RODO: kolejne wyzwania, kolejne wdrożenia

Po pierwszych próbach dostosowania się do wymogów RODO, czynionych w dużej mierze pod presją czasu i w chaosie interpretacyjnym, nadchodzi pora na kolejne, bardziej przemyślane i zaawansowane wdrożenia. Będą one już jednak osadzone w szerszym kontekście cyberbezpieczeństwa i tzw. compliance'u, czyli zgodności z regulacjami. W ocenie uczestników debaty „RODO w praktyce biznesowej" zapotrzebowanie na nowe rozwiązania będzie również efektem postępującej cyfryzacji wszystkich dziedzin życia.

Uczestnicy debaty:

Szymon Dudek, dyrektor Działu Oprogramowania, pełnomocnik zarządu, Infonet Projekt
Mariusz Kochański, członek zarządu, dyrektor Działu Systemów Sieciowych, Veracomp
Marcin Serafin, szef Zespołu Ochrony Danych Osobowych oraz Zespołu Kontraktów IT, partner w kancelarii prawnej Maruta Wachta
Tomasz Sobol, dyrektor marketingu, Beyond.pl

CRN Niedługo minie rok od wejścia w życie unijnego rozporządzenia o ochronie danych osobowych. To dobry czas na podsumowanie pierwszych doświadczeń i analizę wniosków z dotychczasowego funkcjonowania nowych przepisów w praktyce. Jak wygląda sytuacja z perspektywy branży IT?

Mariusz Kochański Pozytywnym aspektem pojawienia się RODO było zwrócenie uwagi na kwestię ochrony danych osobowych. Wprawdzie obowiązywała już wcześniej ustawa o ochronie danych osobowych, ale wiedza o zawartych w niej regulacjach nie była powszechna. Dyskusje wokół RODO spowodowały olbrzymią zmianę w świadomości decydentów i obywateli. To przełożyło się również na zwiększone zainteresowanie narzędziami informatycznymi. Co nie zmienia faktu, że przed nami jeszcze dużo pracy. W przypadku tego rozporządzenia bowiem nie tylko treść jest ważna, ale i wykładnia. RODO można interpretować na różne sposoby i dojść do zupełnie różnych wniosków. Czekamy więc na doktrynę, na orzeczenia prezesa Urzędu Ochrony Danych Osobowych. W dobrym skądinąd poradniku dla dyrektorów szkół pojawiają się sformułowania typu „wydaje się, że dobrym rozwiązaniem będzie", a nie stwierdzenia „dobrym rozwiązaniem będzie". To pokazuje, że sam regulator jest jeszcze na początku drogi.

Marcin Serafin Od stycznia do października ubiegłego roku szefowie UODO zatrudnili 112 nowych pracowników, podczas gdy w grudniu 2017 roku pracowało w nim mniej niż 200 osób. Nastąpiła więc niemalże całkowita wymiana kadr. Tak samo jak wszystkie przedsiębiorstwa, również i ten urząd musiał się zmierzyć z trudnym problemem wdrożenia RODO. Największym wyzwaniem – zarówno po stronie administracyjnej, informatycznej, prawnej, jak i biznesowo-konsultingowej – jest obecnie brak dobrej kadry, która byłaby w stanie w sposób rzetelny i merytoryczny pomóc tym, którzy są zobligowani do przestrzegania przepisów.

CRN Dosyć powszechne są jednak oczekiwania, że UODO mogłoby być choć trochę bardziej aktywne, co by pomogło wszystkim zainteresowanym w dostosowywaniu się do wymogów RODO...

