ZARZĄDZANIE RYZYKIEM W BIZNESIE

SKUTECZNIE MONITOROWAĆ PŁYNNOŚĆ FINANSOWĄ FIRMY

W dojrzałych firmach, które mają świadomość, że niewypłacalność partnerów biznesowych wpływa na płynność finansową całego przedsiębiorstwa, najważniejsze są działania prewencyjne. Sztuka zarządzania finansami i monitorowania płynności finansowej polega na takim kierowaniu procesami zachodzącymi w firmie, by sprawić, aby nasz klient nigdy nie stał się dłużnikiem niewypłacalnym lub nie zwlekał z płatnościami. W jaki sposób to osiągnąć? Odpowiednio analizując i monitorując trzy zasadnicze etapy współpracy z klientem: proces kredytowania, działania prewencyjne i odzyskiwanie opóźnionych płatności.

Justyna **Przybylska**

ekspert Lindorff

Etap pierwszy: proces kredytowania pod szczególnym nadzorem

Wszystkie firmy, które osiągają korzystne wyniki finansowe, mają dobrze rozwinięte procedury zarządzania ryzykiem kredytowym. W kontaktach z klientem postępują ostrożnie. Przede wszystkim starają się go poznać, sprawdzić jego wiarygodność. Ustalają limity kredytowe, a często przy rozpoczęciu współpracy sprzedaż realizują wyłącznie za gotówkę. Dopiero po weryfikacji wypłacalności klienta przechodzą na system fakturowania z odroczonym terminem płatności. Ważnym elementem jest planowanie limitów kredytowych, ogólnej kwoty udzielonego kredytu handlowego oraz dystrybucji ryzyka dla całego portfela klientów. Takie rozsądne podejście pozwala utrzymywać płynność finansową na odpowiednim poziomie. Jeśli dana firma nie jest w stanie sama sprawdzić potencjalnego partnera, może skorzystać z pomocy profesjonalnych wywiadowni gospodarczych lub też agencji detektywistycznej (np. Lindorff Detektyw). Firmy te na zlecenie swoich klientów przygotowują raporty zawierające informacje formalno-prawne dotyczące potencjalnego kontrahenta, pełne informacje finansowe wraz z historią ewentualnego zadłużenia, powiązaniami kapitałowymi, a także oceną dotyczącą limitu możliwych zobowiązań.. Sprawdzenie klienta to jednak nie wszystko. Aby dobra do tej pory sytuacja nie wymknęła się spod kontroli, warto pomagać klientom w regularnej spłacie zobowiązań.

Etap drugi: współpraca bez długu

Firmy, które zajmują się sprzedażą posiadają rozbudowany system księgowy, w którym mogą sprawdzić saldo należności wymagalnych oraz ocenić, kiedy dojdzie do przekroczenia terminów zapłaty faktur. W sytuacji, kiedy zbliża się termin płatności, jedynie firmy, które dbają o swoją płynność, powiadamiają o tym fakcie swoich klientów. To wbrew pozorom bardzo ważne, by w oczach klientów być firmą, która systematycznie upomina się o swoje należności. Wówczas mamy większe szanse na otrzymanie ich na czas. Klienci zwykle szanują firmy, które potrafią szanować siebie i wymagać płatności w terminie.

Jeśli więc zależy nam na dobrej współpracy z kontrahentem, a co za tym idzie — utrzymaniu płynności finansowej przedsiębiorstwa, warto zastanowić się nad wprowadzeniem monitoringu płatności. Pozwala ona na kontrolę wpływu należności nie tylko dzięki przypominaniu o terminach wymagalności faktur, ale także weryfikacji ich poprawności (danych adresowych, numerów NIP) czy też potwierdzeniu odbioru faktury przez drugą stronę. Monitoring należności zwykle prowadzony jest na dwóch etapach. Po pierwsze przed upływem terminu płatności w postaci tzw. działań prewencyjnych, czyli systemu przypomnień o zbliżającym się terminie zapłaty, co zapobiega opóźnieniom w regulowaniu należności. Drugim etapem jest monitoring należności z bardzo krótkim okresem przeterminowania (nie dłużej niż 30 dni od daty upływu wymagalności). Działania firmy monitorującej polegają w tym przypadku na stałym kontakcie z klientem – częstych rozmowach telefonicznych i wezwaniu do zapłaty. Do głównych korzyści tego typu usługi należy zaliczyć poprawę płynności finansowej firmy, zwiększenie dyscypliny płatniczej klientów, wykrycie nierzetelnych kontrahentów, obniżenie kosztu obsługi należności (w przypadku niedopuszczenia do windykacji), brak konieczności angażowania własnych pracowników w proces odzyskiwania należności, utrzymywanie pozytywnych relacji z kontrahentami. Każdorazowo sposób monitoringu płatności u danego klienta ustalany jest na podstawie dotychczasowej współpracy z partnerami, specyfiki branży, wartości należności, a także terminów płatności i wszelkich kwestii indywidualnych.

