Analiza ryzyka w obszarze bezpieczeństwa informacji

experto24.pl

Analiza ryzyka w obszarze bezpieczeństwa informacji

Spis treści

Wstęp

Każdy administrator danych, czyli podmiot, w którym znajdują się jakiekolwiek dane osobowe, powinien zastosować odpowiednie środki bezpieczeństwa, aby chronić je przed nieuprawnionym ujawnieniem. Środki te mają być odpowiednie, adekwatne do zagrożeń i wartości informacji.

Dane osobowe i inne chronione informacje są cennymi aktywami dla każdej organizacji, a na rynku wymierną, dużą wartością handlową. Dlatego warto opracować, wdrożyć i nadzorować szeroko rozumianą politykę bezpieczeństwa informacji. Trzeba to wykonać nie tylko przez wzgląd na obowiązki ustawowe, ale przede wszystkim z praktycznych względów dla ochrony danych.

Wypada jednak się zastanowić, jakie dane i w jaki sposób chronić w naszej organizacji. Jakie skuteczne środki bezpieczeństwa przedsięwziąć. Kto i za co ma odpowiadać. Co może się stać i jakie będą konsekwencje naruszenia przyjętych zasad ochrony danych. W tym celu analizujemy ryzyko w obszarze bezpieczeństwa informacji: określamy prawdopodobieństwo wystąpienia określonych zagrożeń, skutki ich ewentualnego wystąpienia oraz istotność dla analizowanego obszaru.

Jeśli taką analizę przeprowadzimy rzetelnie, to na podstawie wniosków z niej wypływających przygotujemy sensowną i praktyczną Politykę bezpieczeństwa i zastosujemy odpowiednie środki minimalizujące zagrożenia dla danych osobowych i innych cennych informacji.

Obowiązek wynikający z prawa

Obowiązek przeprowadzenia analizy ryzyka wynika również z różnych przepisów prawa. Już ustawa o ochronie danych osobowych w art. 36 ust. 1 mówi, że administrator danych jest obowiązany zastosować środki techniczne i organizacyjne zapewniające ochronę przetwarzanych danych osobowych odpowiednią do zagrożeń oraz kategorii danych objętych ochroną. W szczególności chodzi o zabezpieczenie danych przed ich udostępnieniem osobom nieupoważnionym, zabraniem przez osobę nieuprawnioną, przetwarzaniem z naruszeniem ustawy oraz zmianą, utratą, uszkodzeniem lub zniszczeniem.

Zwróćmy uwagę na zwrot „ochronę odpowiednią do zagrożeń oraz kategorii danych objętych ochroną". Wyraźnie odnosi się on do analizowania ryzyka w stosunku do określonych informacji i tym samym do stosowania odpowiednich środków bezpieczeństwa.

Z kolei określenie „odpowiednie" środki bezpieczeństwa oznacza takie, jakie powinny ochronić dane przed kradzieżą czy innym wyciekiem. Niektóre z tych środków są określone w przepisach wykonawczych i branżowych. W większości jednak przypadków to administrator danych decyduje, jakie środki, kiedy i gdzie zastosować i czy są w tym celu na przykład niezbędne metalowe szafy, czy wystarczą niemetalowe, czy blokować porty USB, czy nie.

To powinno wynikać z analizy ryzyka. Przypominam przy tej okazji o art. 36 ust. 2 uodo, który mówi, że administrator danych prowadzi dokumentację opisującą sposób przetwarzania danych oraz środki, o których mowa w ust. 1.

Przykład

Na dokumentację opisującą sposób przetwarzania danych i odpowiednie środki bezpieczeństwa składa się polityka bezpieczeństwa i instrukcja zarządzania systemem informatycznym służącym do przetwarzania danych osobowych. Aby taka dokumentacja spełniła swoje zadanie, a nie była jedynie krótkim i teoretycznym streszczeniem ustawy czy rozporządzeń, to powinna być oparta na rzeczywistej analizie ryzyka, a załączniki do niej powinny np. opisywać faktycznie podjęte środki bezpieczeństwa.

Innym aktem prawnym, jaki wprost nakazuje przeprowadzenie analizy ryzyka, jest rozporządzenie Rady Ministrów z 12 kwietnia 2012 r. w sprawie Krajowych Ram Interoperacyjności, minimalnych wymagań dla rejestrów publicznych i wymiany informacji w postaci elektronicznej oraz minimalnych wymagań dla systemów teleinformatycznych.

