OGÓLNE ROZPORZĄDZENIE O OCHRONIE DANYCH

(ANG. GENERAL DATA PROTECTION REGULATION, GDPR)

CZAS DZIAŁAĆ!

Raport przedstawiający stan przygotowania przedsiębiorstw działających w Polsce do wdrożenia przepisów zawartych w GDPR oraz podjęcia działań mających na celu ochronę przed cyberzagrożeniami

ORGANIZATORZY:

TREND MICRO™

vmware®

PATRON:

FUNDACJA bezpieczna cyberprzestrzeń

WPROWADZENIE

Po czteroletnich negocjacjach Europa uczyniła duży krok w stronę stworzenia skuteczniejszych, ogólnoeuropejskich przepisów o ochronie danych. W grudniu 2015 r. państwa europejskie uzgodniły treść nowego rozporządzenia unijnego, tzw. ogólnego rozporządzenia o ochronie danych, które wchodzi w życie z dniem 25 maja 2018 r. i ma zastosowanie w przedsiębiorstwach oraz instytucjach przetwarzających lub gromadzących dane osobowe osób przebywających w krajach Unii Europejskiej. Nowe przepisy o ochronie danych nie dotyczą wyłącznie przestrzegania wymogów formalnych. Zmianie ulegną również zasady rejestrowania, przechowywania, przetwarzania i udostępniania danych pracowników i klientów – wszystkich osób fizycznych, których dotyczą, w tym członków stowarzyszeń, odbiorców reklam, pacjentów, petentów etc.

Wejście w życie ogólnego rozporządzenia o ochronie danych[1] stanowi najistotniejszą zmianę ustawodawstwa w zakresie ochrony danych w ostatnim dwudziestoleciu. Po raz pierwszy podjęto próbę stworzenia skutecznych, praktycznych i możliwych do wyegzekwowania przepisów chroniących dane ponad 500 mln obywateli Europy. Nowy akt prawny będzie mieć daleko idące konsekwencje i najprawdopodobniej spowoduje gruntowną zmianę dotychczasowych procesów i procedur organizacyjnych we wszystkich obszarach działania przedsiębiorstw — od kadr po sprzedaż i marketing.

W krajobrazie gospodarczym Europy coraz silniej dominują zglobalizowane lub działające ponad granicami państw przedsiębiorstwa wirtualne, dynamicznie rozwijające się technologie oraz modele działalności oparte na danych. W tej sytuacji konsekwencje niezapewnienia ochrony danych lub nieprzestrzegania nowych przepisów unijnych będą mieć ogromny wpływ na rozwój i kształt rynku w przyszłości.

Nowe przepisy stworzą organom regulacyjnym realne możliwości przeciwdziałania nadużyciom. Nie będzie już miejsca na nieprzestrzeganie zasad, o czym świadczy zapis: „na firmy łamiące unijne przepisy o ochronie danych mogą być nakładane kary finansowe w wysokości nawet 4% rocznych obrotów — zwłaszcza w przypadku globalnych firm internetowych". Co więcej, rozporządzenie będzie mieć również zastosowanie w przypadku dostawców i sprzedawców mających siedzibę poza Europą, którzy dostarczają towary i usługi osobom przebywającym na terenie Unii Europejskiej oraz przetwarzają lub przechowują ich dane osobowe.

Nawet firmy przetwarzające dane poza terytorium Unii Europejskiej muszą podporządkować się przepisom ogólnego rozporządzenia o ochronie danych i liczyć się z sankcjami w przypadku ich nieprzestrzegania. W rezultacie wiele przedsiębiorstw z sektora technologicznego staje przed koniecznością stosowania się do prawa europejskiego, chociaż wcześniej wydawało się, że prawo to ich nie dotyczy.

Michał Jarski, Regional Director CEE w firmie Trend Micro

[1] Dokument jest nazywany „rozporządzeniem GDPR" od angielskiej nazwy General Data Protection Regulation; w Polsce funkcjonuje również skrót RODO od nazwy Rozporządzenie o Ochronie Danych Osobowych.

Rozporządzenie zawiera jednoznaczne przepisy dotyczące prawa obywateli do usunięcia swoich danych. Ponadto uzyskają oni prawo do otrzymywania powiadomień o wycieku danych oraz do przenoszenia danych między dostawcami, a także będą mieć łatwiejszy dostęp do tych informacji i szerszy nadzór nad sposobem ich przetwarzania.

Do wejścia w życie rozporządzenia GDPR zostały niecałe dwa lata, ale firmy już dzisiaj stają przed poważnymi wyzwaniami logistycznymi związanymi z nadzorem nad informacjami — zwłaszcza nieusystematyzowanymi danymi rozproszonymi na wielu różnych platformach. W tej sytuacji konieczne jest uświadomienie przedsiębiorcom skutków wprowadzenia nowych przepisów, ponieważ polskie firmy nie zdają sobie sprawy z wynikających z tego daleko idących zmian i nie są na nie gotowe.

Firmy Trend Micro oraz VMware we współpracy z agencją badawczą ARC Rynek i Opinia przeprowadziły badanie, którego celem było sprawdzenie, czy polskie firmy zdążyły już przygotować się na wejście w życie nowego rozporządzenia, a także poznanie ich aktualnych obaw dotyczących przestrzegania nowych przepisów. Już na wstępie warto zauważyć pewną niepokojącą sytuację, jaka ma miejsce w polskich przedsiębiorstwach. Okazuje się, że zarząd i wyższa kadra menedżerska zazwyczaj nie mają wiedzy o aspektach związanych z nowo ustanowionymi przepisami. Wobec tej sytuacji pytania były skierowane do pracowników faktycznie zajmujących się kwestiami przetwarzania i ochrony danych osobowych. Warto podkreślić, że Administratorzy Bezpieczeństwa Informacji reprezentują znikomą liczbę respondentów – najczęściej na pytania odpowiadali pracownicy kadr, specjaliści ds. administracji oraz informatycy.