Etap trzeci: gdy zawiedzie prewencja

Jeśli nie podjęliśmy działań prewencyjnych w odpowiednim czasie lub też okazały się one nieskuteczne, kolejnym etapem, który uchroni nas przed zachwianiem płynnością finansową naszej firmy jest właściwa windykacja zaległych należności. Decyzja o zleceniu działań windykacyjnych zewnętrznemu podmiotowi oraz jego wybór powinien być podyktowany naszymi potrzebami. Dla czystości relacji biznesowych, tak jak w przypadku działań monitorujących, warto zdjąć obowiązek windykowania klientów z pracowników firmy. Wyspecjalizowane podmioty zarządzające należnościami zrobią to w pełni profesjonalnie i z poszanowaniem zasad etyki. Zatrudniają doświadczonych negocjatorów i windykatorów terenowych, posiadają pełną bazę danych dłużników, znają mechanizmy windykacyjne, a także kwestie prawne z nimi związane.

Należy jednak pamiętać, że współczesna, profesjonalna windykacja to już nie tylko ściąganie długów, ale przede wszystkim kompleksowe zarządzanie należnościami. Im wcześniej zdecydujemy się więc na współpracę z firmą specjalizującą się w tym obszarze, tym łatwiej będzie nam zatrzymać proces współpracy z klientem na etapie prewencji lub nawet na etapie procesu kredytowania. Wówczas nasz klient nigdy nie stanie się dłużnikiem. A to świadczyć będzie o biznesowej dojrzałości naszego przedsiębiorstwa.

BIZNES RAPORT
GAZETA FINANSOWA
15–21 września 2017 r.

Zdolność identyfikacji zagrożeń

Zmieniające się warunki biznesowe wymagają od specjalistów ciągłej gotowości do poszerzania swoich kompetencji. To szczególnie ważne w przypadku specjalistów ds. rachunkowości zarządczej, którzy zajmują się przewidywaniem potencjalnych zdarzeń. Nie tylko z pola finansowego, ale również społecznego czy politycznego. W ten sposób obniżane jest ryzyko, wpływające na operacyjność i wynik finansowy organizacji.

Dodatkowo z danych CIMA wynika, że zaledwie 1/3 europejskich firm wdrożyło zaawansowany model zintegrowanego zarządzania ryzykiem (ERM), nad którym pieczę sprawują komitety audytu lub specjalnie powoływane komitety ryzyka. Tak wynika z badań przeprowadzonych przez Instytut CIMA, który jednocześnie zwraca uwagę, że zarządzanie ryzykiem powinno stać się jednym z priorytetów każdej organizacji działającej we współczesnej gospodarce.

Działać dynamicznie

Otoczenie biznesowe, ze względu na aktualne wyzwania gospodarcze, wymusza na firmach niespotykaną dotąd dynamikę działań. Przedsiębiorstwa muszą elastycznie dopasowywać się do warunków panujących na rynku, wdrażając zmiany w krótkim czasie. Wynika to między innymi z intensywnego postępu technologicznego i rewolucji cyfrowej, która naraża nieprzygotowane na nią firmy na poważne konsekwencje biznesowe. To nie jedyna grupa ryzyk, z którą muszą zmierzyć się przedsiębiorstwa. Nowe technologie przynoszą ze sobą nowe modele biznesowe dla firm. Co ważne, na ich skuteczność w zglobalizowanej gospodarce nie wpływa wyłącznie sprawne samodzielne działania instytucji, ale także liczne czynniki geopolityczne. W tej sytuacji kluczowa staje się nie tylko zdolność identyfikacji zagrożeń, lecz także oceny ich wagi dla firm i instytucji w określonym czasie oraz rzetelnej analizy możliwych konsekwencji.

