DELL EMC

ZARZĄDZANIE I ZABEZPIECZANIE DANYCH W KONTEKŚCIE NOWYCH WYZWAŃ DZIAŁÓW IT

Rola działu IT w przygotowaniu do RODO

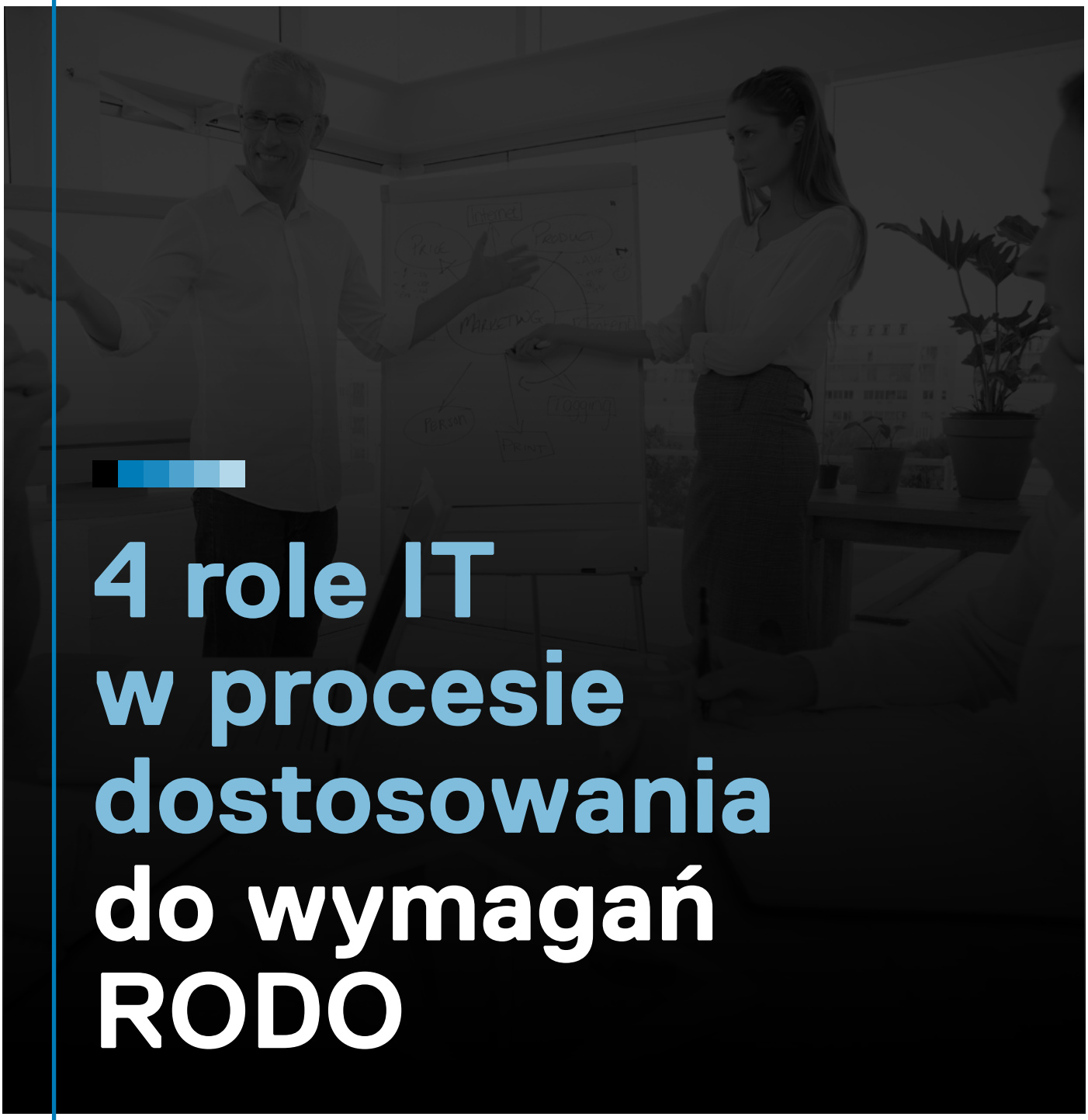
Badanie: podejście polskich firm do RODO

Co zrobić, aby nic nas nie zaskoczyło **w obszarze zabezpieczania danych**

Badanie: zmieniająca się rola CIO i nowe zasady współpracy z działami biznesowymi

Dell EMC: jak rozwinie się polski rynek IT?

RAPORT OPRACOWANY PRZEZ ITWIZ



4 role IT w procesie dostosowania do wymagań RODO

Wdrożenie wymagań Rozporządzenia ogólnego o ochronie danych osobowych jest wyzwaniem, które organizacja musi podjąć jako całość. Być może nie jest to intuicyjne, bo ochrona danych osobowych jest często błędnie pojmowana jako wyłączna kompetencja departamentu prawnego, Compliance lub dedykowanego zespołu administratora bezpieczeństwa informacji. Jako taka nie znajduje się więc w obszarze zainteresowania innych linii serwisowych.

Tymczasem, nowe podejście do ochrony danych osobowych – wprowadzane przez unijne rozporządzenie 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (Rozporządzenie ogólne) – wymaga, aby ochrona danych osobowych została wpisana w DNA organizacji.

Filozofia Privacy by Design, będąca jednym ze znaków rozpoznawczych Rozporządzenia ogólnego, może być realizowana w praktyce tylko wtedy, gdy w realizację zadań związanych z ochroną prywatności zostanie zaangażowana cała organizacja. Z uwagi na to, że duża część istotnych procesów przetwarzania danych odbywa się z reguły z wykorzystaniem systemów IT, szczególna rola w procesie dostosowania przypada szeroko rozumianemu IT.

ZAPEWNIENIE ORGANIZACYJNYCH I TECHNICZNYCH ŚRODKÓW BEZPIECZEŃSTWA

Najbardziej intuicyjnym wymiarem działań IT, w obszarze dostosowania firmy do nowych wymagań ochrony danych osobowych, jest wdrożenie organizacyjnych i technicznych środków zapewniających bezpieczeństwo przetwarzania danych. Przykładowy, wskazany w Rozporządzeniu ogólnym katalog funkcji i procedur, które można wdrożyć w tym celu, obejmuje: pseudonimizację i szyfrowanie danych osobowych; zdolność do ciągłego zapewnienia poufności, integralności, dostępności i odporności systemów i usług przetwarzania; zdolność do szybkiego przywrócenia dostępności danych osobowych i dostępu do nich w razie incydentu fizycznego lub technicznego; regularne testowanie, mierzenie i ocenianie skuteczności środków technicznych i organizacyjnych mających zapewnić bezpieczeństwo przetwarzania.

Decyzja o zastosowaniu tych lub innych technicznych i organizacyjnych środków bezpieczeństwa powinna być poprzedzona analizą ryzyka, związanego z przetwarzaniem danych osobowych, w konkretnym procesie lub grupie podobnych procesów przetwarzania. Adekwatność wykorzystanych środków będzie ostatecznie oceniana właśnie z perspektywy ryzyka. Realnym problemem może się okazać dopasowanie odpowiedniego standardu zabezpieczeń do zidentyfikowanego poziomu ryzyka. Pomocne w tym zakresie będą standardy i dobre praktyki stosowane na rynku, w tym standardy sektorowe, stworzone z myślą o zaadresowaniu ryzyk typowych dla danego sektora. Ostatecznie, to jednak administrator i podmiot przetwarzający będą musieli podjąć decyzję o tym, jakie środki bezpieczeństwa zastosować, biorąc pod uwagę, obok zidentyfikowanego poziomu ryzyka, także stan wiedzy technicznej oraz koszt wdrażania dostępnych rozwiązań.

RODO umożliwia otrzymanie w ustrukturyzowanym, powszechnie używanym formacie nadającym się do odczytu maszynowego danych osobowych, które podmiot danych dostarczył administratorowi, oraz przesłanie tych danych osobowych innemu administratorowi. Stosownie do wytycznych Grupy Roboczej art. 29, **możliwe ma być pobranie przez użytkownika pliku zawierającego komplet dostarczonych przez niego danych osobowych lub, o ile będzie to możliwe, umożliwienie pobrania danych przez innego administratora, przy wykorzystaniu odpowiednio skonfigurowanego i zabezpieczonego API.**

Rozporządzenie RODO przewiduje m.in. prawo osoby fizycznej do uzyskania od administratora potwierdzenia, czy przetwarzane są dane osobowe jej dotyczące, a jeżeli ma to miejsce, do uzyskania dostępu do nich (otrzymania kopii) oraz informacji obejmujących m.in. cel przetwarzania, kategorie danych osobowych, informację o odbiorcach danych, planowanym okresie przechowywania danych, a także źródle, z którego pochodzą dane. **Zadanie pozornie tylko jest nieskomplikowane. W praktyce zebranie w jednym miejscu i w krótkim czasie informacji dotyczących konkretnej osoby może stanowić wyzwanie.**

WSPARCIE REALIZACJI PRAW PODMIOTÓW DANYCH

Drugim wymiarem działań IT w procesie dostosowywania organizacji do wymagań Rozporządzenia ogólnego jest wsparcie realizacji praw osób, których dotyczą dane osobowe. Rozporządzenie ogólne przewiduje szerokie uprawnienia podmiotów danych, z których większość pozornie nie odnosi się do IT, jednak ich realizację w średniej lub dużej organizacji trudno sobie wyobrazić bez istotnego udziału IT.