GDPR: PONAD POŁOWA POLSKICH FIRM NIE MA ŚWIADOMOŚCI ISTNIENIA NOWEGO PRAWA DOTYCZĄCEGO OCHRONY DANYCH

Wyniki badania wskazują, że znajomość rozporządzenia GDPR wśród ogółu respondentów jest niepokojąco niska — ponad połowa badanych (52%) do tej pory nie słyszała o reformie ochrony danych osobowych mającej na celu zmianę dotychczasowych przepisów unijnych. Odległa perspektywa czasowa (nowe prawo zacznie obowiązywać w 2018 roku a prace nad jego nowelizacją zostały zakończone w bieżącym roku) nie sprzyja znajomości GDPR.

Jeśli spojrzymy na poszczególne sektory gospodarki, okaże się, że najniższa znajomość nowego prawa charakteryzuje sektor handlowy, w którym aż 62% firm nie słyszało o wydanym przez Komisję Europejską rozporządzeniu. Znajomość GDPR jest najwyższa wśród pracowników sektora usług (56%). Jedynie niespełna dwie trzecie badanych (61%) stwierdziło, że rozporządzenie GDPR będzie miało zastosowania w przypadku ich firmy, zaś prawie jedna piąta (18%) jest przeciwnego zdania; podobny odsetek (21%) nie ma sprecyzowanego poglądu na ten temat.

Rozporządzenie dotyczy wszystkich podmiotów przetwarzających dane osobowe — niezależnie od charakteru działalności czy wielkości firmy. Możemy przypuszczać, że dopiero, gdy nagłośniony zostanie przypadek firmy, która musiała zapłacić karę za niedostosowanie się do nowego rozporządzenia, sprawi, że firmy faktycznie zainteresują się tematem i zaczną dbać o zgodność z przepisami.

Paweł Korzec, Regional Presales Manager, Eastern Europe w firmie VMware

Nieprzestrzeganie przepisów zawartych w GDPR może mieć duży wpływ na finanse — w obliczu niezgodności z nowym prawem na firmę może być nałożona grzywna wynosząca nawet do 4% rocznego obrotu. Jak się okazuje, wśród ogółu respondentów przeważa niski stopień wiedzy na temat możliwych kar za nieprzestrzeganie przepisów rozporządzenia — łącznie około dwie trzecie z nich nie wie, czy jakiekolwiek kary będą istnieć, bądź nie jest w stanie określić, jaki będzie ich wymiar. Jedynie 11% badanych wskazało prawidłowo, że będzie to kara do 4% rocznego obrotu przedsiębiorstwa. Co ważne, istotnie większym poziomem wiedzy w tym zakresie wykazali się pracownicy dużych firm zatrudniających powyżej 250 pracowników. Ponad połowa (58%) respondentów określiła karę 2% rocznego obrotu jako bardzo dotkliwą – podobną odpowiedź udzielili wszyscy badani bez względu na sektor oraz wielkość firmy. Nie dziwi zatem fakt, że prawie trzy czwarte firm (72%) postrzega grzywnę na wyższym poziomie za bardzo surową.

Poziom kar oraz potencjalny wpływ na funkcjonowanie firmy w obliczu przymusowego ujawnienia naruszenia danych osobowych uczynił z rozporządzenia GDPR problem na poziomie zarządu, a nie działu IT. W przeszłości to zespół informatyczny najczęściej był kojarzony z odpowiedzialnością za opracowanie i wdrożenie strategii dotyczącej cyberbezpieczeństwa. Niestety takie podejście budziło sprzeciw dyrekcji, dla której kwestie bezpieczeństwa generowały dodatkowe i niepotrzebne inwestycje. Obecnie, gdy świadomość odpowiedzialności jest większa, w interesie zarządu jest ochrona firmy, marki, a ostatecznie źródła dochodu i zabezpieczenie się przed wysokimi karami. Częściej też praktykuje się podejście „Security by Design".

Paweł Korzec, Regional Presales Manager, Eastern Europe w firmie VMware

Jeśli firma nie dostosuje się do nowego prawa, będzie zmuszona zapłacić ogromne kary. W odróżnieniu od poprzednich uregulowań prawnych tym organizacjom, które nie zastosowały odpowiednich zabezpieczeń lub nie zgłosiły naruszenia w momencie ich wystąpienia, grozić będzie grzywna w wysokości do 10 mln € lub 2% całkowitego obrotu rocznego. Jeśli natomiast przedsiębiorstwo będzie funkcjonować bez zgodności z niektórymi podstawowymi przepisami zawartymi w rozporządzeniu (na przykład uzyskanie niezbędnej zgody na przetwarzanie danych), grzywna może wzrosnąć do 4% całkowitego rocznego dochodu lub 20 mln €. Taka wysokość kar może być katastrofalna dla firm szczególnie z sektora MŚP.

Michał Jarski, Regional Director CEE w firmie Trend Micro

SANKCJE

Rozporządzenie GDPR przewiduje wielopoziomową strukturę kar za naruszenie obowiązujących przepisów. W przypadku niektórych uchybień organy ochrony danych mogą nakładać na przedsiębiorstwa kary finansowe w wysokości maksymalnie 4% rocznych obrotów w skali globalnej (dotyczy to na przykład niespełnienia wymogów w zakresie przesyłania danych za granicę bądź naruszenia podstawowych zasad przetwarzania, takich jak warunki wyrażenia zgody). Inne naruszenia wyszczególnione w rozporządzeniu są zagrożone karą wynoszącą maksymalnie 2% łącznych obrotów firmy.

