarowali, że sami kupują, wdrażają oraz zarządzają rozwiązaniami z zakresu cyberbezpieczeństwa.

Dwie piąte dużych i tylko co piąta średnia firma zatrudnia specjalistę odpowiedzialnego za obszar bezpieczeństwa cyfrowego.

Obawy o wyższe koszty są szczególnie widocznie wśród średnich firm, co jest zrozumiałe, gdyż generują one niższe przychody niż duże firmy.

Większe firmy częściej decydują się na zatrudnienie specjalnej osoby odpowiedzialnej za cyberbezpieczeństwo, ponieważ – jak wynika z deklaracji badanych – częściej borykają się z problemem cyberataków.

ZNACZENIE FIRM ZEWNĘTRZNYCH I WŁASNYCH SPECJALISTÓW – OPINIA EKSPERTA T-MOBILE

Sebastian Pióro
Główny Specjalista ds. Produktu ICT,
T-Mobile Polska S.A.

Większość przedsiębiorstw nie tworzy oddzielnych stanowisk dla osób, których podstawowym obowiązkiem jest dbanie o bezpieczeństwo. Z badania wynika, że aż 61% firm nie planuje poszukiwania specjalisty z tej dziedziny. Obowiązki te przydzielane są zazwyczaj pracownikom działu IT – administratorom systemów i/lub sieci. Badanie pokazuje także, że firmy nie odczuwają skutków ataków, dlatego też nie decydują się na zatrudnienie ekspertów z zakresu cyberbezpieczeństwa.

Na tle badanych firm wyróżnia się branża ICT i media, w której 61% przedsiębiorstw już posiada dedykowane stanowisko ds. cyberbezpieczeństwa. Proporcje są zatem odwrócone w stosunku do pozostałych branż, wśród których około 60% respondentów nie ma takiego stanowiska.

Co ciekawe, zbliżające się zmiany w prawie RODO/GDPR nie przekładają się na plany zatrudnienia specjalistów. Pod tym względem deklarowane działania stanowią odwrotność przewidywań i sytuacji na rynku pracy. Zgodnie z wynikami badania infrastruktura zabezpieczeń jest w tych przedsiębiorstwach nieskomplikowana, dlatego zmiany prawne (RODO) sprowadzają się jedynie do szkoleń pracowników.

Większość firm inwestuje we własny sprzęt i ludzi (80%), natomiast z outsourcingu ekspertów lub zasobów korzysta co szóste przedsiębiorstwo. Jednak poziom zaufania do zewnętrznych dostawców, w szczególności operatorów usług z zakresu bezpieczeństwa, powinien z każdym rokiem rosnąć. Wynika to przede wszystkim z ograniczonej liczby kompetencji w kwestii cyberbezpieczeństwa na rynku oraz wysokich kosztów zatrudnienia specjalistów pokrywających wszystkie obszary zabezpieczeń środowiska IT.

USŁUGI BEZPIECZEŃSTWA W OFERCIE T-MOBILE

T-Mobile jest dostawcą usług zarządzanego bezpieczeństwa (tzw. managed security services), obejmujących rozwiązania takie jak:

SECURITY OPERATIONS CENTER

monitorowanie i rozwiązywanie incydentów bezpieczeństwa przez zespół SOC

USŁUGI PROFESJONALNE

od audytów bezpieczeństwa, szkoleń, testów penetracyjnych począwszy, po doradztwo w zakresie najlepszych praktyk przy budowie systemów zabezpieczeń IT

NEXT GENERATION FIREWALL

zabezpieczenie styku z Internetem za pomocą zarządzanego firewalla następnej generacji

OCHRONA PRZED ATAKAMI DDoS

wolumetrycznymi i aplikacyjnymi

WEB APPLICATION FIREWALL

zabezpieczenie systemów i aplikacji webowych (w chmurze prywatnej, publicznej, lokalnych) przy użyciu zarządzanego firewalla aplikacyjnego

PODSUMOWANIE – OKIEM ANALITYKA

Paweł Olszynka
Head IT&Telecoms Analyst, PMR

Analiza trendów w obszarze ICT na krajowym rynku B2B wskazuje na zderzenie dwóch trwałych tendencji. Niezmiennie polskie przedsiębiorstwa inwestują przede wszystkim we własny sprzęt, rozbudowują i utrzymują własne systemy. Równolegle rośnie wykorzystanie chmury, głównie w modelu hybrydowym. Nawet najbardziej konserwatywni klienci coraz rzadziej negują elastyczność, skalowalność, potencjał i możliwości, jakie daje cloud computing. Mimo dynamicznego rozwoju, problemem pozostaje skala. Udział chmury w wydatkach na sprzęt czy w relacji do zakupów klasycznych licencji softwareowych i utrzymania własnych systemów pozostaje w Polsce na niskim, jednocyfrowym poziomie.