Marcin Serafin Od 25 maja do 21 lutego UODO wszczęło 50 kontroli i jednocześnie 1379 postępowań w sprawie naruszenia przepisów – na podstawie różnego rodzaju skarg lub informacji własnych pozyskanych przez urząd. Spośród 50 kontroli 44 zostały zakończone. Ogłoszony został również plan kontroli sektorowych na rok 2019. Widać więc, że wiele rzeczy już działa. Problem leży jednak w czym innym. Przed wejściem rozporządzenia w życie każdy z nas – każda firma czy instytucja – robił wiele, żeby wywiązać się z nałożonych nowymi przepisami obowiązków. I każdy dotarł po swojemu do momentu, w którym sam uznał określony stan za zgodny z RODO. Kłopot w tym, że jest on tak naprawdę nieuchwytny, nie da się go jednoznacznie zidentyfikować ani umiejscowić w czasie. To proces i zmienna, którą trzeba bez przerwy śledzić i waloryzować.

CRN Jak w praktyce firmy i instytucje radziły sobie z tą niejednoznacznością czy otwartą formułą nowych przepisów? Czy po zgłaszanych przez klientów potrzebach widać było, czy i jak rozumieją RODO? Czy dały się zauważyć jakieś trendy, na przykład zwiększone zapotrzebowanie na określone rozwiązania?

Szymon Dudek Z naszych doświadczeń wynika, że przedsiębiorstwa i urzędy interpretowały przepisy po swojemu. Z samego rozporządzenia nie wynikało bowiem wprost, co trzeba zrobić, żeby być z nim zgodnym. Nasi klienci robili więc zazwyczaj maksymalnie dużo, wszystko, co było w ich mocy, na co było ich stać, żeby w razie czego móc wykazać, że zrobili jak najwięcej, żeby sprostać wymogom RODO, że postarali się jak najbardziej dostosować swoje procedury i technologie do nowych przepisów. Po części zainteresowanie rozwiązaniami służącymi zapewnieniu zgodności z regulacjami nadal daje się zaobserwować, ale jest już znacznie, znacznie słabsze niż przed majem ubiegłego roku.

Tomasz Sobol Mimo niejednoznaczności zapisów RODO mogliśmy jednak dokonać podziału, kto jest administratorem danych, a kto procesorem. Zarówno jako zleceniodawcy, jak i zleceniobiorcy zdaliśmy sobie sprawę z różnych zakresów odpowiedzialności. To było do tej pory bardzo niejasne. ›

W wielu przypadkach nadal zapewne takie pozostanie, ale istnieje już punkt odniesienia do określenia tych ról. W naszym przypadku to jest ogromne wyzwanie, by uświadomić klientom, co my – jako dostawca usług – im gwarantujemy, a za co oni sami są odpowiedzialni. Wiele rzeczy musimy razem z nimi wypracować. Przy czym zapewnienie zgodności z RODO to proces ciągły, ale nie można związanych z nim wymagań sprowadzać do absurdu, jak to się w niektórych miejscach działo czy dzieje. Działania nadmiarowe, wprowadzanie nieuzasadnionych obecnymi wyzwaniami rozwiązań nie przybliżą nas do ustalenia, co jest zgodne z RODO, a co nie, bo za chwilę wiele rzeczy może ulec zmianie.

CRN W jakim stopniu wprowadzenie nowych zasad ochrony danych osobowych wygenerowało zapotrzebowanie na nowe technologie i stało się faktycznie powodem nowych zamówień na rynku informatycznym?

Marcin Serafin W drugiej połowie 2017 roku były wielkie plany, wszyscy wkoło opowiadali, jakich to systemów nie będą wdrażać albo jakie powinny zostać wdrożone. Kiedy na początku 2018 roku zaczęto uświadamiać sobie, że do terminu wejścia w życie rozporządzenia pozostało już naprawdę niewiele czasu, wydawało się, że wszyscy rzucą się do szerokiego informatyzowania zasobów, automatyzowania procesów, uruchamiania programów klasyfikacji danych. W ostateczności okazało się, że wiele rzeczy jest nadal robionych „ręcznie". Nowych systemów informatycznych, które zostały wdrożone z powodu RODO – a muszę podkreślić, że pracowałem dla ponad 100 klientów, pomagając im wdrażać unijne rozporządzenie – widziałem dosłownie dwa i oba dotyczyły zarządzania zgodami. Tak naprawdę dopiero teraz nadchodzi moment, kiedy będziemy mieli do czynienia z pojawianiem się przemyślanych wdrożeń IT służących ochronie danych osobowych zgodnie z regułami RODO.