Nadszedł czas, by działać! Jeśli organizacje chcą uniknąć kar, muszą wykorzystać nadchodzące miesiące, aby przygotować się do nowego rozporządzenia. Czasu jest niewiele, bo tylko niespełna dwa lata. Problem polega na tym, że nie wszystkie polskie przedsiębiorstwa są tego świadome. Jak wynika z badań, aż 67% firm nie wie, ile czasu pozostało na zastosowanie się do GDPR. Jedynie co trzeci respondent (33%) potrafił prawidłowo wskazać, ile czasu pozostało na przygotowanie firmy do zgodności z GDPR. Większą wiedzą w tym temacie wykazują się firmy z sektora usług, gdzie niemal połowa (49%) ma świadomość, że do wdrożenia nowej regulacji pozostało zaledwie półtora roku.

Problem może dotyczyć w szczególności małych firm, mikroprzedsiębiorstw oraz firm jednoosobowych. Nawet jeśli mają świadomość wejścia nowych przepisów, nie czują się zobligowane do ich przestrzegania, wychodząc z założenia, że nie są głównymi adresatami rozporządzenia. Co więcej, stanowi dla nich niemały problem to, ile czasu i kosztów pochłonęłoby wprowadzenie zgodności z GDPR.

Michał Jarski, Regional Director CEE w firmie Trend Micro

Osiemnaście miesięcy (jakie pozostają od ukazania się niniejszego raportu do wejścia w życie regulacji zapisanych w treści rozporządzenia GDPR) to czas, który organizacje powinny efektywnie wykorzystać. Pamiętać należy, że wdrożenie odpowiednich środków technicznych i organizacyjnych powinno być uzasadnione skrupulatną, a więc i czasochłonną analizą. Szczególnie w zakresie identyfikacji zagrożeń dla zinwentaryzowanych zasobów informatycznych. To nie jest trywialne zadanie. Wdrożone, szeroko rozumiane zabezpieczenia powinny zostać przetestowane jeszcze przed majem 2018 r.

Michał Grzybowski, dyrektor wykonawczy Fundacji Bezpieczna Cyberprzestrzeń

Świadomość czasu, jaki pozostał do zastosowania się do nowej regulacji, nie jest jedynym problemem — kluczowe jest również to, jakie kroki organizacje przedsiębiorstwa planują podjąć w celu zapewnienia zgodności z GDPR. Jeśli mowa o zrozumieniu wymagań nowej regulacji, to jak zwykle diabeł tkwi w szczegółach. Ponad połowa respondentów (61%) deklaruje, że zna warunki, jakie stawia przed organizacjami GDPR, jednak tylko 24% z nich zdaje sobie sprawę z potrzeby zatrudnienia Inspektora Ochrony Danych (odpowiednik dzisiejszego Administratora Bezpieczeństwa Informacji) w celu dostosowania się do nowych regulacji. Rodzi się pytanie, kto zatem będzie odpowiedzialny za zapewnienie zgodności z przepisami w pozostałych firmach.

INSPEKTORZY OCHRONY DANYCH

W określonych okolicznościach administrator danych lub podmiot przetwarzający dane ma obowiązek wyznaczyć (w ramach programu zgodności) Inspektora Ochrony Danych. Wymóg ten obowiązuje, jeśli (i) przetwarzania dokonuje organ publiczny, (ii) główna działalność administratora lub podmiotu przetwarzającego polega na przetwarzaniu, które ze względu na swój charakter, zakres lub cele wymaga regularnego i systematycznego monitorowania osób, których dane dotyczą, na dużą skalę bądź (iii) główna działalność danego podmiotu polega na przetwarzaniu na dużą skalę szczególnych kategorii danych.

Dwie trzecie przebadanych firm (67%) uważa, że odpowiedzialność za stosowanie się do rozporządzenia GDPR ponosi cała organizacja, a prawie jedna trzecia (31%) sądzi, że jest nią obarczony dyrektor generalny (CEO) lub zarząd firmy. Równocześnie ponad połowa respondentów (57%) nie odnotowała faktu zaangażowania zarządu firmy w przygotowania do wdrożenia GDPR. Mimo grożących kar finansowych i ogromnego ryzyka dla funkcjonowania firmy, brak świadomości sprawia, że osoby zarządzające nie angażują się póki co w przygotowania do wdrożenia nowego rozporządzenia. W tym miejscu warto również zwrócić uwagę na niezrozumienie przepisów mówiących o współpracy z podmiotami spoza Unii Europejskiej przetwarzającymi dane osobowe obywateli UE. Prawie żadna (96%) z przebadanych firm nie potrafiła wskazać, kto ponosi odpowiedzialność za naruszenie danych z Unii Europejskiej przetwarzanych przez usługodawcę spoza Unii Europejskiej np. z USA. Zdaniem 41% badanych odpowiedzialne są obie strony, przy czym zgodnie z obowiązującym prawem — jest to dostawca usługi, w tym przypadku z USA.

W przypadku firm publicznych oraz prywatnych, które przetwarzają dane osobowe na dużą skalę, niezbędne będzie zatrudnienie Inspektora Ochrony Danych. Osoba na tym stanowisku powinna posiadać rzetelną wiedzę na temat rozporządzenia, jak również posiadać doświadczenie w organizacji oraz klasyfikacji poszczególnych typów danych, oraz wiedzę, w jaki sposób firma przetwarza dane, gdzie je magazynuje, jak one zostały pozyskane oraz w jaki sposób i komu są udostępniane.