Coraz trudniejsze wyzwania

Potwierdzają to badania przeprowadzone przez Instytut CIMA. – Aż 60 proc. organizacji reprezentujących różne branże mierzy się z coraz trudniejszymi wyzwaniami, które w sposób znaczący mogą wpłynąć na strategiczny sukces ich przedsięwzięć. Efektywne wdrożenie modeli identyfikacji zagrożeń spowalnia w ich wypadku przede wszystkim konieczność ustalenia priorytetów. 2 na 5 reprezentantów badanych firm uważa, że nie posiada odpowiednich zasobów, by zoptymalizować nadzór nad ryzykiem. Raport CIMA pokazuje, że niemal drugie tyle specjalistów odczuwa konieczność przeznaczenia budżetu na inne, bardziej pilne i znaczące wydatki. Z jednej strony mamy więc sytuację, w której na organizacje wpływa coraz więcej zewnętrznych czynników, trudnych do zrozumienia i uwzględnienia w strategii. Jednocześnie jednak osoby odpowiedzialne za zarządzanie przedsiębiorstwami wydają się jeszcze nie doceniać powagi tych zmian. A ta sytuacja będzie się w najbliższych latach tylko pogłębiać – tłumaczy Jakub Bejnarowicz, szef CIMA w Europie Środkowo–Wschodniej.

GAZETA FINANSOWA
15–21 września 2017 r.

BIZNES RAPORT

Cyberzagrożenia – lekceważone czy niezrozumiałe? Kto w przedsiębiorstwie odpowiada za bezpieczeństwo w sieci.

Panuje powszechne przekonanie, że cyberataki dotyczą głównie sektorów rządowych, choć tak naprawdę narażeni jesteśmy na nie wszyscy. Prywatne przedsiębiorstwa często nie zdają sobie sprawy, że „ciosy" są wymierzane także w ich dane. Co zrobić, aby uniknąć zagrożenia? Czy w dobie cyfryzacji to w ogóle możliwe?

Marcin **Marczewski**

kierownik studiów podyplomowych „Cyberbezpieczeństwo – normy, standardy i dobre praktyki" w Akademii Leona Koźmińskiego oraz CEO w firmie Resilia | architekci odporności biznesu.

Żyjemy w przeświadczeniu, że pewne problemy nas nie dotyczą. Dokładnie tak jest z atakami cyfrowymi. Słyszymy o nich i zdajemy sobie sprawę, że nasz komputer potrzebuje zabezpieczenia w postaci antywirusa, ale nie wiemy, jakie dane mamy chronić. W pierwszej chwili wskażemy zapewne na maile, umowy i konta bankowe, ale tak naprawdę ścisłym nadzorem objęte są wszystkie informacje, które są istotne dla firmy z punktu widzenia biznesowego, m.in. dane finansowe, technologia, wiedza, know-how i strategie marketingowe. To też dane klientów, które nam powierzyli w celu świadczenia usług również podczas rozmów i czatów. Właśnie dlatego zarówno jako pracownik, jak i pracodawca, jesteśmy zobowiązani, by poznać zasady cyberbezpieczeństwa.

Ochrona przede wszystkim

Opieka nad danymi firmowymi obowiązuje nas przez cały czas. Jest niezwykle ważna z punktu widzenia wizerunkowego i prawnego. Trudno sobie wyobrazić by klienci, których poufne informacje znalazły się na „czarnym rynku", nie wystosowali przeciwko nam pozwu. Może to doprowadzić do odejścia klientów i kontrahentów oraz braku napływu nowych, co w dłuższej perspektywie wiąże się z upadłością organizacji. – Dlatego ważne jest zrozumienie, że obecnie dane nie są wyłącznie przetwarzane w systemach IT. Oznacza to, że firmy powinny nie tylko wdrażać techniczne zabezpieczenia, lecz także proaktywnie działać, podnosząc świadomość pracowników w zakresie istotnych zagrożeń dla bezpieczeństwa w miejscu pracy, jak i poza nim. Zatrudnione osoby nie zawsze rozumieją to pojęcie. I choć w umowach zalecamy im ścisły nadzór nad informacjami dotyczącymi spółki, zabezpieczamy firmowy sprzęt i prosimy o podpisanie NDA, to do naszych obowiązków należy ich merytoryczne przygotowanie – tak, aby zrozumieli, jak istotne jest bezpieczeństwo informacji. Pomoże to zwłaszcza, gdy nastąpi wyciek poufnych danych, a to może zdarzyć się nawet najlepiej przeszkolonemu pracownikowi – w końcu wszyscy jesteśmy ludźmi i popełniamy błędy.