Mariusz Kochański, Veracomp

Mariusz Kochański Inwestycje w rozwiązania informatyczne wprawdzie się pojawiły, ale nie wszystkie były bezpośrednio efektem RODO. Instytucje, które zawsze cechował wysoki poziom ryzyka związany z cyberzagrożeniami – bankowość, przedsiębiorstwa użyteczności publicznej, telekomy – musiały wykonać szereg prac związanych ze zmianą procedur czy procesów biznesowych. Nie zauważyłem tam jednak drastycznej zmiany architektur zabezpieczeń. Pojawiły się natomiast środki na narzędzia pozwalające zidentyfikować, kiedy i w jakich okolicznościach doszło do wycieku danych. Przyczynił się do tego nie tylko wymóg zgłaszania incydentów w ciągu 72 godzin. To jest również pochodna wielkich strat firm na rynku amerykańskim wskutek wycieków danych w dużych korporacjach. Jeśli chodzi o polskie banki czy telekomy, to RODO wywołało rewolucję prawną, procesową, ale nie technologiczną. Natomiast w sektorze publicznym, który od dawna zmaga się z brakiem funduszy, RODO spowodowało, że decydenci lepiej zaczęli rozumieć problem. Pojawiło się przekonanie, że jednak pieniądze na bezpieczeństwo trzeba wydać i nie można dalej stosować zasady „jakoś to będzie".

Szymon Dudek Nowe przepisy skłoniły wiele firm do optymalizacji procesów przetwarzania danych. Zaczęto się zastanawiać, jak sprawdzić, jakimi danymi dysponujemy, czy wszystkie są nam faktycznie potrzebne, z których możemy zrezygnować, co wymaga dodatkowej inwentaryzacji. Średnio połowa naszych klientów dysponowała już potrzebnymi do tego systemami i stosowną infrastrukturą. Pozostali dopiero szukali rozwiązań w tym zakresie, co wiązało się często z zamówieniami na nowe narzędzia czy produkty, na przykład dodatkowy storage, system do zarządzania uprawnieniami czy zabezpieczenie styku z internetem. W większości przypadków były to w zasadzie działania na ostatnią chwilę, tuż przed terminem wejścia w życie RODO.

CRN Jak z niejednoznacznymi zapisami unijnego rozporządzenia radziła sobie branża IT? Przedsiębiorstwa informatyczne chciały być postrzegane przez swoich klientów jako ich wybawcy z kłopotu. Z jakimi wyzwaniami wiązało się przygotowanie oferty adekwatnej do wymogów RODO?

Mariusz Kochański Jako podmiot, który również przetwarza dane osobowe, zmagaliśmy się dokładnie z takim samym problemem jak kilkanaście lat temu, gdy wchodziło w życie rozporządzenie unijne dotyczące towarów podwójnego zastosowania. Wszyscy je znali w kontekście czołgów, broni, ale mało kto wiedział, że dotyczy to również produktów związanych z szyfrowaniem. Jako dystrybutor mozolnie edukowaliśmy resellerów odnośnie do konieczności wypełniania stosownych oświadczeń o przeznaczeniu końcowym produktu. Okres adaptacji do nowych warunków trwał około dwóch lat. W przypadku rozporządzenia o ochronie danych osobowych proces uświadamiania partnerów był już znacznie krótszy – zajął około dwóch, trzech miesięcy. Tyle czasu wymagało powszechne

zrozumienie w kanale sprzedaży wyzwań związanych z RODO. Teraz rozmowa z resellerami dotyczy już innych aspektów. Nie trzeba chociażby tłumaczyć różnic między rolą administratora a procesora.

CRN A w jaki sposób pojawienie się RODO wpłynęło na współpracę firm informatycznych z użytkownikami rozwiązań IT?