Michał Jarski, Regional Director CEE w firmie Trend Micro

Do obszaru ryzyk dla przedsiębiorstwa zaliczyć można również rozproszoną odpowiedzialność interpretowaną jako fakt, że 67% ankietowanych osób wskazała, że odpowiedzialność za GDPR ponosi organizacja jako całość. Takie podejście może skutkować minimalnym zaangażowaniem w sprawy bezpieczeństwa i wręcz nieprzykładaniem do niego wagi. Potencjalna kara dla grupy kapitałowej może się wydawać tak odległa i abstrakcyjna, że wręcz niewiarygodna. Stąd system szkolenia, praktykowania sytuacji awaryjnych wydaje się koniecznością.

Paweł Korzec, Regional Presales Manager, Eastern Europe w firmie VMware

Zgodnie z nowymi przepisami każda firma lub osoba, która przetwarza dane osobowe, będzie odpowiedzialna za ich skuteczną ochronę — dotyczy to w takim samym stopniu firm zewnętrznych, jak na przykład dostawców usług chmurowych. Mówiąc w wielkim uproszczeniu, każdy, kto ma dostęp do danych (niezależnie od lokalizacji), jest pociągnięty do odpowiedzialności w przypadku naruszenia bezpieczeństwa informacji.

Dla wielu firm zwiększenie inwestycji w bezpieczeństwo IT oraz szkolenie pracowników w zakresie ochrony danych są kluczowymi inicjatywami podejmowanymi w celu dostosowania się do GDPR:

Jakie kroki musi podjąć firma w celu wdrożenia zasad zawartych w GDPR?

Zwiększenie liczby szkoleń z zakresu ochrony danych	50%
Zwiększenie inwestycji w bezpieczeństwo IT	34%
Zatrudnienie Inspektora Ochrony Danych	24%
Zwiększenie wartości polisy ubezpieczeniowej na wypadek naruszenia danych	14%
Zatrudnienie firmy zewnętrznej w celu zapewnienia przestrzegania GDPR	6%
Nie rozumiemy, jakie kroki musimy podjąć w celu zapewnienia przestrzegania przepisów	5%
Nic, to nas nie dotyczy	2%
Inne	7%
Nic, nie musimy podejmować żadnych dodatkowych działań. Jesteśmy przekonani, że nie potrzebujemy żadnej dodatkowej ochrony	11%
Nie wiem	8%

Co ciekawe największa liczba badanych (39%) uważa, że ich firma nie ma większych problemów z przestrzeganiem przepisów o ochronie danych. Wśród tych, którzy wskazali konkretne problemy, najczęściej wymieniane były: brak formalnych procedur powiadamiania o naruszeniu (24%) oraz ograniczenia wynikające ze stosowanych systemów IT (20%). Wśród innych wyzwań wymieniono:

- Ograniczone zasoby na poprawę aktualnych procedur 19%
- Brak dostatecznej ochrony systemów informatycznych 17%
- Brak formalnych procedur umożliwiających jednoznaczną identyfikację lokalizacji i właściciela danych 16%
- Brak środków finansowych 15%
- Brak jednoznaczności co do tego, kto odpowiada za ten obszar 15%
- Brak skutecznej ochrony danych 15%

Brak większych problemów z przestrzeganiem przepisów istotnie częściej wskazywali pracownicy z sektora usług, zaś najczęściej konkretne problemy wymieniali badani zatrudnieni w przemyśle — szczególnie często wspominali oni o braku formalnych procedur w tym zakresie oraz niejednoznaczności kompetencji. Należy podkreślić, że skutki utraty informacji w każdym przypadku mogą być tak samo dotkliwe.

Zgodnie z rozporządzeniem GDPR osoby zajmujące się kontrolą i przetwarzaniem danych powinny wdrażać najnowocześniejsze zabezpieczenia stosownie do zagrożeń i charakteru danych osobowych, które mają być chronione. Okazuje się jednak, że organizacje nie zawsze potrafią jednoznacznie wskazać, co dokładnie kryje się pod hasłem „najnowocześniejsze”[2]. Prawie jedna piąta firm (19%) nie wie, czym są najnowocześniejsze zabezpieczenia. Natomiast połowa przebadanych (50%) uważa, że są to rozwiązania oferowane przez doświadczonych liderów na rynku. Warto podkreślić, że aż 22% respondentów wskazało, że koszt jest silniejszym czynnikiem korzystania z poszczególnych zabezpieczeń niż zapewnienie „najnowocześniejszej” ochrony. Natomiast 17% firm uważa, że decyzje o wdrożeniu konkretnych systemów zabezpieczających powinny być podejmowane na podstawie raportów niezależnych analityków z takich instytucji jak Gartner, Forrester, IDC etc.

Dokument GDPR jest sformułowany w sposób odmienny od obecnie obowiązujących przepisów. Zamiast nakazać organizacjom stosowanie konkretnego algorytmu szyfrowania lub kompleksowych rozwiązań, rozporządzenie GDPR skupia się na tym, w jaki sposób organizacje realizują własne interesy i jak przetwarzają informacje. Jest bardziej otwarte na interpretację, co sprawia, że jest również trudniejsze do wdrożenia. Jednocześnie świadczy to o bardziej strategicznym podejściu, które ma zachęcić firmy do tego, aby myślały o bezpieczeństwie w bardziej kompleksowy sposób.