Szczerość w przypadku „wpadki"

Najważniejszym aspektem jest jak najszybsze zgłoszenie incydentu bezpieczeństwa odpowiednim osobom i pełna szczerość z pracodawcą. Możliwe jest wtedy ograniczenie strat wynikających ze zdarzenia oraz wdrożenie procesów powiadamiania klientów o wycieku danych.
Zatajenie takiego zajścia będzie miało dla pracownika poważne konsekwencje. Podobnie jest z umyślnym naruszeniem tajemnicy przedsiębiorstwa czy danych osobowych. Oprócz kar umownych sprawę możemy skierować do sądu.

Ewolucja czy rewolucja?

Ochrona danych osobowych w kontekście zmian związanych z wejściem w życie Rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/67 z dnia 27 kwietnia 2016 r. w sprawie ochrony danych osobowych (dalej- RODO) jest obecnie jednym z głównych tematów, który interesuje przedsiębiorców, a w szczególności tych działających na rynku finansowym. W związku z nową regulacją warto zastanowić się, czy czeka nas rewolucja, czy może ewolucja w zakresie ochrony danych osobowych.

Marcin **Kamiński**

ekspert Mikrokasa

RODO wprowadza do systemu prawnego kilka nowych obowiązków dla przedsiębiorców, jak również praw dla klientów. Często wiążą się one z rozszerzeniem już funkcjonujących instytucji, a czasami wymagają wprowadzenia nowych rozwiązań. Należy jednak zauważyć, że będzie to raczej ewolucja dotychczasowego modelu ochrony danych osobowych, a nie jego rewolucja.

Ewolucja w zakresie obowiązków przedsiębiorców i praw klientów

Przykładowo RODO wymaga od przedsiębiorcy, aby w zrozumiałej i łatwo dostępnej formie, jasnym i prostym językiem udzielił osobie, której dane dotyczą, wszelkich informacji dotyczących przetwarzania danych osobowych. Nowe przepisy modyfikują również obowiązek informacyjny, a także wprowadzają pewne zmiany w zasadach uzyskiwania ważnych zgód na przetwarzanie danych osobowych od osób, których dane dotyczą. Nowelizacja w tym zakresie nie powinna być dla przedsiębiorców dużym problemem, ponieważ dotychczas również musieli takie obowiązki spełniać, czy to na podstawie przepisów obowiązującej ustawy o ochronie danych osobowych, czy na tle decyzji Generalnego Inspektora Ochrony Danych Osobowych lub orzecznictwa sądów. W większości będą konieczne jedynie drobne modyfikacje w dotychczas prowadzonej działalności gospodarczej.
Więcej wysiłku będzie mogło wymagać wprowadzenie nowych praw dla klientów, o których mowa w RODO. Prawo do bycia zapomnianym (zgodnie z którym osoba, której dane dotyczą, będzie mogła domagać się usunięcia swoich danych), prawo do przenoszenia danych osobowych, a także wzmocnione prawo dostępu i wglądu obywatela w jego dane może wiązać się z większymi uciążliwościami. Konieczne w ich przypadku będzie często nie tylko dostosowanie systemu informatycznego przedsiębiorcy, ale również odpowiednie przeszkolenie ludzi i wprowadzenie nowych procedur. W związku z powyższym pomimo tego, że RODO wchodzi w życie w maju 2018 r., to większość przedsiębiorców już teraz powinno starać się dostosować swoją działalność do nowych przepisów, wprowadzając swoistą ewolucję w dotychczasowym systemie ochrony danych osobowych.

Rewolucja w zakresie sposobu myślenia o ochronie danych osobowych i zarządzaniu ryzykiem z tym związanym