Tomasz Sobol Dla nas to była dobra okazja do wytłumaczenia, czym jest chmura obliczeniowa. RODO spowodowało, że klienci chcieli bardzo dokładnie poznać, zrozumieć, jak jest skonstruowany i jak logicznie działa cloud computing. To było potrzebne chociażby do precyzyjnego rozdzielenia odpowiedzialności za przetwarzanie danych – za co bierzemy odpowiedzialność my, a za co musi odpowiadać klient. Często bowiem kontrahenci wyobrażają sobie, że jak kupują usługę, to automatycznie uwalniają się od odpowiedzialności. A prawda jest taka, że odpowiedzialność musi być współdzielona. To spowodowało, że klienci zaczęli zwracać większą uwagę również na rozwiązania, które mają wdrożone w firmach. Uświadomili sobie, że mogą istnieć luki w zabezpieczeniach także po ich stronie, co w wielu przypadkach skutkowało na przykład inwestycjami w narzędzia do monitorowania przetwarzanych danych. Przedsiębiorstwa zaczęły wprowadzać szyfrowanie, wiele odkryło, że może mieć specjalne szyfrowane łącza między lokalizacjami, tj. VPN. Dzięki RODO biznes zyskał szanse na odrobienie lekcji z zakresu bezpieczeństwa: jak najlepiej zaprojektować i zbudować swoją infrastrukturę, żeby nie narażać się na niepotrzebne zagrożenia? Okazało się również, że czynnik ludzki też można trzymać w ryzach dzięki wprowadzonym procedurom.

Tomasz Sobol, Beyond.pl

Marcin Serafin Pod adresem firm informatycznych pojawiły się jednak także nadmiarowe oczekiwania czy wymagania. Widać to na przykładzie umów powierzenia przetwarzania danych. Wielu klientów wychodziło z założenia, że gdy nie wiadomo, co zrobić, to lepiej na wszelki wypadek zawrzeć umowę, chociaż nie zawsze było to uzasadnione. W przypadku standardowych usług kolokacji umowa na powierzenie przetwarzania danych osobowych nie jest potrzebna, gdyż przy prostej kolokacji usługodawca nie ma w ogóle dostępu do danych osobowych. W wielu innych sytuacjach firmy chciały nakładać na swoich partnerów biznesowych różne wymogi i obowiązki, na przykład narzucać stosowanie określonych rodzajów środków technicznych czy żądać kar umownych za niespełnienie tego rodzaju warunków. To ani nie miało uzasadnienia w samych przepisach, ani nie wynikało z istoty rozporządzenia czy faktycznej sytuacji firmy. Chodziło raczej o szukanie za wszelką cenę sposobów zabezpieczenia się przed ewentualnymi zarzutami niedopełnienia wymogów prawnych.

Tomasz Sobol W informatyce nie zawsze jednak mamy do czynienia z prostymi, jednoznacznymi sytuacjami. W usłudze kolokacji musimy uwzględniać czynnik, który wiąże się z zapewnieniem ciągłości dostępu do danych. Nawet jeśli usługodawca nie ma w ogóle dostępu do danych osobowych, to w interesie klienta leży zadbanie o warunki, w których będzie miał stały dostęp do swoich danych. Także w sytuacji, gdy jest to tylko dostęp do ich fizycznego nośnika. I właśnie z tego powodu umowa powierzenia danych pomiędzy usługodawcą kolokacji a klientem powinna być zawarta. Dobrze jest określić wzajemne powinności i działania, chociażby po to, aby klient wiedział, co się dzieje z jego danymi, gdyby ewentualnie w konkretnym momencie nie mógł z nich skorzystać, i jak sam ma się na taką sytuację przygotować. RODO nakłada więc w pewien sposób na dostawcę usług chmurowych i kolokacyjnych obowiązek zapewnienia ciągłości dostępu do danych.

CRN Można powiedzieć, że rozporządzenie uruchomiło pewne procesy, które będą dalej trwać. Jak będą się one przekładały na dalsze wykorzystanie nowych technologii? Czego branża IT może się w tym kontekście spodziewać? Czego w kolejnych latach obowiązywania RODO będą potrzebować przedsiębiorstwa przetwarzające dane osobowe?