Michał Jarski, Regional Director CEE w firmie Trend Micro

[2] Artykuł 32 GDPR wyraźnie wskazuje, że administrator i podmiot przetwarzający wdrażają odpowiednie środki techniczne, uwzględniając m.in. stan wiedzy technicznej. To ten „stan wiedzy technicznej” jest sformułowaniem na tyle ogólnym, że może wprowadzać w zakłopotanie przedsiębiorców co do prawidłowej interpretacji przepisu. Aktualny stan wiedzy technicznej należy czerpać przede wszystkim z ogólnie przyjętych praktyk i norm powszechnie uznawanych za standardy w zakresie bezpieczeństwa informacji. Są nimi np. normy ISO/IEC z serii 27000.

BRAK REAKCJI NA DONIESIENIA O ZAISTNIAŁYCH WYCIEKACH DANYCH

W 2016 roku miały miejsce wycieki danych osobowych z systemów bankowych, transportowych, firm energetycznych, a nawet rejestrów publicznych, który mogły dotyczyć nawet setek tysięcy Polaków. Skala oraz specyfika naruszeń powinna być przestrogą dla firm oraz zmusić je do przemyślenia tego, w jaki sposób podchodzą do kwestii związanych z cyberbezpieczeństwem. Informacje o wyciekach danych osobowych w innych firmach na ogół przyczyniają się do weryfikacji własnych strategii ochrony danych, jednak niewielki odsetek respondentów przyznał, że konsekwencją kontroli systemów zabezpieczających jest wdrożenie nowych rozwiązań, mających na celu usprawnienie obowiązujących systemów i procedur (16%). Kluczowymi inicjatywami w tym zakresie jest stosowanie szyfrowania (81%) oraz zwiększenie świadomości pracowników w zakresie ochrony danych (80%).

Inne kroki podejmowane w celu zwiększenia bezpieczeństwa to:

- Blokada sprzętu w celu uniknięcia użycia zainfekowanych nośników USB (66%)
- Wprowadzenie przejrzystych procesów, które pozwalają na identyfikację, lokalizację oraz zabezpieczenie danych (65%)
- Wprowadzenie technologii ochrony przed wyciekami (utratą) danych (57%)

Dzięki zastosowaniu odpowiednich technologii oraz wdrożeniu właściwych procesów, organizacje zaczynają proaktywnie działać na rzecz zapewnienia swoim klientom najwyższej ochrony. Martwić może jednak fakt, że ci ostatni nie są wciąż świadomi swoich praw w tym zakresie. Jak się okazuje, według opinii respondentów, w ponad połowie firm (54%) klienci nie domagają się transparentności w zakresie tego, jakie dane osobowe są przechowywane i gdzie.

Pomimo braku zainteresowania klientów względem sposobów przetwarzania danych osobowych, firmy czują się zobligowane do zapewnienia jak najlepszej ochrony. Większość respondentów uważa, że dane osobowe przechowywane w ich bazach są wystarczająco chronione przed wyciekami (75%), jednak największą pewnością zabezpieczeń charakteryzują się bardzo duże przedsiębiorstwa, zatrudniające powyżej 250 osób oraz firmy działające w sektorze usług (82%).

Aby zapobiec utracie danych klientów, firmy najczęściej stosują szyfrowanie (po 82% w sektorze przemysłu i handlu, 79% w sektorze usług). Równie często kładzie się nacisk na zwiększenie świadomości pracowników w zakresie ochrony danych (83% w przemyśle, 77% w usługach i 74% w handlu) oraz blokadę sprzętu w celu uniknięcia użycia zainfekowanych nośników USB (74% w handlu, 65% w usługach i 64% w przemyśle).

Rozporządzenie GDPR określa prawo konsumentów do bycia zapomnianym, które „odzwierciedla roszczenia osoby do zagwarantowania usunięcia informacji o niej umieszczonych w Internecie tak, by nie mogły być wyszukane przez osoby trzecie". Okazuje się, że wciąż istnieje dużo firm, które nie dysponują procesami czy technologiami zapewniającymi konsumentowi prawo do bycia zapomnianym.

	TAK %	NIE %
Zapewnienie klientom firmy prawa do bycia zapomnianym przez nią samą	**35%**	**50%**
Zapewnienie klientom firmy prawa do bycia zapomnianym przez firmy zewnętrzne	**18%**	**46%**
Zapewnienie klientom firmy prawa do bycia zapomnianym przez dostawców usług chmurowych, z którymi firma współpracuje	**16%**	**48%**
Zapewnienie klientom firmy prawa do bycia zapomnianym przez partnerów	**22%**	**46%**

Temat możliwości „bycia zapomnianym" jest niezwykle istotny. Powszechnie wiadomo, że trudno jest należycie usunąć informację z systemu informatycznego. Dodatkowy poziom komplikacji jest spowodowany możliwością przetwarzania danych w dowolnym miejscu, w tym w chmurze publicznej (o ile taka znajduje się na terytorium UE). Przedsiębiorstwa powinny dysponować narzędziami, które będą chronić bezpośrednio dane, a nie fizyczne serwery, a to wiąże się ze zmianą klasycznego modelu podejścia do przetwarzania informacji.

Paweł Korzec, Regional Presales Manager, Eastern Europe w firmie VMware

PRAWO DO USUNIĘCIA DANYCH (PRAWO DO BYCIA ZAPOMNIANYM)

W określonych przypadkach osoba fizyczna może zażądać od administratora danych niezwłocznego usunięcia jej danych osobowych. Dobrym przykładem jest sytuacja, w której osoba taka wycofuje zgodę na przetwarzanie danych, a nie istnieją już żadne inne podstawy prawne do ich przetwarzania

W ponad jednej czwartej firm istnieje procedura powiadamiania organu ochrony danych osobowych o naruszeniu (27%), istotnie częściej jest ona stosowana w firmach z sektora usługowego (37%) oraz w przedsiębiorstwach powyżej 250 pracowników (37%). Cieszy fakt, że prawie wszystkie firmy nie starają się unikać informowania klientów o zaistniałych incydentach (tylko 1% przyznało się do takiego postępowania), jednakże alarmujące jest to, że prawie w połowie przedsiębiorstw (42%) nie istnieje żadna formalna procedura w tym zakresie.