Przedsiębiorców będzie natomiast czekała rewolucja w sposobie myślenia o ochronie danych osobowych oraz zmiany w systemie zarządzania ryzykiem z tym związanym. Celem powinno być znalezienie odpowiedniego balansu pomiędzy ochroną danych osobowych jako prawa podstawowego oraz rozwojem działalności gospodarczej.
Powyższe będzie wiązało się z nowym obowiązkami takimi jak przygotowanie procedur przed przetwarzaniem danych osobowych oraz wprowadzenie odpowiednich rozwiązań technologicznych. Znikną sztywne regulacje jak np. dotychczasowe rozporządzenie Ministra Spraw Wewnętrznych i Administracji w sprawie dokumentacji przetwarzania danych osobowych oraz warunków technicznych i organizacyjnych, jakim powinny odpowiadać urządzenia i systemy informatyczne służące do przetwarzania danych osobowych z dnia 29 kwietnia 2004 r. (Dz.U. Nr 100, poz. 1024).
Przedsiębiorcy będą musieli uwzględniając charakter, zakres, kontekst i cele przetwarzania oraz ryzyko naruszenia praw lub wolności klientów wdrożyć odpowiednie środki, a także wykazać, że przetwarzania danych osobowych odbywa się zgodnie z RODO. Administratorzy danych będą musieli przyjąć wewnętrzne polityki i wdrożyć środki, które będą zgodne w szczególności z zasadą uwzględnia danych w fazie projektowania (privacy by design) oraz zasadą domyślnej ochrony danych osobowych (privacy by default). Ciężar odpowiedniego zabezpieczenia danych będzie spoczywało na przedsiębiorcy.
Wywiązywanie się z obowiązków administratora danych przez przedsiębiorców będzie można wykazać między innymi przez stosowanie zatwierdzonych kodeksów postępowania lub mechanizmów certyfikacji dokonywanych przez uprawnione podmioty certyfikujące. Dodatkowo, jeżeli dany rodzaj przetwarzania danych, zwłaszcza z użyciem nowych technologii, ze względu na swój charakter, zakres, kontekst i cele może nieść duże zagrożenie dla praw i wolności osób fizycznych, przedsiębiorca przed rozpoczęciem przetwarzania danych osobowych będzie musiał dokonać oceny skutków planowanych operacji przetwarzania dla ochrony danych osobowych.

Podsumowanie

Jako podsumowanie niniejszych rozważań dotyczących RODO chciałbym przytoczyć fragment wypowiedzi dr Edyty Bielak-Jomaa obecnego Generalnego Inspektora Danych Osobowych, którą wygłosiła na Konferencji „Ochrona danych osobowych w kontekście zmian prawa" organizowanej przez Uniwersytet Gdański w maju 2017 r., a mianowicie, iż w systemie ochrony danych osobowych czeka nas „ewolucja, ale są elementy rewolucji". Moim zdaniem to krótkie stwierdzenie najlepiej oddaje charakter zmian, jakie wprowadza RODO. Konieczne jest nie tylko odpowiednie zmodyfikowanie obowiązków przedsiębiorców oraz praw klientów, które już funkcjonują, ale przede wszystkim zmienienie sposobu myślenia o ochronie danych osobowych. Dzisiejszy świat oparty na informacji oraz rozwoju nowych technologii wprowadza również nowe zagrożenia, a co za tym idzie, konieczne jest dostosowywanie się przedsiębiorców do ryzyka z tym związanego. Powyższe jest niemożliwe w przypadku narzucenia zbyt sztywnych ram prawnych, a wymagane w takim przypadku jest raczej wprowadzenie odpowiednich systemów zarządzania ryzykiem z tym związanym przez samych przedsiębiorców.

BIZNES RAPORT
GAZETA FINANSOWA
15–21 września 2017 r.

Pamiętajmy, że przekazanie informacji na temat zdarzenia w przypadku takich incydentów to również nasz, jako pracodawców, obowiązek. Jeśli nie wyjaśnimy podwładnym, jak wyglądają formalności w tym zakresie, nie możemy spodziewać się, że zadziałają zgodnie z nimi.

Merytoryczne szkolenia

Za wyciek danych nie odpowiadają tylko osoby zatrudnione. Spora część odpowiedzialności leży po naszej stronie. Dla realnego podniesienia poziomu bezpieczeństwa w firmie potrzebny jest cały cykl szkoleń. Mogą to być wewnętrzne e-learningi przygotowywane przez dział IT. Ale muszą to być naprawdę dobre merytorycznie materiały, które zainteresują pracownika. Po każdym takim szkoleniu przeprowadźmy test on-line, który da władzom firmy obraz świadomości pracowników. Analizujmy wyniki tych sprawdzianów: ci, którzy nie osiągną odpowiednich rezultatów, powinni kurs powtórzyć.

Również testy socjotechniczne powinny być przeprowadzane cyklicznie. To dobre rozwiązanie, żeby sprawdzić, czy zatrudnieni w naszej firmie są świadomi zagrożeń oraz jak zapamiętują najważniejsze przekazy szkoleń. Dział IT będzie wiedział, jak sobie z tym poradzić, zwłaszcza, że jednym z narzędzi są np. spreparowane maile, których celem jest wyłudzenie m.in. danych do logowania.