Rozporządzenie ogólne przewiduje m.in. prawo osoby fizycznej do uzyskania od administratora potwierdzenia, czy przetwarzane są dane osobowe jej dotyczące, a jeżeli ma to miejsce, do uzyskania dostępu do nich (otrzymania kopii) oraz informacji obejmujących m.in. cel przetwarzania, kategorie danych osobowych, informację o odbiorcach danych, planowanym okresie przechowywania danych, a także źródle, z którego pochodzą dane. Zadanie pozornie tylko jest nieskomplikowane. W praktyce zebranie w jednym miejscu i w krótkim czasie informacji dotyczących konkretnej osoby może stanowić wyzwanie, szczególnie jeśli dane są rozproszone po wielu bazach danych i wielu systemach, które niekoniecznie się ze sobą komunikują.

Ponadto problemem może być, w przypadku niektórych administratorów, liczba tego typu wniosków. O ile obsługa kilku takich wniosków miesięcznie mogłaby zapewne odbywać się „ręcznie", o tyle większa liczba zapytań może stanowić poważne wyzwanie organizacyjne. Z tego powodu organizacje, które ze względu na specyfikę działalności mogą się spodziewać zwiększenia liczby wniosków, które trzeba będzie obsłużyć, powinny rozważyć wdrożenie do swoich systemów informatycznych funkcjonalności, wspierającej agregację danych osobowych z różnych baz i różnych systemów.

Innym prawem podmiotów danych, którego realizacja wymaga wsparcia IT, jest prawo do ograniczenia przetwarzania. Treścią tego prawa jest ograniczenie sposobu wykorzystania danych osobowych w ten sposób, że będą mogły zostać wykorzystane tylko do określonych celów. W skrajnym przypadku dane będą musiały być przechowywane, jednak nie będą mogły być przetwarzane w żaden inny sposób. Realizacja tego prawa wymaga, aby dane osobowe były odpowiednio oznaczone w systemach IT, w sposób gwarantujący, że dane nie zostaną wykorzystane wbrew uprawnieniu do ograniczenia ich przetwarzania.

Prawem podmiotów danych odnoszącym się bezpośrednio do obszaru IT jest prawo do przenoszenia danych. Prawo to ma zastosowanie wyłącznie do przetwarzania zautomatyzowanego oraz odbywającego się na podstawie zgody lub umowy, a zatem będzie mogło być realizowane m.in. wobec dostawców usług elektronicznych, w tym platform e-commerce, sieci społecznościowych itp. Prawo umożliwia otrzymanie w ustrukturyzowanym, powszechnie używanym formacie nadającym się do odczytu maszynowego danych osobowych, które podmiot danych dostarczył administratorowi, oraz przesłanie tych danych osobowych innemu administratorowi. Realizacja tego prawa wymaga, stosownie do wytycznych Grupy Roboczej art. 29, umożliwienia pobrania przez użytkownika pliku zawierającego komplet dostarczonych przez niego danych osobowych lub, o ile będzie to możliwe, umożliwienia pobrania danych przez innego administratora, przy wykorzystaniu odpowiednio skonfigurowanego i zabezpieczonego API.

DOSTOSOWANIE WŁASNYCH PROCESÓW IT

Trzeci wymiar roli IT w procesie dostosowywania do wymagań Rozporządzenia ogólnego wiąże się z koniecznością opisania, oceny i dostosowania tych procesów przetwarzania danych osobowych, których właścicielem biznesowym jest IT. Takie procesy trzeba w pierwszej kolejności zidentyfikować, ich liczba i rodzaj mogą się znacznie różnić między różnymi organizacjami, jednak z całą pewnością występują w każdej firmie, nawet jeśli organizacja korzysta z outsourcingu funkcji IT. Przykładem takiego procesu jest testowanie oprogramowania, które w wielu firmach odbywa się z wykorzystaniem kopii danych rzeczywistych.

Potencjalnie taki proces testowania może się wiązać z wysokim ryzykiem dla praw i wolności osób fizycznych, zwłaszcza jeśli obejmuje przetwarzanie danych szczególnie wrażliwych, np. danych dotyczących stanu zdrowia czy danych objętych tajemnicami zawodowymi. Taki proces powinien zostać opisany w rejestrze czynności przetwarzania, przeanalizowany z punktu widzenia zgodności z podstawowymi zasadami i wymaganiami formalnymi Rozporządzenia ogólnego oraz odpowiednio dostosowany, tak aby ewentualne ryzyka związane z procesem były adekwatnie zabezpieczone. IT, jako właściciel biznesowy procesu testowania, będzie musiał wziąć udział w opisaniu procesu, zebrać informacje i dokumenty, które go dotyczą, a następnie zdecydować o sposobie i zakresie dostosowania procesu do rekomendacji wynikających z analizy procesu i ryzyka z nim związanego.

Przykładowy, wskazany w Rozporządzeniu ogólnym katalog funkcji i procedur, które można wdrożyć, aby być zgodnym z RODO:

- **pseudonimizacja i szyfrowanie danych osobowych;**
- **zdolność do ciągłego zapewnienia poufności,** integralności, dostępności i odporności systemów i usług przetwarzania;
- **zdolność do szybkiego przywrócenia dostępności danych osobowych** i dostępu do nich w razie incydentu fizycznego lub technicznego;
- **regularne testowanie, mierzenie i ocenianie skuteczności środków technicznych i organizacyjnych** mających zapewnić bezpieczeństwo przetwarzania.

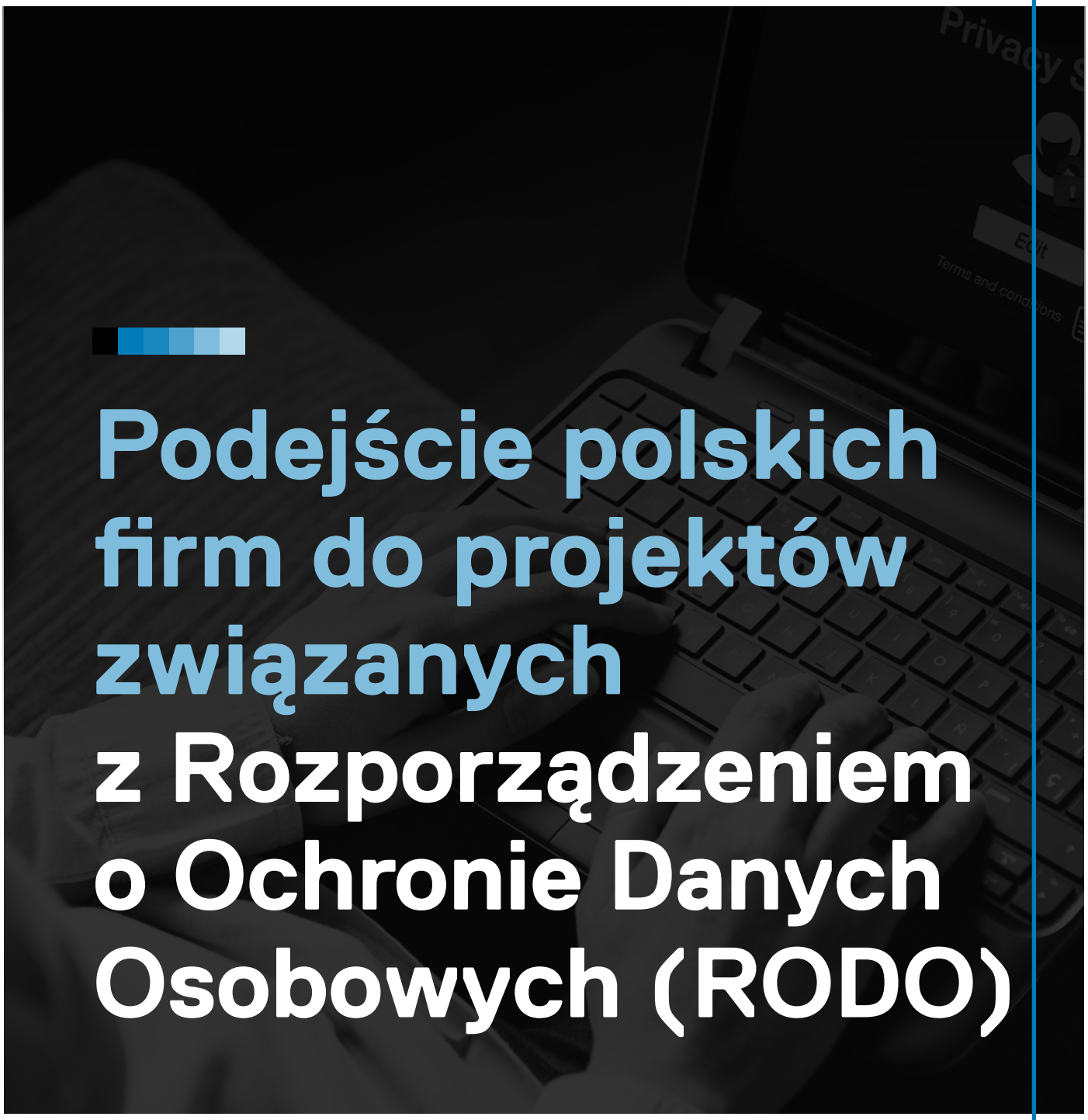
Decyzja o zastosowaniu tych lub innych technicznych i organizacyjnych środków bezpieczeństwa w związku ze spełnieniem wymogów RODO powinna być poprzedzona analizą ryzyka, związanego z przetwarzaniem danych osobowych, w konkretnym procesie lub grupie podobnych procesów przetwarzania. Adekwatność zastosowanych środków będzie ostatecznie oceniana właśnie z perspektywy ryzyka. **Praktycznym problemem może się okazać dostosowanie odpowiedniego standardu zabezpieczeń do zidentyfikowanego poziomu ryzyka.**