Marcin Serafin Jedna grupa niezbędnych produktów związana jest z całym obszarem bezpieczeństwa danych, niekoniecznie osobowych – zarówno w zakresie zapewnienia ich poufności, dostępności, jak i integralności. Rynek tych rozwiązań będzie się cały czas rozwijał, gdyż każdy klient będzie potrzebował innych, dostosowanych do swoich wymogów i możliwości narzędzi. Drugi obszar, który jest dotychczas najsłabiej zagospodarowany, a do którego wielką wagę przykłada RODO, dotyczy skutecznego usuwania i anonimizowania danych. W większości firm odbywa się to w sposób „ręczny", proceduralny, a nie na poziomie zautomatyzowanym. Nieliczne przedsiębiorstwa mają rozwiązania, które rzeczywiście ›

potrafią zrealizować to wielostopniowe zadanie. W rzeczywistości nie chodzi bowiem o usuwanie danych fizycznie z nośnika, tylko o uniemożliwienie uzyskiwania dostępu do nich w określonych procesach biznesowych lub przez poszczególne działy czy pracowników.

CRN A co będzie w tym kontekście kluczową kwestią, na którą szczególnie warto zwrócić uwagę?

Marcin Serafin Najważniejszą sprawą będzie możliwość skutecznego zarządzania dostępem do danych osobowych. Na jeden z portugalskich szpitali została nałożona kara za to, że nie odebrał uprawnień dostępu do danych osobom, które nie powinny ich mieć. To jest obszar, który będzie wymagał szczególnej uwagi i nadzoru, a z drugiej strony zapewniał olbrzymie możliwości wykorzystania rozwiązań informatycznych do wspomagania i automatyzacji niezbędnych działań. Tym bardziej że w zdecydowanej większości przedsiębiorstw i instytucji rozwiązania informatyczne mają charakter rozproszony – nie ma jednego systemu, który by wszystkim zarządzał. Potrzebny więc będzie rodzaj nakładki, która dopilnuje, by z jednego systemu dane zniknęły, ale w drugim były nadal dostępne.

Marcin Serafin,
kancelaria prawna Maruta Wachta

Szymon Dudek Zanim dojdzie do pełnej automatyzacji zarządzania uprawnieniami dostępu do danych, można wykorzystać również rozwiązania półautomatyczne. Decyduje się na to, jak widzimy, wiele firm przetwarzających duże ilości danych osobowych. Jeśli w jednym systemie, na przykład CRM, następuje „skasowanie" danych, do operatorów innych systemów zostaje wysłana informacja o konieczności zablokowania dostępu również u nich. Zanim w przedsiębiorstwie pojawi się rozwiązanie docelowe w postaci pełnej programowej integracji mechanizmów udostępniania danych, warto pomyśleć o mechanizmach pośrednich, które też znacznie wspomagają i ułatwiają spełnienie wymogów RODO. Mogą one dać firmom informatycznym szansę na współpracę z klientem, którego nie stać na wdrożenie zaawansowanych, w pełni zautomatyzowanych systemów lub u którego nie ma takiej potrzeby.

CRN Warto, jak widać, szukać wyzwań związanych z ochroną danych osobowych ze względu na nowe, obiecujące perspektywy rozwoju biznesu dla integratorów i resellerów...

Mariusz Kochański Wszystko, o czym rozmawiamy, trzeba wpisać w szerszy kontekst. Po pierwsze mamy do czynienia z ogromnym deficytem specjalistów. Dotyczy to nie tylko sektora publicznego, lecz także firm prywatnych. Przedsiębiorstw nie będzie stać na utrzymywanie wszystkich potrzebnych specjalistów. Konsekwencją tego będzie rozwój outsourcingu. Jednym z obszarów w coraz większym zakresie powierzanych do obsługi na zewnątrz będzie ochrona firmowych danych i zasobów. Ten trend trzeba będzie zderzyć z wymogami RODO.