> **Świadomość, świadomość i jeszcze raz świadomość. Nie ma lepszego sposobu dla pracodawcy na zminimalizowanie ryzyka związanego z bezpieczeństwem danych w firmie niż nieustanne akcje podnoszenia wiedzy: przypominanie zasad bezpieczeństwa teleinformatycznego, pokazywanie przykładów**

Świadomość

Dobra ochrona to też sprawdzone zabezpieczenia. Ważne są zarówno programy służące do monitorowania aktywności pracowników, jak i kampanie uświadamiające. Jak zaznacza ekspert, w tym wypadku nie chodzi o prostą prezentację z pisemnym potwierdzeniem zapoznania się z treścią, a to niestety częsta praktyka w polskich firmach. Świadomość, świadomość i jeszcze raz świadomość. Nie ma lepszego sposobu dla pracodawcy na zminimalizowanie ryzyka związanego z bezpieczeństwem danych w firmie niż nieustanne akcje podnoszenia wiedzy: przypominanie zasad bezpieczeństwa teleinformatycznego, pokazywanie przykładów – negatywnych konsekwencji nieprzestrzegania zasad zarówno dla firmy, jak i dla osoby prywatnej. Powinniśmy sobie uświadomić, że cyberbezpieczeństwo nie jest stanem, a procesem. Jeśli organizacje nie postarają się o jego skuteczne wdrożenie, zawsze będą na straconej pozycji.

Cyberataki przestały być iluzoryczne. Media cały czas nagłaśniają te skierowane w duże organizacje rządowe, ale następnymi ofiarami możemy być my sami. Choć teoretycznie wiemy, co robić, okazuje się, że nie potrafimy ochronić nawet własnego konta bankowego, nadając mu te same hasła, co do Facebooka i innych portali, z których mogą wyciekać dane. Szkolenie z bezpieczeństwa w sieci to kurs, z którego skorzystają wszyscy.

GAZETA FINANSOWA
15–21 września 2017 r.
BIZNES RAPORT

„By default" i „by design" – czyli ochrona prywatności według RODO

Już teraz wiele organizacji traktuje bezpieczeństwo informacji bardzo poważnie i bierze pod uwagę ochronę danych osobowych w projektowaniu nowych produktów czy usług. Te dobre praktyki, zgodnie z nowym unijnym rozporządzeniem o ochronie danych osobowych (RODO), staną się od 25 maja 2018 roku obowiązkowe. Wymóg ochrony danych domyślnie („by default") i w fazie projektowania („by design") przyniesie użytkownikom i firmom korzyści – oto 3 najważniejsze z nich.

adv. Marcin **Zadrożny**
ekspert Fundacji
Wiedza To Bezpieczeństwo

1. Większa troska o dane osobowe konsumentów
Według RODO, ochrona danych ma być uwzględniona już na etapie projektowania systemu ochrony danych osobowych („by design"), a także ma być aktywna domyślnie („by default"). Dzięki realizacji „data protection by design" przez przedsiębiorstwo, użytkownik korzystając np. z aplikacji mobilnej, strony internetowej lub biorąc udział w konkursie będzie miał pewność, że ochrona jego danych została wdrożona przez administratorów jeszcze na etapie projektowania tejże usługi. Unijne regulacje w zakresie ochrony danych osobowych mają służyć konsumentowi – „data protection by default" to zapewnienie użytkownikowi ochrony jego danych.

2. Budowanie zaufania konsumentów i wizerunku wiarygodnego przedsiębiorstwa
Nowe przepisy, które przyjęła Unia Europejska mają mobilizować przedsiębiorców do stosowania nowoczesnego podejścia w przetwarzaniu danych osobowych. Firmy, które do tej pory traciły wizerunkowo nie zapewniając odpowiedniej ochrony danym swoich klientów, mają szansę odbudować swoją wiarygodność. Mogą to zrobić właśnie dzięki m.in. przyjęciu odpowiednich wewnętrznych polityk i wdrożeniu środków, które są zgodne w szczególności z zasadą uwzględniania ochrony danych w fazie projektowania oraz wdrożeniem domyślnej ochrony danych. Firmy będą musiały udowadniać, że przetwarzają dane osobowe klientów zgodnie z prawem, a także później to wykazać zgodnie z zasadą rozliczalności przed organem nadzorczym. Będzie to możliwe m.in. poprzez uzyskanie certyfikacji.