OPROGRAMOWANIE WSPIERAJĄCE INNE ZADANIA W OBSZARZE OCHRONY PRYWATNOŚCI

Ostatnim wymiarem roli IT w dostosowaniu do Rozporządzenia ogólnego jest dostarczenie (wsparcie w wyborze) i obsługa oprogramowania wspierającego działania organizacji w obszarze ochrony prywatności. Do takiego oprogramowania trzeba zaliczyć aplikacje wspierające funkcję inspektora ochrony danych poprzez agregowanie, porządkowanie, archiwizowanie i prezentowanie informacji o procesach przetwarzania danych osobowych w organizacji (mapa procesów). Średnim i dużym firmom trudno będzie efektywnie zarządzać obszarem ochrony danych osobowych, w tym analizować procesy przetwarzania i weryfikować ich zgodność z Rozporządzeniem ogólnym oraz bez wsparcia w postaci odpowiedniego oprogramowania.

Ponadto, oprogramowanie powinno wspierać realizację zasady rozliczalności, zgodnie z którą administrator ma obowiązek wykazania zgodności swoich działań z prawem. Zgodność danego działania z prawem nie jest wystarczająca do spełnienia wymagań Rozporządzenia ogólnego. Konieczna jest także zdolność organizacji do wykazania tej zgodności. Oprogramowanie może skutecznie wspierać proces tworzenia i utrwalania informacji, które będą mogły posłużyć do wykazania zgodności z określonymi wymaganiami Rozporządzenia ogólnego. Przykładowo, w przypadku zbierania za pośrednictwem portalu internetowego zgód na przetwarzanie danych osobowych w celach marketingowych, odpowiednie oprogramowanie pozwoli odnotować fakt wykonania przez użytkownika działań, odpowiadających złożeniu oświadczenia o zgodzie na przetwarzanie danych osobowych, a także powiązać z nim informację o czasie, w którym zgoda została udzielona, zakresie zgody (oznaczonych i nieoznaczonych checkboxach) oraz wykonaniu obowiązku informacyjnego i jego treści. Odpowiednie oprogramowanie będzie również w stanie wspierać proces obiegu dokumentacji i podejmowania decyzji w sprawach, które mogą dotyczyć ochrony prywatności oraz go dokumentować na potrzeby realizacji zasady rozliczalności.

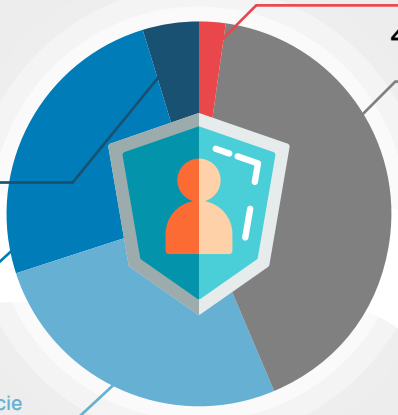
Sławomir Kowalski
W kancelarii Maruta Wachta sp.j. koordynuje prace w zakresie projektów dotyczących ochrony danych osobowych. Jego doświadczenie obejmuje również doradztwo transakcyjne w zakresie praw własności intelektualnej, doradztwo przy projektach badawczych i rozwojowych, a także reprezentację w postępowaniach karnych i cywilnych dotyczących naruszeń praw własności intelektualnej, tajemnic prawnie chronionych oraz czynów nieuczciwej konkurencji.



Podejście polskich firm do projektów związanych z Rozporządzeniem o Ochronie Danych Osobowych (RODO)

Aż 26% firm zaplanowało projekty związane z RODO na II połowę tego roku, a kolejne 25% czeka na polskie przepisy dotyczące tego rozporządzenia. Zdaniem 62% ankietowanych, RODO to jeden z wielu priorytetów, a dla ponad 3% jest on najważniejszy. W przypadku 23% firm budżet przeznaczony na projekty związane z dostosowaniem się do RODO wyniesie od 100 tys zł. do 500 tys. zł.

Podejście polskich firm do projektów związanych z RODO



2,3% – już zakończyło ten projekt

41,3% – prowadzi przygotowania do wdrożenia GDPR

4,6% – nie planuje takich projektów

25,3% – czeka na polskie ustawy

26,5% – planuje rozpoczęcie ich w II połowie 2017 roku

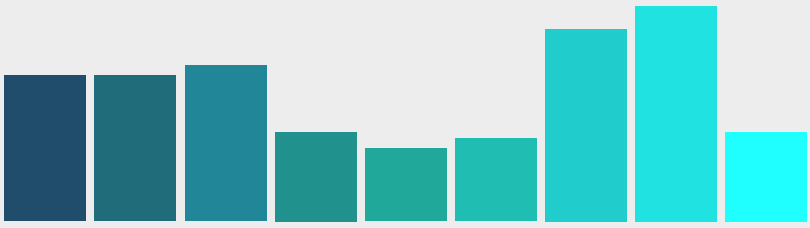
Jak ważne są dla firm w Polsce projekty związane z wdrożeniem RODO?

62,0% – to jeden z wielu priorytetów

3,5% – są najważniejszym projektem

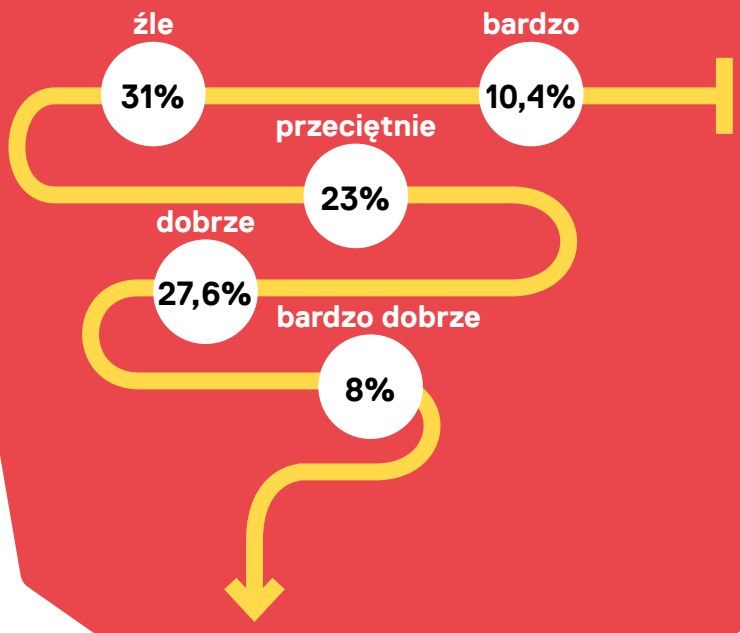
34,5% – projekt ten nie jest najważniejszy

Jakiego typu projekty związane z RODO zamierzają przeprowadzić firmy w Polsce?

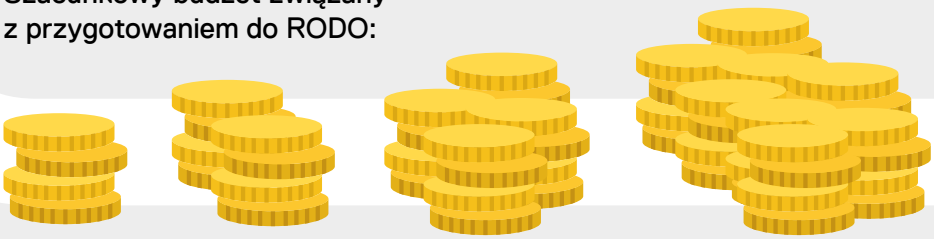


- **51%** Określenie, gdzie i w jaki sposób przechowywane są dane klientów.
- **51%** Wprowadzenie zmian w procesach związanych z przetwarzaniem danych osobowych.
- **54%** Zmiany w systemach IT, w których przetwarzane są dane osobowe klientów.
- **31%** Wdrożenie rozwiązań pozwalających na pseudonimizację i szyfrowanie danych osobowych.
- **25%** Wdrożenie rozwiązań zapewniających zdolność do szybkiego przywrócenia dostępności danych osobowych i dostępu do nich w razie incydentu fizycznego lub technicznego.
- **29%** Wdrożenie rozwiązań wspierających funkcję Inspektora Ochrony Danych poprzez agregowanie, porządkowanie, archiwizowanie i prezentowanie informacji o procesach przetwarzania danych osobowych w organizacji (mapa procesów).
- **67%** Wprowadzenie zmian w polityce bezpieczeństwa.
- **75%** Edukacja pracowników w zakresie ochrony danych osobowych.
- **31%** Zmiana umów z firmami, które przechowują nasze dane (tzw. umowy powierzenia).