Ze względu na wielość i złożoność systemów informatycznych duże przedsiębiorstwo czy urząd dużego miasta nie będzie w stanie korzystać z usług jednego outsourcera – może współpracować z kilkoma lub kilkunastoma. Potrzebne więc będą zautomatyzowane rozwiązania umożliwiające zarządzanie dostępem do określonych systemów dla różnych partnerów. Tu pojawia się duża szansa dla resellerów i integratorów. Rosło będzie również zapotrzebowanie na wszelkiego rodzaju rozwiązania analityczne: narzędzia do analityki ruchu, zachowań użytkowników, sytuacji w centrum danych. Inny obszar, w którym firmy informatyczne znajdą miejsce dla siebie, to doradztwo w zakresie samej architektury – czyli jak zaprojektować i zbudować środowisko IT, żeby było zgodne z RODO, a do tego optymalne kosztowo i efektywne biznesowo. Resellerzy i integratorzy mogą też doradzać, jak postępować z oprogramowaniem, które jest coraz bardziej niedoskonałe, bo tworzone pod coraz większą presją czasu. Na przykład część tych niedoskonałości można niwelować na poziomie infrastruktury. Większą wagę będą mieć też kwestie dotyczące zapewnienia odpowiedniego poziomu bezpieczeństwa terminala użytkownika. Coraz więcej osób loguje się do aplikacji krytycznych w firmie ze smartfona lub laptopa. Same systemy w przedsiębiorstwie mogą być doskonale zabezpieczone, ale jak nie będzie kontroli nad urządzeniami dostępowymi, to zagrożenia pozostaną.

Tomasz Sobol W cyberświecie liczba zagrożeń będzie raczej rosnąć, niż maleć. Chociażby dlatego, że informatyka bazuje na różnych technologiach, firmy korzystają z wielu różnych aplikacji i usług różnych dostawców – nie ma jednego uniwersalnego kodu, nie ma jednego dla wszystkich systemu. Z tego powodu tak istotne staje się zapewnienie odpowiedniej architektury zabezpieczeń. To jest dzisiaj pierwszoplanowe zadanie – żeby mieć świadomość, jak działają systemy i gdzie mogą się pojawić naprawdę poważne zagrożenia. RODO może nam w tym pomóc, bo nakłada na nas obowiązek zastanowienia się, jak ukształtować

Fot. Adrian Stykowski

środowisko funkcjonowania firmy, aby czuć się zabezpieczonym na różnych poziomach i etapach. Nie musimy dawać dostępu z telefonu komórkowego bezpośrednio do infrastruktury krytycznej, lecz na przykład do swoistej bramki zewnętrznej, gdzie będzie się pojawiał tylko obraz kokpitu z wywołanej aplikacji. Konieczność radzenia sobie z takimi wyzwaniami z całą pewnością przyczyni się do rozwoju informatyki i projektowania bezpiecznej architektury systemów czy aplikacji.

Szymon Dudek Wiele informacji potrzebnych do znalezienia odpowiednich rozwiązań może dostarczyć dobrze przeprowadzona analiza ryzyka. Ona jest kluczowa dla wdrożenia rozwiązań ochronnych zgodnych z unijnym rozporządzeniem. Pokaże nam, gdzie są największe zagrożenia dla bezpieczeństwa danych w firmie. Bardzo często okazuje się jednak, że jest to sam użytkownik i urządzenie, z którego korzysta. Pojawia się też jednocześnie coraz więcej narzędzi do przeciwdziałania tym zagrożeniom, jak na przykład konteneryzowanie danych osobowych na smartfonach pracowników. Zainteresowanie zabezpieczeniami urządzeń mobilnych będzie w najbliższym czasie rosło, bo znajduje się na nich coraz więcej informacji, które są warte przechwycenia.