3. Koszty wdrożeń mechanizmów ochrony danych i szybsza reakcja na problemy
Wejście w życie RODO wiąże się z kosztami – często sporymi – dla przedsiębiorców. Każda organizacja przetwarzająca dane osobowe będzie zobligowana do wdrożenia odpowiednich środków technicznych i organizacyjnych. Będzie musiała przy tym uwzględnić stan wiedzy technicznej, koszt wdrażania oraz charakter, zakres, kontekst i cele przetwarzania, a także ryzyko naruszenia praw lub wolności osób fizycznych o różnym prawdopodobieństwie wystąpienia i wadze zagrożenia. Podsumowując organizacje będą zobligowane do analizy ryzyka. Jeżeli firma nie zapewni stopnia bezpieczeństwa odpowiadającego ryzyku, czyli nie wdroży odpowiednich środków technicznych i organizacyjnych, będzie mogła zostać ukarana wysokimi karami administracyjnymi.
Działy IT również będą mogły szybko reagować na wszelkie sytuacje kryzysowe. W przypadku produktów i usług online istotnym elementem jest technologia komputerowa, dlatego też w odpowiednie procedury firmy będą musiały wdrożyć zwłaszcza architektów rozwiązań informatycznych oraz programistów.

> **Firmy będą musiały udowadniać, że przetwarzają dane osobowe klientów zgodnie z prawem, a także później to wykazać zgodnie z zasadą rozliczalności przed organem nadzorczym. Będzie to możliwe m.in. poprzez uzyskanie certyfikacji.**

Ochronić dane klienta – analiza ryzyka jako niezbędny element ochrony danych osobowych

Najbliższe miesiące zapowiadają się niezwykle pracowicie dla wszystkich specjalistów od cyberzagrożeń, ale nie tylko. Nowa regulacja – Ogólne Rozporządzenie o Ochronie Danych Osobowych (RODO/GDPR) – wymaga od firm holistycznego podejścia do kwestii ochrony danych osobowych. Wynika to przede wszystkim z coraz większej potrzeby zachowania prywatności osób w dobie internetu.

Radek **Kaczorek**
CEO IMMUSEC

Zgodnie z wynikami badań Eurobarometru (2016) dla 72 proc. badanych mieszkańców UE ważne jest zagwarantowanie tajności ich e-maili i innej korespondencji online, a 71 proc. nie akceptuje, gdy firmy dzielą się informacjami o użytkownikach bez ich pozwolenia. Dlatego też Unia Europejska zdecydowała się na szczególną ochronę danych swoich obywateli.

RODO – rewolucja w dziedzinie ochrony danych
RODO zacznie obowiązywać 25 maja 2018 roku, zatem przedsiębiorcom zostało niecałe pół roku na przystosowanie się do nowych zaleceń. Czy to dużo, czy mało – zależy od charakteru firmy, rodzaju i ilości przetwarzanych i gromadzonych danych, a przede wszystkim od świadomości i gotowości na zmiany.
Obowiązująca jeszcze Ustawa o Danych Osobowych (UODO) wymagała wypełnienia zamkniętego katalogu zabezpieczeń, które od czasu ich wprowadzenia stały się archaiczne i nieprzystające do obecnych zagrożeń. RODO oznacza natomiast nowe podejście: wewnętrzne regulacje i mechanizmy kontrolne powinny opierać się na regularnie wykonywanej analizie ryzyka – a nie wprost wskazanych przez regulatora rozwiązaniach. Menedżerowie spółek są zobowiązani do oceny ryzyka związanego z danymi osobowymi przetwarzanymi przez organizację oraz zaprojektowania rozwiązania, które to ryzyko obniża do akceptowalnego poziomu.

Kto powinien wdrożyć wymagania RODO?
RODO dotyczy wszystkich firm przetwarzających dane osobowe: czy to w procesach rekrutacji czy HR, w procesach marketingowych i sprzedażowych (np. generowanie leadów, CRM), czy też bieżącej obsługi klientów, o własnych pracownikach nie wspominając. Przejście z UODO na RODO obejmuje zatem wiele dziedzin, na przecięciu nie tylko technologii i prawa, ale też zarządzania.
Zarządzający biznesem powinni być otwarci na zmiany i zrozumieć, że obecnie nie ma „bezpiecznych" branż. Rokrocznie liczba incydentów bezpieczeństwa (włamań, wycieków danych) rośnie o 70 proc., a skutki finansowe tych incydentów na świecie przekraczają astronomiczne kwoty rzędu 500 miliardów dolarów rocznie. Dotyczą one nie tylko dużych firm, coraz częściej ofiarami incydentów padają przedsiębiorstwa średnie i małe. Aż 94 proc. incydentów wynika – mniej więcej w równych proporcjach – z błędu ludzkiego albo złośliwego oprogramowania. Antywirus i firewall już nie wystarczą, by zachować bezpieczeństwo. Jednocześnie polski rynek specjalistów bezpieczeństwa jest bardzo płytki i od kilku lat notuje rosnący deficyt na poziomie nawet kilkunastu tysięcy ekspertów. Tej luki nie uzupełnią kancelarie prawne dotychczas zajmujące się pomocą w ochronie danych osobowych.