Ocena świadomości bezpieczeństwa informatycznego pracowników oraz konsekwencji nieprzestrzegania zasad bezpiecznego przetwarzania informacji:



Szacunkowy budżet związany z przygotowaniem do RODO:



69% poniżej 100 tys. zł

23% od 101 tys. zł do 500 tys. zł

6% od 501 tys. zł do 1 mln zł

2% powyżej 1 mln zł

Liczba incydentów związanych z bezpieczeństwem IT:

48,3% – wzrosła w ciągu ostatniego roku

5,7% – zmalała w ciąg ostatniego roku

46% – pozostała bez zmian

Poziom wykrywalności incydentów związanych z bezpieczeństwem IT:

3,5% – pogorszył się

51,7% – poprawił się

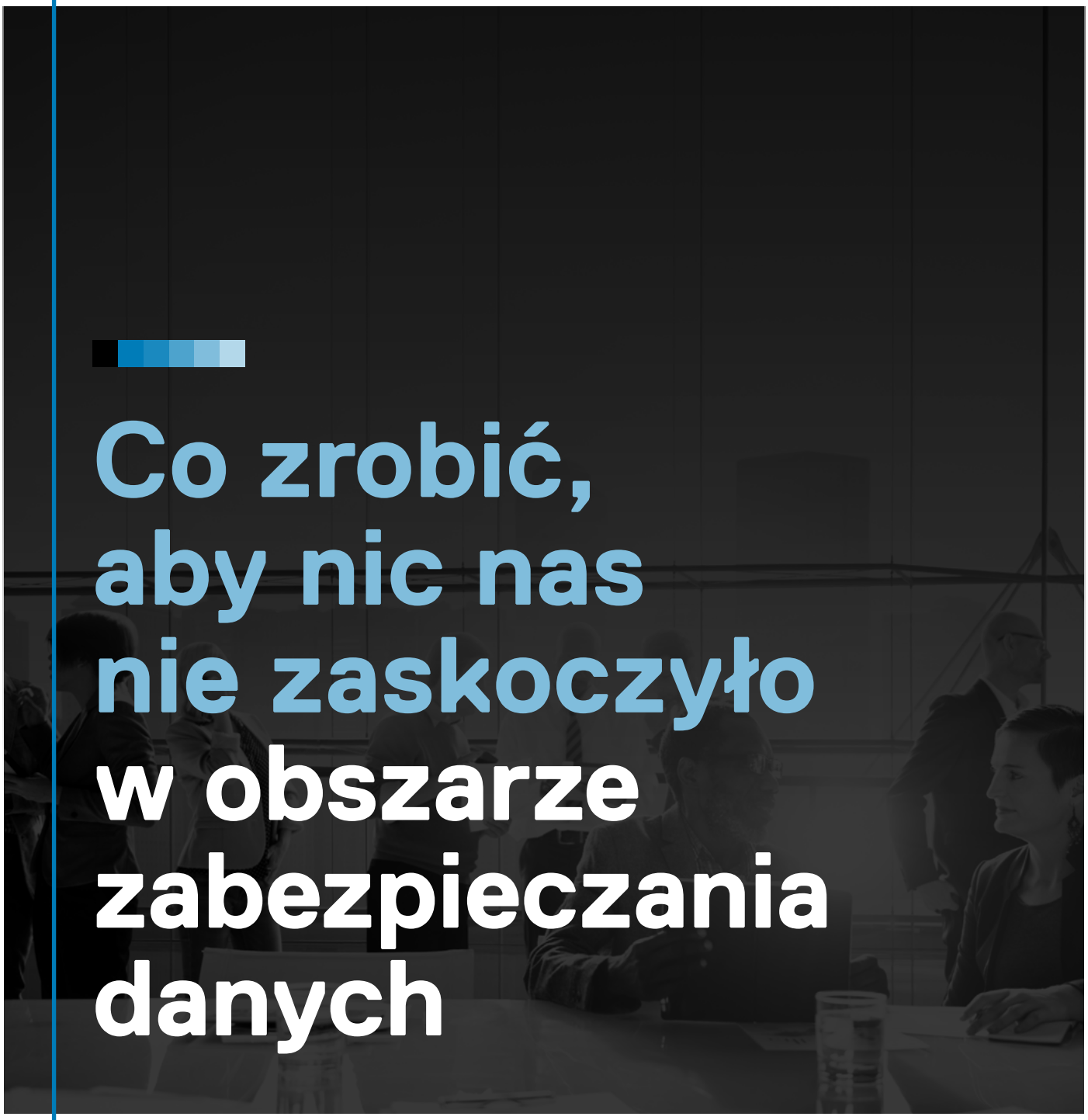
44,8% – pozostał bez zmian

Czego najbardziej brakuje w skutecznej walce z cyberprzestępcami?

39% odpowiednich narzędzi

48% odpowiednio przeszkolonych specjalistów ds. bezpieczeństwa

75% odpowiedniej edukacji wśród użytkowników firmowych rozwiązań IT



Co zrobić, aby nic nas nie zaskoczyło w obszarze zabezpieczania danych

W ostatnich latach systemy wykonywania kopii zapasowych przyzwyczaiły nas do wydajności i bezpieczeństwa. Prędkość backupu na poziomie 20 TB/h jest już codziennością. Jednocześnie rozwiązania takie jak Dell EMC Data Domain zawdzięczają gigantyczny, 60-proc. udział w rynku gwarancji odtworzenia. Administrator może mieć pewność, że w razie awarii szybko odzyska dane.

Czy administrator backupu na pewno chce śledzić z wytężoną uwagą zmiany w infrastrukturze? Czy chce aktualizować polityki backupu po każdej utworzonej lub usuniętej maszynie wirtualnej? **To niewykonalne.** Jednocześnie rola administratora backupu staje się bardziej biznesowa. Definiuje on politykę bezpieczeństwa firmy, determinuje, która część infrastruktury jest krytyczna, która produkcyjna, i która ma znaczenie testowe. **Nowoczesne rozwiązanie backupowe będzie wiedziało, jak ma zareagować na nowo powstałą infrastrukturę.**

Wyobraźmy sobie jednak, że w naszej infrastrukturze pojawiło się nowe środowisko wirtualne z bazą danych i systemem plików. W sumie kilka maszyn wirtualnych. Nie do końca wiemy, kto i kiedy je uruchomił. Nie ma to dla nas jednak znaczenia. System backupu natychmiast rozpoznaje nową infrastrukturę. Sam zakwalifikował ją jako środowisko krytyczne i od razu wdrożył odpowiednią politykę zabezpieczania z największą możliwą częstotliwością wykonywania kopii zapasowych. Wychodząc z pracy, administrator otrzymuje raport, z którego dowiaduje się, że danego dnia maszyn krytycznych było np. o 5 więcej i wszystkie były zabezpieczane co godzinę w 2 różnych ośrodkach.

Inny przykład. Gdy grupa deweloperska usuwa środowisko, w którym testowała nową wersję aplikacji, naturalną reakcją klasycznego systemu backupu jest wyświetlenie komunikatu o błędzie: „Nie wykryto grupy maszyn wirtualnych, które miały zostać zbackupowane". Takie błędy są irracjonalne i przeszkadzają w codziennej pracy. Jednak administratorów bardziej zaboli obniżenie SLA i gorsza ocena ich pracy. Po wdrożeniu nowoczesnego rozwiązania nic takiego się nie dzieje. System backupu tuż po usunięciu środowiska wie, że go nie ma. Dlatego po prostu przestaje wykonywać jego kopie zapasowe. Oczywiście wciąż możemy usunięte środowisko odtworzyć, gdyż dotychczasowe backupy są przechowywane w tylu lokalizacjach, ilu potrzeba, i przez tyle czasu, ile potrzeba.

ZMIANA ROLI ADMINISTRATORA BACKUPU NA BARDZIEJ BIZNESOWĄ

Brzmi jak science fiction? Nic z tych rzeczy. Dla nowoczesnych systemów backupu – takich jak Dell EMC Avamar – to standardowa funkcjonalność. Pozostaje jedynie pytanie: czy w takim podejściu jest jeszcze miejsce dla administratora backupu? Czy jest on nadal potrzebny? To pytanie należy jednak zadać inaczej. Czy administrator backupu na pewno chce śledzić z wytężoną uwagą zmiany w infrastrukturze? Czy chce aktualizować polityki backupu po każdej utworzonej lub usuniętej maszynie wirtualnej? To niewykonalne, bez względu na to, czy nasza infrastruktura jest zmieniana przez jedną, czy kilkadziesiąt osób.