Marcin Serafin Dobrze, rzetelnie zrobiona analiza ryzyka jest sposobem poradzenia sobie z brakiem precyzyjności nowych przepisów o ochronie danych osobowych. Przy czym nie ma ucieczki od nieoznaczoności, bo taka jest istota RODO jako inteligentnego aktu prawnego. Gdy jednak uczciwie zdiagnozujemy, co nam może naprawdę zagrażać, co się faktycznie może wydarzyć, to będziemy wiedzieli, jakie środki zastosować. W informatyce to zresztą nic nowego – każdy projekt nowego wdrożenia, wprowadzenia nowych funkcji czy usług poprzedzony jest analizą ryzyka. A RODO dodatkowo mówi: zwróćcie uwagę na ryzyko nie tylko informatyczne, nie tylko z zakresu cyberbezpieczeństwa, ale również wynikające z tego, że ktoś utraci dostęp do swoich danych, przez co nie będzie mógł skorzystać z jakiejś bardzo ważnej dla niego funkcji lub przysługującego mu prawa. W kontekście unijnego rozporządzenia musimy pamiętać, że chronimy nie tyle przedsiębiorstwo jako organizację i jej zasoby, ale przede wszystkim osoby, które są z nią w ten czy inny sposób związane. I tu jest klucz do zrozumienia istoty wymogów RODO. Skupiamy się na tym, żeby było dobrze pojedynczemu Janowi Kowalskiemu, którego dane u siebie przetwarzamy. Jeśli to zrozumiemy, łatwiej nam będzie określić, kiedy już osiągnęliśmy zgodność z nowymi przepisami, a kiedy jeszcze musimy zrobić coś więcej. Ważne jest, by mieć świadomość, że nie chodzi o samo bezpieczeństwo informacji, lecz zadbanie o komfort osoby, której dane mamy u siebie.

Szymon Dudek, Infonet Projekt

Czy w kontekście branży IT można mówić o czymś takim jak specjalizacja w RODO?

Mariusz Kochański Moim zdaniem jest to szeroko pojęty obszar bezpieczeństwa. Bo za chwilę pojawi się też nowe rozporządzenie e-privacy. Jeśli będzie traktowane równie poważnie jak RODO, to dotyczyć będzie kolejnych obszarów, w tym rozwiązań technologicznych, ale przede wszystkim procesów biznesowych. Poza tym mamy postępujący proces cyfryzacji, który obejmuje kompletnie wszystkie sfery naszego życia. Wycieki danych będą momentalnie nagłaśniane w sieciach społecznościowych i będą psuły reputację podmiotów, które padły ofiarą ataków. Zapewnienie bezpieczeństwa zasobów będzie się więc stawało coraz ważniejszym wyzwaniem na polu informatyki. Postępująca cyfryzacja życia spowoduje, że kompetencje w dziedzinie zabezpieczeń wśród resellerów staną się najważniejszym wyróżnikiem ich konkurencyjności.

Marcin Serafin Według mnie istotniejsza będzie specjalizacja w ogólnie pojętym obszarze zgodności z regulacjami. RODO to tylko jeden z elementów procesu ustawicznego dostosowywania informatyki do zmian wynikających z prawa. Już niedługo wejdzie w życie ustawa o odpowiedzialności podmiotów zbiorowych, która wymusi budowanie zaawansowanych systemów zarządzania zgodnością z regulacjami prawnymi. Z drugiej strony od wielu lat widzimy na Zachodzie coraz silniejszy trend polegający na tworzeniu wewnętrznych regulacji. Równolegle możemy powiedzieć o wyzwaniach związanych z przeciwdziałaniem praniu brudnych pieniędzy, o dyrektywie PSD2, która wpłynęła na działalność wielu firm w zakresie usług płatniczych. Warto pamiętać również o szeregu innych regulacji, które będą wymagały umiejętności szybkiego zidentyfikowania wyzwań i przełożenia nowych aktów prawnych na systemy informatyczne. Dlatego, poza bezpieczeństwem, obszar compliance będzie potrzebował coraz więcej ekspertów znających się na związanych z nim wyzwaniach.

Rozmawiał
Andrzej Gontarz