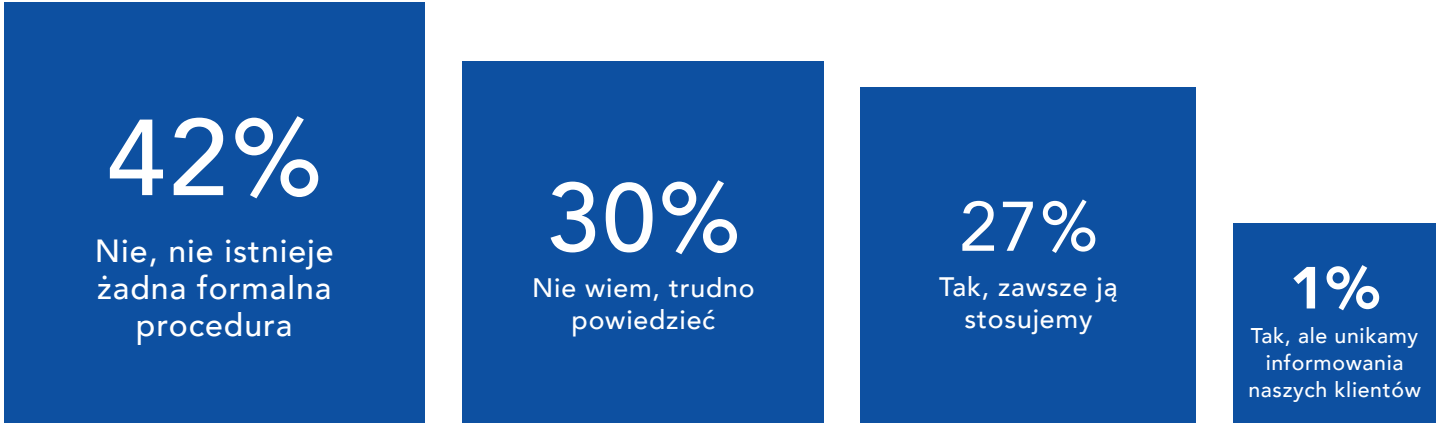
Organizacje bardzo często nie są świadome, że przetwarzane przez nie dane zostały naruszone już kilka miesięcy przed wykryciem zdarzenia. Co więcej, istnieje dość dużo udokumentowanych przypadków, gdzie klienci nie zdają sobie z tego sprawy nawet przez kilka lat! Najnowsze badania pokazują, że średni czas wykrycia naruszenia wzrósł o 50% w ciągu ostatnich 12-18 miesięcy, co oznacza, że mija około 200 - 300 dni, zanim ktokolwiek zda sobie sprawę, że doszło do przestępstwa. Ostatnio głośnym przypadkiem naruszenia danych było włamanie do brytyjskiego operatora telekomunikacyjnego TalkTalk, które, jak się później okazało, miało znacznie poważniejsze skutki, niż wydawało się podczas początkowego rozpoznania. Reputacja tej firmy bardzo poważnie ucierpiała. Dlatego też tak ważne jest, aby raportować wszelkie naruszenia danych w jak najkrótszym czasie, co z kolei jest niezwykle trudne i wymaga wyjątkowego przygotowania całej organizacji.

Michał Jarski, Regional Director CEE w firmie Trend Micro

POWIADAMIANIE O WYCIEKU DANYCH

Administratorzy mają obowiązek zgłaszać większość przypadków wycieku danych właściwym organom ochrony danych. Zgłoszenia należy dokonać bez zbędnej zwłoki, w miarę możliwości w ciągu **72 godzin** od momentu powzięcia wiadomości o wycieku, a w razie niedotrzymania powyższego terminu konieczne jest przedstawienie należytego uzasadnienia. W niektórych przypadkach administrator danych jest również zobowiązany do niezwłocznego powiadomienia o zaistniałej sytuacji zainteresowanych osób, których dane dotyczą.

Czy w firmie istnieje formalna procedura powiadamiania organu ochrony danych osobowych w ciągu 72 godzin od ich naruszenia?



[3] Verizon's 2016 Data Breach Investigations Report, http://www.verizonenterprise.com/verizon-insights-lab/dbir/2016/.

Największą obawę w zakresie bezpieczeństwa danych stanowi przypadkowa utrata danych przez pracowników. Uwzględniając podział na branże, szpiegostwo przemysłowe i wiążące się z nim bezprawne, pozyskiwanie tajemnic handlowych stanowi istotnie większy problem wśród firm działających w sektorze przemysłowym. Z kolei zagubienie lub utratę urządzeń wskazywano częściej w sektorze usług.

Co stanowi największe zagrożenie dla bezpieczeństwa danych firmy?

Przypadkowa utrata danych przez pracowników	56%
Cyberprzestępcy	52%
Kradzież danych przez pracowników	36%
Zgubione/utracone urządzenia	35%
Szpiegostwo przemysłowe	28%
Konkurencja	19%
Klienci	13%
Rząd	7%
Nie wiem	7%
Inne	1%

Najrzadziej wskazywanymi przez respondentów źródłami zagrożenia dla bezpieczeństwa danych byli klienci oraz rząd. Niewielki odsetek badanych — w granicach 7-8% (nie licząc sektora handlowego) — nie potrafił wskazać konkretnego elementu stanowiącego ryzyko w zakresie ochrony danych osobowych.