Rola administratora backupu staje się bardziej biznesowa. Definiuje on politykę bezpieczeństwa firmy, determinuje, która część infrastruktury jest krytyczna, która produkcyjna, i która ma znaczenie testowe. Nowoczesne rozwiązanie backupowe będzie wiedziało, jak ma zareagować na nowo powstałą infrastrukturę: jak często zabezpieczać nowe maszyny wirtualne, jak długo przechowywać kopie zapasowe, czy i jaką zastosować politykę Disaster Recovery itd.

BIZNESOWE USŁUGI STOJĄCE ZA SYSTEMEM BACKUPU

Zmierzamy z jednej strony w kierunku prostoty rozwiązań, a z drugiej – ku IT jako usłudze biznesowej. Ta biznesowa część systemu backupu wymusza jeszcze inne aspekty, takie jak rozliczanie departamentów ze zużytych zasobów rozwiązania backupowego, możliwość podziału i współdzielenia zasobów Data Protection między wieloma organizacjami przy zachowaniu bezpieczeństwa itp. To nowe zadania stawiane administratorom backupu. Aby móc je zrealizować, potrzebują oni nowoczesnych narzędzi – takich jak dostarczane przez Dell EMC rozwiązania Avamar czy Data Domain.

Praktyka pokazuje, że walkę konkurencyjną wygrywają rozwiązania bezobsługowe. Tak było w Stanach Zjednoczonych w przypadku samochodów i montowanych w nich skrzyń biegów. Wygrały przekładnie automatyczne, mimo wyższej ceny. Wydaje się, że systemy backupu weszły w kolejny etap walki o klientów. Dla administratorów jest to szansa, aby udźwignąć coraz większą ilość obowiązków.

Administratorzy muszą ocenić, które rozwiązania rzeczywiście dają im pełen „automat", przy zachowaniu... gwarancji odtworzenia. Pamiętajmy, że rozwiązanie backupowe – choćby najszybsze, choćby w pełni bezobsługowe – jest nic nie warte, jeśli nie mamy stuprocentowej pewności odtworzenia.

Daniel Olkowski,
Solution Architect, Dell EMC

Współpraca z biznesem i priorytety IT oczami CIO

Prawie 92% ankietowanych przez nas CIO i IT Managerów uważa, że ich rola stała się bardziej wymagająca ze względu na konieczność łączenia strategii technologicznej z innowacjami w biznesie. Wśród najczęściej wymienianych obszarów współpracy IT z biznesem – po rekomendacji rozwiązań IT (77%) – znajduje się wskazywanie potencjalnych zmian modelu biznesowego w oparciu o dostępne technologie (72%).

Jeśli chodzi o czas poświęcany przez ankietowane przez nas osoby poszczególnym „rolom", najwięcej uwagi CIO i IT Managerowie poświęcają obecnie wsparciu transformacji biznesu firmy (29,5%). Dopiero na drugim miejscu jest zarządzanie pionem IT (30,3%). Na trzecim miejscu znalazło się zaś strategiczne planowanie rozwoju technologicznego (22,9%).

IT NA STYKU Z BIZNESEM

Po wspomnianych już obszarach współpracy IT z biznesem – rekomendacji rozwiązań IT i wskazywaniu potencjalnych zmian modelu biznesowego w oparciu o dostępne technologie – do najważniejszych z nich należą także: opracowywanie – wspólnie z biznesem – tzw. business cases (68%), opracowywanie technicznych wymogów na potrzeby nowych projektów (56%) oraz... współpraca ze start-upami lub rozwijanie wewnętrznie tego typu projektów (21%).

Wśród najczęstszych problemów na styku IT z biznesem wbrew pozorom nie jest wymieniane tzw. Shadow IT (zaledwie 28% odpowiedzi), lecz: zbyt duża dynamika zmian oczekiwań (63%), niezrozumienie ograniczeń technologicznych posiadanych w firmie rozwiązań IT (55%) oraz dążenie do nadmiernej optymalizacji kosztów (42%). Shadow IT znalazło się dopiero na 4. pozycji.

JAK CYFROWO ZMIENIĆ ORGANIZACJĘ?

Ponad 80% CIO i IT Managerów przyznało, że w ich firmach prowadzone są projekty związane z tzw. cyfrową transformacją. Jeśli zaś takie projekty nie są prowadzone, to aż 52% respondentów stwierdziło, że zamierza je rozpocząć w ciągu najbliższych 6 miesięcy (38%) albo najbliższego roku (14%). Ich zdaniem (71%) to CIO i pion IT powinni odpowiadać za projekty związane z cyfryzacją biznesu. Jedynie 38% wskazało dedykowaną osobę – CDO (Chief Digital Officer). W komentarzach pojawiały się też informacje, że za cyfrową transformację powinna odpowiadać cała organizacja, jak również, że zaangażowany powinien być dział HR, bo wiąże się ona także ze zmianą kulturową organizacji.

Po IT (99%), najbardziej w projekty cyfrowej transformacji zaangażowane są takie działy, jak: zarząd (76%), sprzedaż (49%), marketing (48%), R&D (44%) i obsługa klienta (42%). Budżet na tego typu projekty jest najczęściej częścią budżetu działu IT (55%) lub elementem budżetów działów biznesowych (28%). W niektórych firmach został jednak wydzielony do osobnego działu, np. Innovation Lab (17%).

Celem projektów związanych z cyfrową transformacją są przede wszystkim: zdobycie przewagi konkurencyjnej w obecnej sferze działalności (78%), obniżenie kosztów w celu poprawy rentowności (55%) i nadążenie za tym, co robi bezpośrednia konkurencja (50%). Dopiero na 4. miejscu znalazło się wykreowanie nowych źródeł przychodów, spoza dotychczasowej działalności (48%). W komentarzach uczestnicy zwracali także uwagę na dodatkowy aspekt cyfrowej transformacji – poprawę tzw. Customer Experience.

PRIORYTETY I BUDŻETY PIONÓW IT

W naszym badaniu pytaliśmy także o to: Jakie projekty uznawane są za strategiczne w polskich firmach? Czy polskie firmy przetwarzają zbiory Big Data w celu lepszego dopasowania swoich usług i produktów do oczekiwań klienta? W jaki sposób zmienił się budżet polskich firm na IT w roku 2017? W których obszarach budżet ten się zwiększył, a w jakich zmniejszył? W jaki sposób zmieni się budżet polskich firm na IT w roku 2018? Które projekty infrastrukturalne, aplikacyjne, sieciowe i związane z bezpieczeństwem zamierzają przeprowadzić polskie firmy? Oraz czy strategia IT polskich firm jest zintegrowana ze strategią związaną z bezpieczeństwem IT? Zapraszamy do zapoznania się z wynikami badania.

Adam Jadczak,
redaktor naczelny magazynu ITwiz

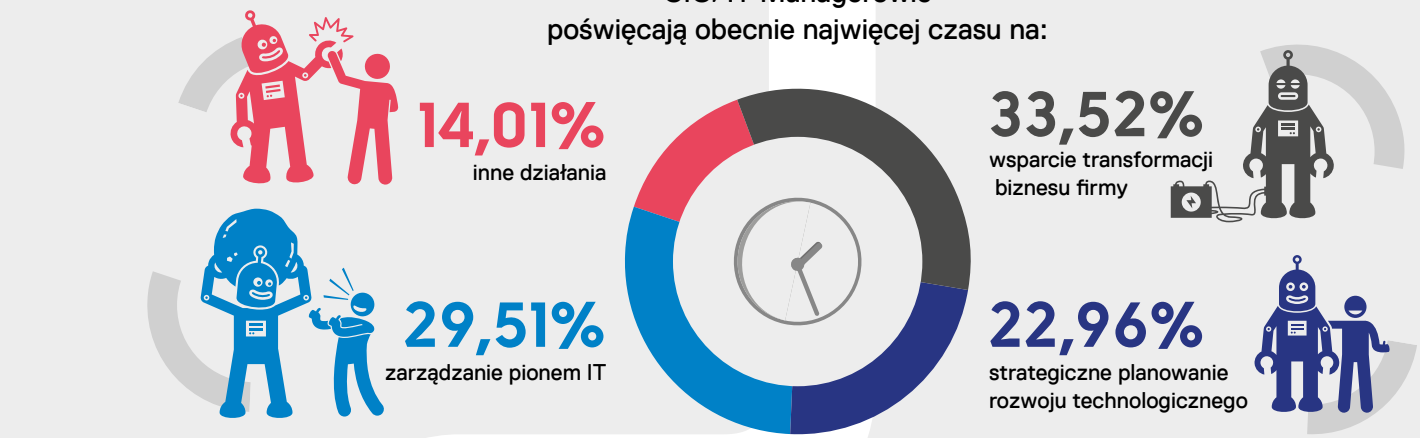
Najwięcej uczestników naszego badania pochodziło z firm zatrudniających od 1001 do 9999 pracowników (37%), a następnie od 251 do 1000 (29%) i ponad 10 000 osób (18%). Badanie przeprowadziliśmy w pierwszych dwóch tygodniach czerwca 2017 roku, wysyłając ankietę do ponad 500 CIO i IT Managerów. Badanie zrealizowaliśmy we współpracy z CIONET Poland.