Tegoroczne badania strony popytowej realizowane przez PMR potwierdzają, że odbiorcy IT nadal są mocno skoncentrowani na utrzymaniu własnych zasobów i jest to zdecydowanie priorytet firm w krótkim okresie. Na drugim miejscu znajduje się zapewnienie bezpieczeństwa. W przypadku tej dość szerokiej kategorii przedsiębiorcy wskazują na chęć inwestycji zarówno w rozwiązania sprzętowe oraz aplikacyjne, utrzymywane we własnym zakresie, jak również zakup usług z obszaru cyberbezpieczeństwa od zewnętrznego dostawcy. Trzecia pozycja to mobilność i zapewnienie zdalnego dostępu do zasobów. Z badań strony podażowej, przeprowadzanych cyklicznie przez PMR, wynika, że największe firmy IT, działające w Polsce, pytane o bieżące trendy na rynku, wskazują zdecydowanie na chmurę, mobilność i cyberbezpieczeństwo. Widać więc zgodność percepcji przedstawicieli popytu i podaży, co należy brać za dobrą monetę.

Najważniejszy wniosek to rosnące znaczenie cyberbezpieczeństwa, które znajduje się na liście priorytetów polskich firm, jeśli chodzi o wydatki na IT. Nie powinno to specjalnie dziwić, bo temat jest wielowymiarowy. Zapewnienie bezpieczeństwa ważne jest w każdym przypadku: chmury, dostępu zdalnego, utrzymania infrastruktury własnej, wykorzystania bardziej zaawansowanych narzędzi analitycznych, Internetu Rzeczy itp. Można się spierać, na ile jest to teoria i tylko deklaracje, że bezpieczeństwo ma priorytet, ale faktem jest, że presja rośnie. Najmocniej oczywiście działają bezpośrednie, negatywne doświadczenia i straty własne, ale swoje robi też stale rosnący poziom zagrożeń cyberatakami, malware i ransomware. Dodatkowo pojawienie się nowych regulacji unijnych w obszarze danych osobowych (RODO) tylko wymusza dostosowanie się firm i potencjalne inwestycje. Co warto jeszcze raz podkreślić, cyberbezpieczeństwo jest tematem ważnym, niezależnie od sposobu dostępu do infrastruktury. Nie jest istotne, jak szybko i w jakim stopniu nastąpi migracja polskich firm w kierunku chmury. Zapewnienie bezpieczeństwa danych i wykorzystywanych systemów jest niezależne od wyniku starcia: własne zasoby kontra chmura. Zarówno w jednym, jak i w drugim przypadku cyberbezpieczeństwo nie straci na znaczeniu.

METODOLOGIA BADANIA

1. Próba

W badaniu wykorzystano losową, warstwową próbę firm zatrudniających 50-249 osób oraz co najmniej 250 osób reprezentujących sektory gospodarki pokazane na schemacie. Próba została dobrana z bazy danych jednego z liderów wśród firm dostarczających bazy kontaktowe B2B. W badaniu nie uwzględniono stowarzyszeń, służb mundurowych i administracji publicznej.

METODOLOGIA BADANIA

W sumie zrealizowano 681 pełnowartościowych wywiadów (334 ze średnimi firmami oraz 347 z dużymi). Respondentami były osoby posiadające najlepszą wiedzę na temat wykorzystywanych rozwiązań w obszarze IT i telekomunikacji w firmie. Dużą liczbę wywiadów przeprowadzono także z osobami zajmującymi najwyższe stanowiska kierownicze (np. dyrektor finansowy, prezes, wiceprezes) w badanych firmach.

2. Technika badawcza

Badanie zostało przeprowadzone techniką wywiadu telefonicznego CATI z użyciem wystandaryzowanego kwestionariusza wywiadu. Wywiady zostały wykonane przez studio PMR w Krakowie.

T-Mobile Polska S.A.
ul. Marynarska 12
02-674 Warszawa

Więcej informacji o usługach:
www.t-mobile.pl/biznes

LIFE IS FOR SHARING.