Człowiek staje się narzędziem w rękach przestępców, którzy szukają sposobów kradzieży informacji. Jako najsłabszy element z jego wszystkimi ułomnościami, wrażliwościami i podatnościami jest celem ataków. „Przypadkowa" utrata danych coraz częściej jest konsekwencją precyzyjnie zaplanowanego ataku na przedsiębiorstwo.

Paweł Korzec, Regional Presales Manager, Eastern Europe w firmie VMware

WNIOSKI

Czasu na dostosowanie się do wymogów nowego rozporządzenia jest coraz mniej. Jednocześnie nie ulega wątpliwości, że polskie firmy mają dużo do zrobienia, aby osiągnąć zgodność i uniknąć dotkliwych kar finansowych. Poziom wiedzy polskich przedsiębiorstw na temat rozporządzenia GDPR jest niezadowalający, organizacje muszą postarać się lepiej poznać terminy i wymagania określone nowymi przepisami. Jest to pierwszy niezbędny krok na drodze do zapewnienia należytej ochrony danych klientów. Większość przedsiębiorstw podlega już zresztą obowiązkom prawnym wynikającym z obecnego ustawodawstwa. Zakres wymagań, które firmy mogą i powinny spełnić w związku z ochroną danych, jest bardzo szeroki.

Ogólne rozporządzenie o ochronie danych może zburzyć dotychczasowe strategie ochrony danych, a proponowany system kar finansowych zmusi przedsiębiorstwa do przestrzegania obowiązujących przepisów. W związku z nieuchronnym wejściem w życie rozporządzenia zarysowuje się też jednak znacznie szerszy problem. Chociaż polskie firmy są coraz mocniej przekonane, że potrafią obronić się przed wyciekami danych, rzeczywista sytuacja w dziedzinie ochrony danych pozostawia wiele do życzenia. Wciąż istnieje część przedsiębiorstw nieprzestrzegających nawet obecnych przepisów o ochronie danych.

Najpopularniejszym dokumentem regulującym pracę firm w zakresie ochrony danych jest Ustawa o ochronie danych (88%). Jest ona wykorzystywana istotnie częściej w sektorze usług (95%). 45% przedsiębiorców deklaruje również zgodność z Dyrektywą UE dotyczącą ochrony danych osobowych. 27% bierze pod uwagę założenia wchodzącego prawa GDPR, natomiast 20% stosuje się również do zapisów Dyrektywy UE w zakresie cyberbezpieczeństwa. Martwi fakt, że wciąż istnieją firmy, które nie wiedzą, do jakich przepisów się stosować (6%).

Poruszanie się w gąszczu zawiłych przepisów jest dla wielu przedsiębiorstw dużym wyzwaniem, ale nie usprawiedliwia to bezczynności. Nadmierne zaufanie do posiadanych systemów bezpieczeństwa, brak świadomości zróżnicowanych zagrożeń czy pozornie odległy termin wejścia w życie rozporządzenia GDPR (2018 r.) sprawiają, że wiele firm odkłada na później zapewnienie zgodności z przepisami o ochronie danych. Wynikające z tego oszczędności są jednak pozorne.

Zachowanie zgodności z nowym prawem nie podlega dyskusji i to w interesie organizacji leży dołożenie wszelkich starań, aby ostrożnie i z rozmysłem zaplanować wszystkie kroki mające zapewnić pełne przestrzeganie zasad zawartych w rozporządzeniu. Szkolenia są tu nieodzowne.

Paweł Korzec, Regional Presales Manager, Eastern Europe w firmie VMware

Na zakończenie należy również wspomnieć o jeszcze jednej kwestii istotnej dla wszystkich firm. Przestrzeganie przepisów jest często tylko pierwszym krokiem na drodze do zapewnienia większego bezpieczeństwa danych. W związku z tym należy pamiętać, że osiągnięcie zgodności z przepisami nie powinno być celem samo w sobie, a jedynie krokiem na drodze do zapewnienia maksymalnego poziomu bezpieczeństwa.

Zgodność z przepisami jest obowiązkiem, jednak wszystkie firmy powinny dążyć do jak najwyższego poziomu bezpieczeństwa.

Michał Jarski, Regional Director CEE w firmie Trend Micro

TRZY NAJWAŻNIEJSZE SPOSOBY NA PRZYGOTOWANIE FIRMY DO GDPR

01 Lepsze poznanie swoich danych

Firma musi przede wszystkim posiadać świadomość ochrony krytycznych informacji. Ochrona wszystkich posiadanych danych jest zbyt droga, jak również zbyt uciążliwa. Regularnie opracowywana klasyfikacja informacji z zasadami, gdzie i w jaki sposób są one przechowywane, kto ma do nich dostęp oraz czy liczba osób mających taki dostęp powinna być ograniczona, powinna być procesem. Wiedza i wdrożenie należytych mechanizmów kontroli pozwoli zmniejszyć ryzyko wycieku danych, a w rezultacie obniżyć koszty ponoszone przez przedsiębiorstwo — także w związku z utratą reputacji marki.

02 Stworzenie planu powiadamiania o wyciekach danych

Należy opracować plan powiadamiania o wyciekach danych, który obejmie całą strukturę organizacyjną firmy. Umożliwi to sprawne i rzetelne informowanie o incydentach w sposób przynoszący firmie jak najmniejsze szkody. W realizację planu należy zaangażować zarówno dział informatyczny, jak i działy kadr, PR i marketingu oraz kadrę kierowniczą. Po wdrożeniu planu należy organizować próbne ćwiczenia pozwalające przećwiczyć jego zastosowanie.