Jaka jest rola CIO/IT Managera w obecnych czasach?

8,45%
pozostaje bez zmian

91,55%
bardziej wymagająca ze względu na konieczność łączenia strategii technologicznej z innowacjami w biznesie

CIO/IT Managerowie poświęcają obecnie najwięcej czasu na:



14,01%
inne działania

33,52%
wsparcie transformacji biznesu firmy

29,51%
zarządzanie pionem IT

22,96%
strategiczne planowanie rozwoju technologicznego

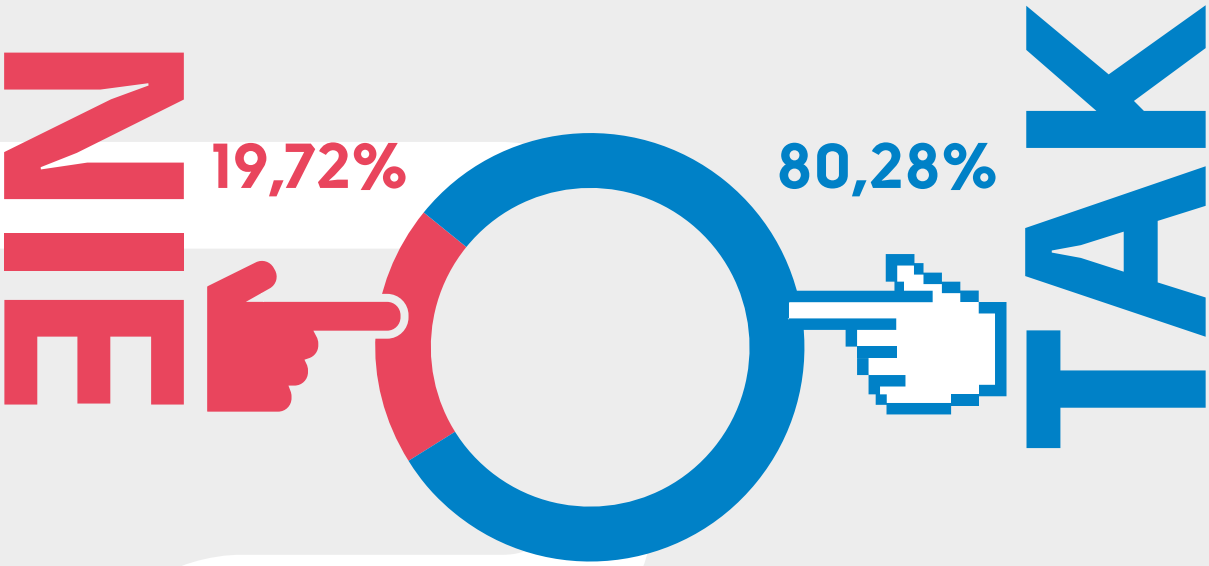
Najważniejsze obszary współpracy CIO/IT Managera z biznesem to:

- **77,46%** rekomendowanie rozwiązań technologicznych
- **67,61%** opracowywanie – wspólnie z biznesem – tzw. business cases
- **56,34%** opracowywanie technicznych wymogów na potrzeby nowych projektów
- **19,72%** współpraca ze startupami lub rozwijanie wewnętrznie tego typu projektów
- **71,83%** wskazywanie potencjalnych zmian modelu biznesowego firmy w oparciu o dostępne technologie IT
- **11,27%** inne

Jakie są najczęstsze obszary „konfliktu” IT z biznesem:

- **28,17%** zjawisko Shadow IT
- **42,25%** dążenie do nadmiernej optymalizacji kosztów
- **63,38%** zbyt duża dynamika zmian oczekiwań
- **54,93%** niezrozumienie ograniczeń technologicznych posiadanych w firmie technologii
- **15,49%** inne

Czy w polskich firmach
prowadzone są projekty określone mianem
tzw. cyfrowej transformacji?



Firmy, które nie prowadzą projektów związanych z cyfrową transformacją planują zrobić to:

w ciągu **6 miesięcy** — **38,10%**

w ciągu **6–12 miesięcy** — **14,29%**

w dalszej **przyszłości** — **19,05%**

Największe bariery w przeprowadzeniu cyfrowej transformacji to:

57,75%
organizacja nie jest dostosowana do cyfrowej transformacji (zmiana kultury firmy)

11,27%
brakuje właściwych informacji, na których mógłby opierać się biznes

42,25%
brakuje odpowiednich specjalistów (zarówno technicznych, jak i z umiejętnościami biznesowymi)

22,54%
brakuje odpowiednich narzędzi (np. do analizy tzw. customer experience)

21,13%
procesy są tak nieelastyczne, że trudno jest osiągnąć korzyść z tego typu projektów

22,54%
trudno przekonać zarząd do tego typu inwestycji (brak budżetu)

50,70%
brak współpracy pomiędzy działami (tzw. silosowość)

Kto odpowiada – powinien odpowiadać – za transformację cyfrową?

35,21%
CEO

71,83%
CIO / dyrektor informatyki

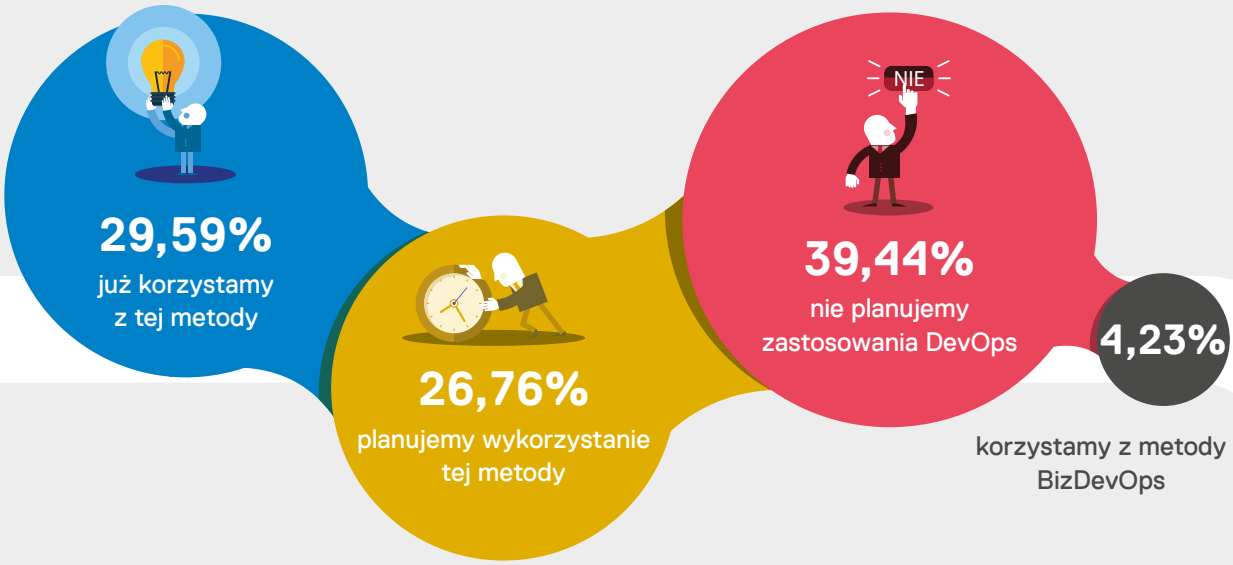
12,68%
CMO/dyrektor marketingu

19,72%
dyrektor sprzedaży

38,03%
dedykowana osoba (np. Chief Digital Officer)

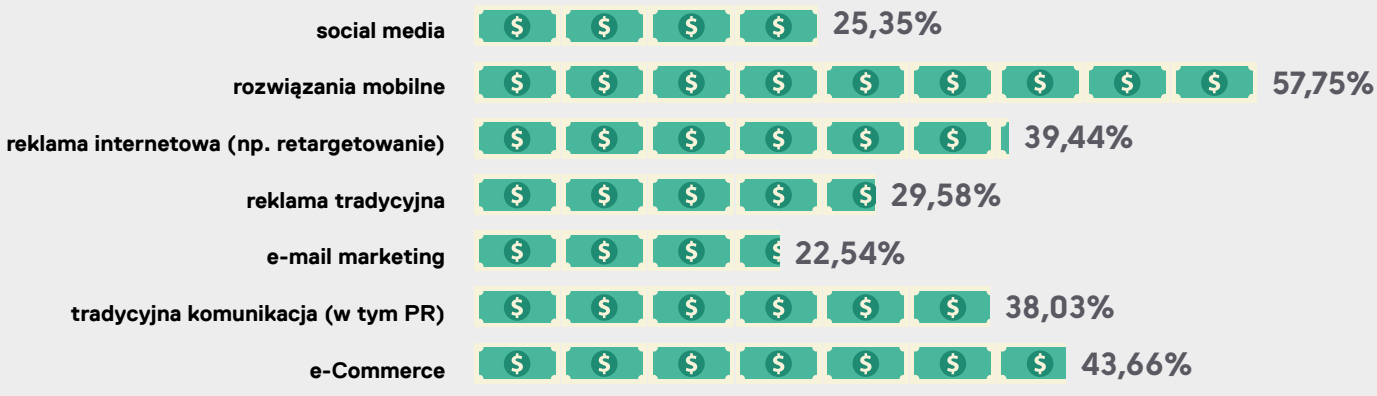
27,28%
zespół łączący różne kompetencje i zakres wiedzy o rynku i działaniu technologii

Czy polskie firmy mają w planach wdrożenie metodologii DevOps?