Jak „ugryźć" RODO – podejście bazujące na ryzyku
O tym, jak złożonym aktem prawnym jest RODO może świadczyć chociażby proste porównanie: obecna ustawa definiuje 11 wymagań technicznych. Z kolei nowa regulacja takiej zamkniętej listy nie definiuje, a jedynie mówi: ma być bezpiecznie w sposób adekwatny do ryzyka. Jak zatem stwierdzić, czy zabezpieczenia są adekwatne? Drogowskazem może być tu np. norma ISO 27 001. Zawiera ona m.in. 114 wymaganych punktów kontrolnych, które pozwalają na określenie wymaganych zabezpieczeń! W praktyce przekłada się to na ponad 500 pytań, które trzeba sobie zadać, żeby ocenić czy chronimy dane osobowe adekwatnie do ryzyka.
Zgodnie ze sztuką zarządzania ryzykiem należy określić krytyczne procesy, wskazać zagrożenia dla ich realizacji oraz określić prawdopodobieństwo i ewentualne skutki ich wystąpienia. To zarządzający decydują jaki poziom ryzyka akceptują i jakie zagrożenie jest priorytetowe, a jakie można przesunąć na drugi plan. Jednak sama analiza ryzyka i jej świadomość w zarządach nie rozwiązują sprawy. Kolejne kroki to wprowadzenie serii zabezpieczeń oraz ciągłe monitorowanie incydentów. RODO wymaga od firm zgłaszania każdego incydentu do organów nadzoru w 72 godziny po jego wykryciu, a statystyki rynkowe mówią, że średni czas, który upływa od incydentu do jego wykrycia, sięga nawet 8 miesięcy! Oczywiście zarządzający mogą każde ryzyko zaakceptować, muszą jednak być świadomi, że nowe kary będą sięgały aż 20 milionów euro lub do 4 proc. całkowitego rocznego światowego obrotu firmy. Mamy więc do czynienia z prostym rachunkiem ekonomicznym – ryzykować nałożenie na firmę ogromnej kary, czy inwestować w bezpieczeństwo i obniżyć to ryzyko.

Najważniejsze wyzwanie – IT czy biznes?
Jednym z największych wyzwań jest identyfikacja ryzyk w obszarze bezpieczeństwa informacji i danych osobowych, które należy określić z punktu widzenia procesów biznesowych, a nie jedynie samej informatyki.
Sam dział informatyki nie zdefiniuje, które procesy biznesowe są dla firmy najważniejsze, ani które dane są najbardziej krytyczne. Właściciele poszczególnych procesów biznesowych powinni określić możliwe ryzyko i jego wpływ na firmę: np. ocenić, które dane niedostępne przez 2 godziny, 1 dzień, czy tydzień będą miały znaczący wpływ na funkcjonowanie i wyniki firmy. Konieczne jest też zidentyfikowanie wszystkich miejsc, w których dane osobowe są przetwarzane. Wraz z wejściem w życie RODO każdy uzyskuje prawo do zapomnienia, a więc żądania usunięcia swoich danych ze wszystkich systemów i baz firmy, która takie dane przetwarza, a także prawo do wydania wszystkich danych osobowych w formie zrozumiałej dla maszyny (np. XML). Oznacza to zbudowanie przez działy informatyki zupełnie nowej zdolności, której obecnie nie posiadają.

Klienci to docenią
Należy wprost powiedzieć, że RODO jest pierwszą regulacją dotyczącą danych osobowych, która narzuca tak rygorystyczne kary. Warto jednak pamiętać, że poszanowanie prywatności jest przede wszystkim kluczowe dla klientów i to oni w ostateczności zadecydują, której firmie ufają, a której nie. Zatem zbudowanie strategii cyberbezpieczeństwa z zastosowaniem podejścia opartego na ryzyku jest nie tylko sposobem na uzyskanie zgodności i uniknięcie kar. To przede wszystkim sposób na zbudowanie przewagi konkurencyjnej i zaoferowanie klientom gwarancji, że ich dane są bezpieczne. Jeśli tylko firma skorzysta z najlepszych praktyk na rynku oraz istniejących rozwiązań procesowych i technicznych, wdrożenie zgodności z RODO nie będzie ani drogie, ani czasochłonne.