03 Zainwestowanie we właściwe technologie pozwalające przeciwdziałać zagrożeniom wewnętrznym i zewnętrznym

Poważnym problemem jest wciąż nieuzasadnione zaufanie do technologii oraz procesów zakupionych i wdrożonych z myślą o przeciwdziałaniu zagrożeniom „starszego typu” — zarówno wewnętrznym, jak i zewnętrznym. Należy przeanalizować, czy rozwiązania techniczne kupione 5-10 lat temu będą skuteczne w walce z najnowszymi zagrożeniami. Wiele firm ma fałszywe poczucie bezpieczeństwa, które może nie wytrzymać konfrontacji z rzeczywistością.

Użytkownicy wewnętrzni. Pomimo najlepszych chęci pracownicy popełniają błędy, a niekiedy zdarzają się również osoby, które próbują umyślnie wykraść informacje należące do przedsiębiorstwa. W związku z tym firmy powinny zastanowić się nad zastosowaniem:

- mechanizmów ochrony danych (takich jak szyfrowanie), dzięki którym dane osobowe są bezpieczne nawet w przypadku utraty urządzenia, w którym są przechowywane;
- funkcji zdalnego wymazywania danych z urządzeń przenośnych;
- technologii zapobiegania utracie danych, które pozwalają kontrolować, jakiego rodzaju informacje są przesyłane w obrębie przedsiębiorstwa i poza nim.

Użytkownicy zewnętrzni. Dodatkowe mechanizmy kontroli zapobiegające wykorzystaniu zasobów firmy przez osoby z zewnątrz obejmują:

- blokady uniemożliwiające uruchamianie szkodliwego oprogramowania w punktach końcowych (zarówno narzędzia chroniące przed szkodliwym oprogramowaniem, jak i technologie kontroli aplikacji w punktach końcowych);
- szyfrowanie danych w urządzeniach przenośnych używanych poza siedzibą przedsiębiorstwa;
- poprawki wirtualne pozwalające zapobiec wykorzystaniu przez zdalnych użytkowników niezałatanych luk w zabezpieczeniach (a tym samym ograniczyć ryzyko związane z korzystaniem z systemów operacyjnych i aplikacji, w których nie zainstalowano wymaganych poprawek);
- rozwiązania do wykrywania włamań, które pozwalają wykryć naruszenie bezpieczeństwa sieci i podjąć właściwe działania, aby uniemożliwić osobom z zewnątrz kradzież cennych danych osobowych.

O BADANIU

Badanie zostało zrealizowane na przełomie września i października 2016 roku przez agencję badawczą ARC Rynek i Opinia wśród zajmujących się ochroną danych 151 przedstawicieli firm zatrudniających powyżej 100 pracowników oraz 51 przedstawicieli firm zatrudniających powyżej 250 pracowników. Zastosowano metodę CATI *(Computer Assisted Telephone Interview)*. Struktura próby jest reprezentatywna ze względu na proporcje sektorowe (przemysł/usługi/handel).

Szczegółowe informacje dostępne na stronie: www.trendmicro.pl oraz www.vmware.com/pl.

INFORMACJE O FIRMIE TREND MICRO

Trend Micro, światowy lider w dziedzinie zabezpieczeń cybernetycznych, nie ustaje w wysiłkach ukierunkowanych na zwiększenie bezpieczeństwa wymiany informacji cyfrowych. Nasze innowacyjne rozwiązania przeznaczone dla użytkowników indywidualnych, firm i instytucji administracji publicznej zapewniają wielowarstwową ochronę centrów przetwarzania danych, środowisk przetwarzania w chmurze, sieci i punktów końcowych. Wszystkie produkty Trend Micro współdziałają ze sobą i zapewniają bezproblemowy dostęp do informacji o zagrożeniach. Dzięki temu powstaje połączony system obrony ze scentralizowanymi funkcjami widoczności i kontroli, który pozwala na szybsze i skuteczniejsze zabezpieczenie systemów. Trend Micro zatrudnia ponad 5000 pracowników w przeszło 50 krajach i dysponuje najbardziej zaawansowanym na świecie globalnym systemem informacji o zagrożeniach, dzięki czemu umożliwia użytkownikom bezpieczne przejście na model przetwarzania w chmurze. Więcej informacji można uzyskać w serwisie www.trendmicro.com.

INFORMACJE O FIRMIE VMWARE

VMware (NYSE: VMW), światowy lider w dziedzinie infrastruktury chmury obliczeniowej i mobilności dla biznesu, ułatwia klientom cyfrową transformację ich przedsiębiorstw poprzez wprowadzanie do biznesu i IT rozwiązań definiowanych programowo. Dzięki stworzonej przez VMware architekturze One Cloud, Any Application, Any Device™ organizacje mogą w nieograniczony sposób zwiększać wykorzystanie mobilności, wyróżniać się na tle konkurencji i szybciej reagować na pojawiające się w biznesie szanse. Takie możliwości dają im nowoczesne aplikacje udostępniane z chmury hybrydowej oraz zaawansowane rozwiązania cyberbezpieczeństwa, chroniące ich markę i poziom zaufania klientów. W 2015 r. VMware zanotowała przychód 6,6 mld USD, obsługując 500 tys. klientów oraz współpracując z 75 tys. partnerów na całym świecie. Więcej informacji na stronie www.vmware.com/pl.


TREND
MICRO
vmware
FUNDACJA
bezpieczna
cyberprzestrzeń