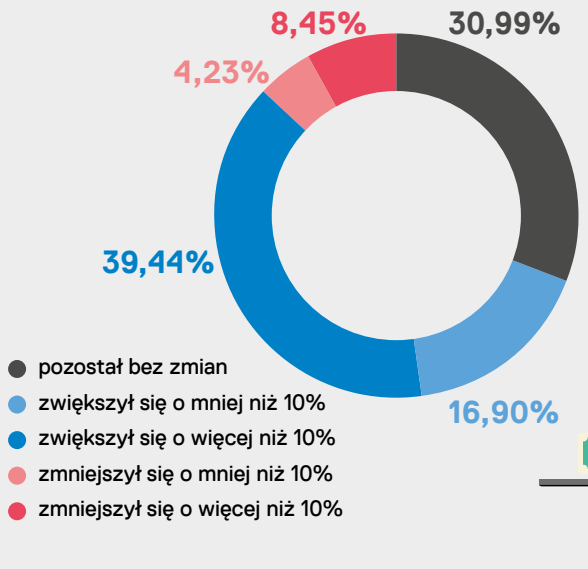


Projekty uznawane za strategiczne w polskich firmach

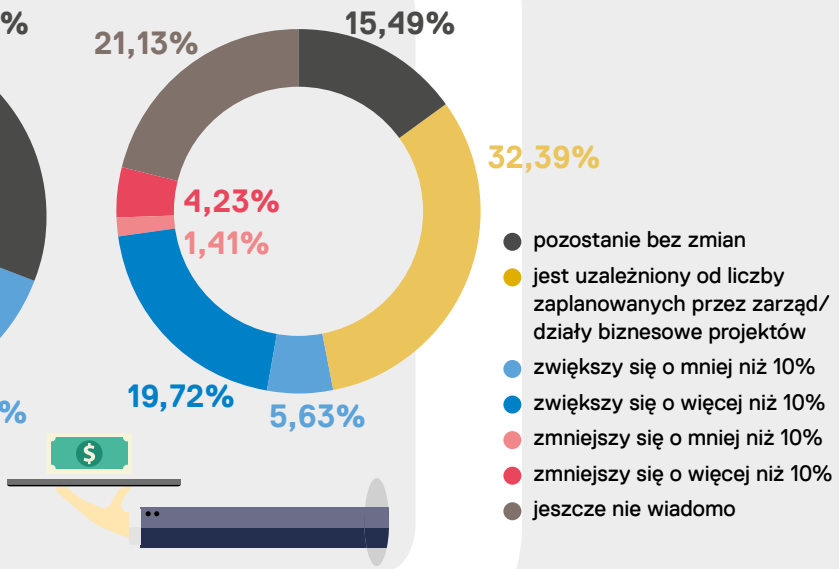
W które kanały kontaktu z klientami polskie firmy inwestują dziś najwięcej?



W jaki sposób zmienił się budżet polskich firm na IT w roku 2017 w porównaniu z 2016?

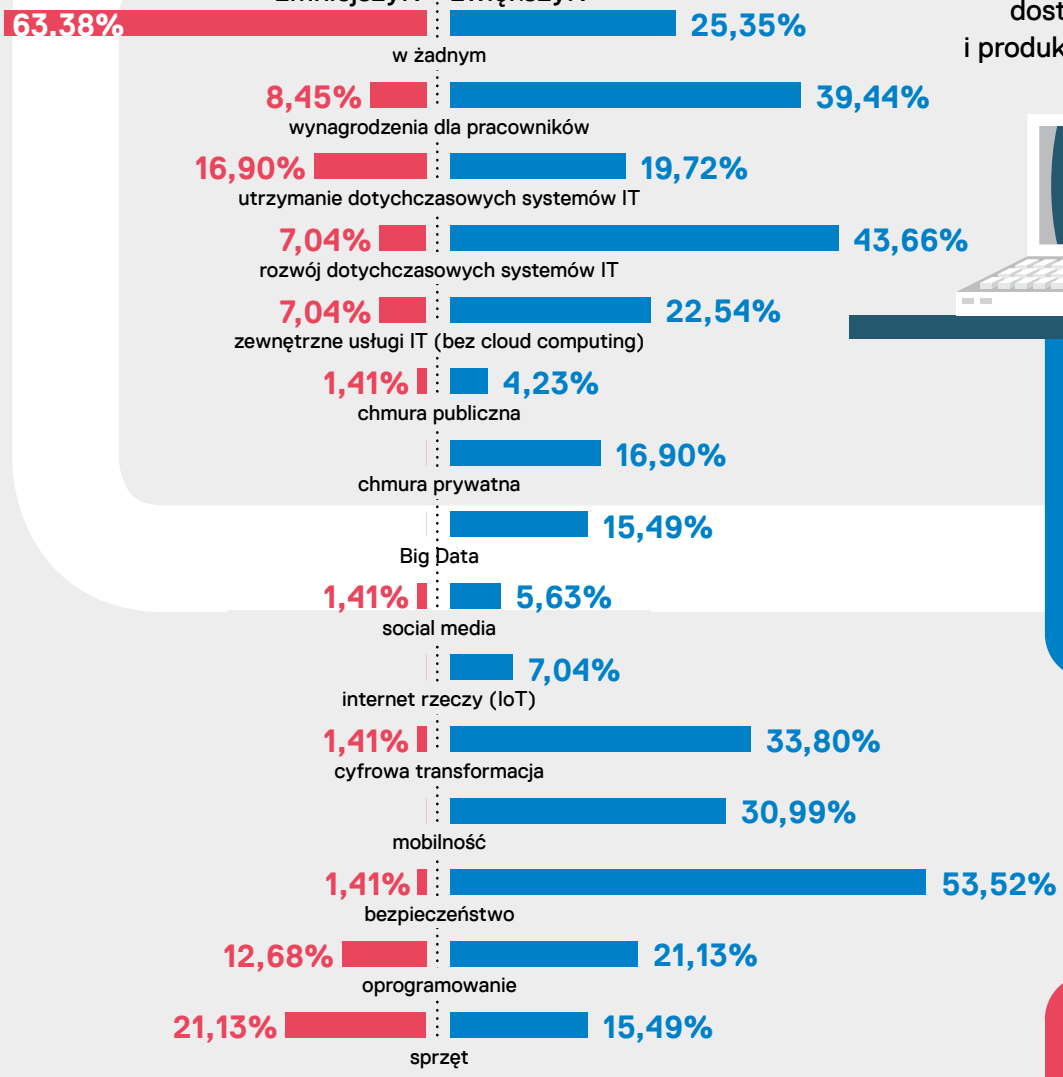


W jaki sposób zmieni się budżet polskich firm na IT w roku 2018 w porównaniu z 2017?

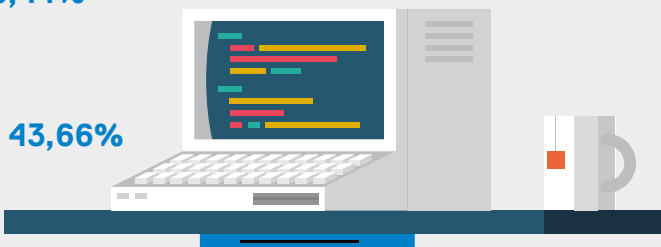


W których obszarach budżet polskich firm się zmniejszył?

W których obszarach budżet polskich firm się zwiększył?



Czy polskie firmy przetwarzają zbiory Big Data w celu lepszego dostosowania swoich usług i produktów do oczekiwań klienta?



42,25% tak

29,58% planują wykorzystanie analityki Big Data

28,17% nie planują przetwarzania zbiorów Big Data

Dell EMC: jak rozwinie się polski rynek IT?

Rok 2016 to spadek sprzedaży w sektorze IT, szczególnie na rynku publicznym. Wielu z naszych partnerów – zwłaszcza tych, dla których sektor ten był jednym z głównych odbiorców produktów i usług – zaczęło szukać szans na rynku komercyjnym. Efektem była rosnąca konkurencja. Adaptując się do mniejszego popytu, partnerzy inwestowali w kompetencje i nowe portfolio usług, w tym tych, opartych na wiedzy własnych inżynierów. Mamy przykłady współpracujących z nami firm, które w 2016 r. odniosły duży sukces dzięki takiej strategii.

Niewątpliwie pomogło im także powstanie firmy Dell EMC. Portfolio naszych rozwiązań wygląda – z punktu widzenia klientów – dużo ciekawiej. Adresuje ono też dużo szerzej ich potrzeby. Przykładowo, w zakresie wirtualizacji do rozwiązań VMware, doszły także np. Microsoft Hyper-V. Z kolei rozwiązania legacy EMC – dzięki wykorzystaniu serwerów Dell – stały się dużo bardziej atrakcyjne cenowo. Wykorzystując efekt synergii, mogliśmy zaproponować nowe, lepsze ceny.

Wspólne rozwiązania Dell EMC to także odpowiedź na potrzeby klientów szukających rozwiązań pozwalających na zintegrowanie w jednym „pudełku" kilku elementów infrastruktury IT. Upraszcza to znacząco jej utrzymanie i rozbudowę w przyszłości. Dzięki wspólnej, bardziej kompleksowej ofercie naszej firmy, partnerzy Dell EMC są też w stanie zaoferować dodatkowe usługi, np. outsourcing sprzedawanych rozwiązań.

W tym roku zauważalnym trendem jest poszukiwanie przez klientów także rozwiązań konwergentnych, stanowiących dziś jeden z podstawowych elementów oferty Dell EMC. Ta nowa architektura stanowi znakomitą alternatywę dla dotychczasowych, złożonych projektów angażujących zarówno dużo zasobów, jak i funduszy klientów. Infrastruktura konwergentna może również stanowić alternatywę dla chmury. Czym bowiem kusi dziś ona klientów? Przede wszystkim niższymi kosztami oraz prostotą i elastycznością użycia. Głównymi zaletami infrastruktury konwergentnej są zaś właśnie: elastyczność, łatwość zarządzania, niski próg wejścia, możliwość szybkiej i bezproblemowej rozbudowy oraz przewidywalne koszty. Tymczasem, wielu klientów, po 2–3 latach używania chmury, stara się dziś dużo bardziej racjonalnie podchodzić do jej wykorzystania. Pojawiają się projekty zmierzające do racjonalizacji jej kosztów. Znacząco rosną one bowiem, gdy klient faktycznie zaczyna korzystać z usług cloud computing i dochodzi koszt transferu danych z i do chmury. To wydatki, które często nie były brane pod uwagę w pierwotnej analizie migracji części rozwiązań do chmury.

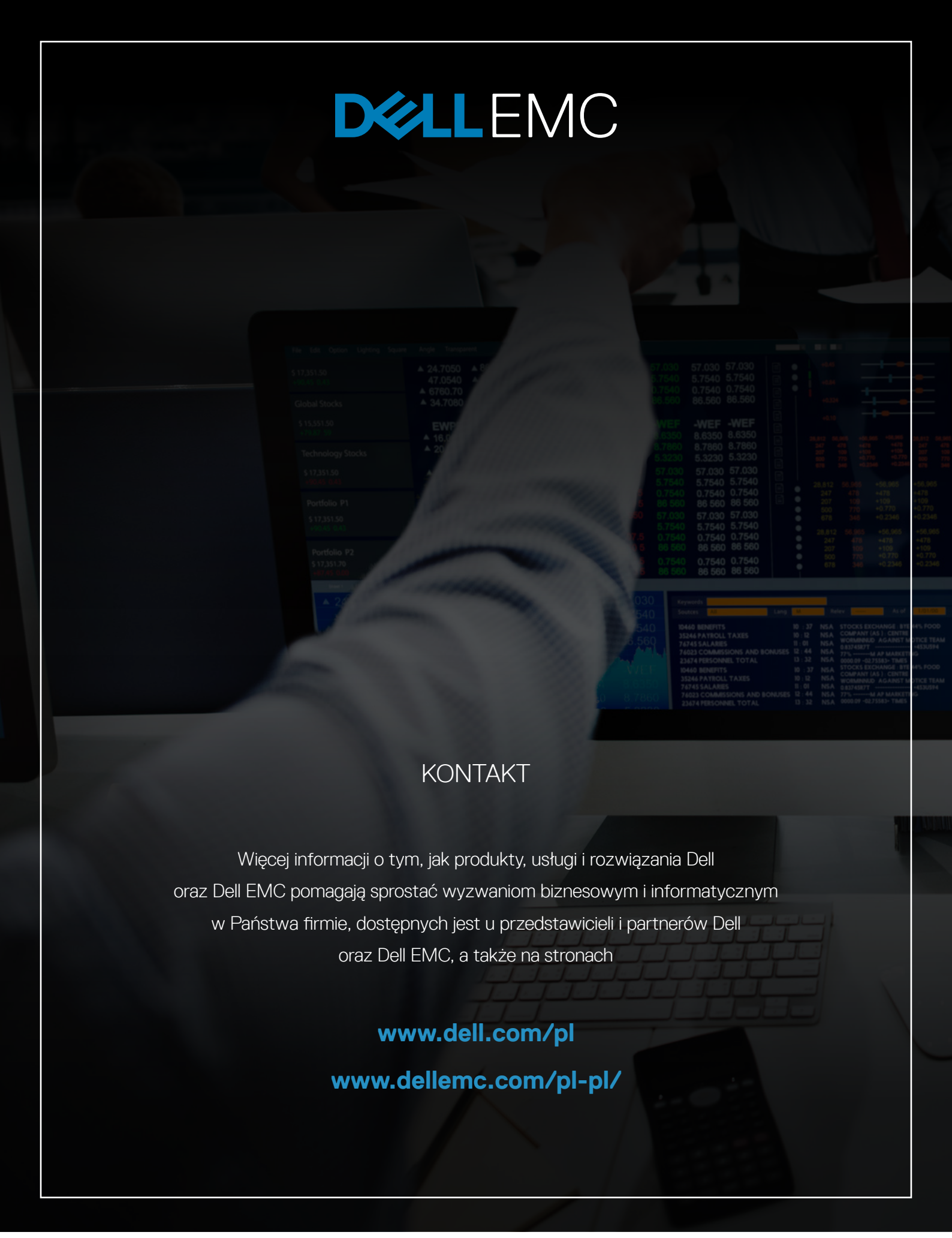
Dużo klientów stara się też uruchamiać projekty konsolidacyjne, np. związane z integracją kilku centrów danych w celu stworzenia wspólnej puli zasobów dla całej firmy lub grupy kapitałowej. Z tym zaś wiążą się projekty wykorzystujące rozwiązania typu Software-Defined Data Center, czyli definiowane programowo poszczególnymi elementami infrastruktury IT i sieci. Pojawiają się też wdrożenia rozwiązań IT opierające się na finansowaniu zewnętrznym – w formie leasingu lub długoterminowego najmu. Rynek IT upodabnia się tym samym do innych sektorów, np. środków transportu czy środków produkcji.

Ten rok to także powrót do dobrej koniunktury w branży IT. Pojawia się coraz więcej zapytań z sektora publicznego. Za tym zaś idą zwiększone inwestycje firm komercyjnych, które uruchamiają nowe inwestycje, aby nadążać za przyspieszającą gospodarką. Widać spory optymizm, który potwierdzają także nasi partnerzy. Jest więcej pieniędzy na rynku, co nie znaczy, że są to środki łatwe do zagospodarowania. Klienci stawiają bowiem na wiedzę i kompetencję.

Dariusz Okrasa,
szef kanału partnerskiego Dell EMC w Polsce

Co dała klientom fuzja Dell EMC

- **Kompleksową ofertę produktów i rozwiązań** – od centrów danych, przez infrastrukturę sieciową, po urządzenia końcowe.
- **Uproszczenie utrzymania infrastruktury IT** dzięki możliwość oparcia jej na rozwiązaniach jednego dostawcy.
- **Gwarancję kompatybilności wszystkich rozwiązań**, łatwości rozbudowy i zarządzania, a także najwyższy poziom wsparcia.
- **Portfolio rozwiązań, które odpowiada na wszelkie potrzeby klientów** – ofertę Dell oraz Dell EMC uzupełniają pozostałe firmy z rodziny Dell Technologies: Pivotal, RSA, SecureWorks, Virtustream i VMware.
- **Efekt synergii, który pozwala na zaproponowanie rozwiązań dużo bardziej atrakcyjnych cenowo.**
- **Elastyczność, łatwość zarządzania, niski próg wejścia, możliwość szybkiej i bezproblemowej rozbudowy systemów IT** oraz przewidywalne koszty dzięki zastosowaniu infrastruktury konwergentnej.
- **Elementy środowiska IT pozwalające połączyć je w logiczną całość**, a także zautomatyzować zarządzanie infrastrukturą IT, i to niezależnie od tego, jaki model wykorzystania infrastruktury wybierze klient.
- **Elementy infrastruktury IT niezbędne do przeprowadzenia cyfrowej transformacji.**



KONTAKT

Więcej informacji o tym, jak produkty, usługi i rozwiązania Dell
oraz Dell EMC pomagają sprostać wyzwaniom biznesowym i informatycznym
w Państwa firmie, dostępnych jest u przedstawicieli i partnerów Dell
oraz Dell EMC, a także na stronach

www.dell.com/pl

www.dellemc.com/pl-pl/