§ 20 ust. 1 tego rozporządzenia mówi, że podmiot realizujący zadania publiczne opracowuje i ustanawia, wdraża i eksploatuje, monitoruje i przegląda oraz utrzymuje i doskonali system zarządzania bezpieczeństwem informacji zapewniający poufność, dostępność i integralność informacji z uwzględnieniem takich atrybutów, jak autentyczność, rozliczalność, niezaprzeczalność i niezawodność.

W § 20 ust. 2 pkt 3 rozporządzenie mówi, że zarządzanie bezpieczeństwem informacji realizowane jest w szczególności przez (...) przeprowadzanie okresowych analiz ryzyka utraty integralności, dostępności lub poufności informacji oraz podejmowania działań minimalizujących to ryzyko, stosownie do wyników przeprowadzonej analizy. Pozostałe punkty tego paragrafu są wręcz zagadnieniami i zadaniami, które powinny być przedmiotem takiej analizy.

Czym jest ryzyko

Tymczasem musimy wiedzieć, że, jak mówi jedna z wielu definicji, ryzyko rozumiane jest jako kombinacja prawdopodobieństwa i skutku wystąpienia danego negatywnego zdarzenia. Ryzyko określane jest też często jako niepewność związana ze zdarzeniem lub działaniem, które wpłynie na zdolność realizacji celów, procesów czy zadań.

Dlatego w procesie zarządzania ryzykiem związanym z bezpieczeństwem informacji należy najpierw zidentyfikować zagrożenia dla przetwarzanych danych. Przez przetwarzanie danych rozumie się jakiekolwiek operacje wykonywane na danych osobowych, takie jak zbieranie, utrwalanie, przechowywanie, opracowywanie, zmienianie, udostępnianie i usuwanie, a zwłaszcza te, które wykonuje się w systemach informatycznych.

Obszary zagrożeń

Zagrożeń, zadań i obszarów do analizy może więc być wiele. Te określone w przepisach prawa i przede wszystkim te, za które odpowiada Administrator Bezpieczeństwa Informacji, to między innymi aktualizacja procedur i dokumentacji dotyczących ochrony danych. To również dbałość o to, aby osoby uczestniczące w procesie przetwarzania informacji posiadały odpowiednie upoważnienia, były przeszkolone i miały dostęp jedynie do tych danych, jakie są im niezbędne do wykonywania obowiązków służbowych.

Przykład

Aby wiedzieć co, gdzie i jak chronić, należy wykonać inwentaryzację sprzętu i oprogramowania służącego do przetwarzania informacji obejmującej ich rodzaj i konfigurację, a przede wszystkim prowadzić rejestr zbiorów danych.

Musimy zapewnić ochronę przetwarzanym informacjom przed ich kradzieżą, nieuprawnionym dostępem, uszkodzeniami lub zakłóceniami, przez monitorowanie dostępu do informacji. Powinniśmy więc wiedzieć, kto i kiedy logował się do systemu lub wchodził do pomieszczenia, w którym są przetwarzane dane.

Podejmujemy czynności zmierzające do wykrycia nieautoryzowanych działań związanych z przetwarzaniem informacji. Chodzi o to, czy np. nie jesteśmy atakowani złośliwym oprogramowaniem lub czy pracownik nie przesyła chronionych informacji na prywatny e-mail.

Zapewniamy środki uniemożliwiające nieautoryzowany dostęp na poziomie systemów operacyjnych, usług sieciowych i aplikacji. Należy więc ustanowić podstawowe zasady gwarantujące bezpieczną pracę przy przetwarzaniu mobilnym i pracy na odległość, zwłaszcza z wykorzystaniem przenośnych urządzeń komputerowych.

Zabezpieczamy informacje przed nieuprawnionym i nieautoryzowanym ujawnieniem, modyfikacją, usunięciem lub zniszczeniem, chociażby przez określanie grup uprawnień w systemie informatycznym i pełną w nim identyfikację i uwierzytelnianie użytkowników. Zagrożenia też może nieść współpraca z podmiotami zewnętrznymi, więc zawieramy w umowach serwisowych podpisanych ze stronami trzecimi zapisy gwarantujące odpowiedni poziom bezpieczeństwa informacji.

Sprawdzamy fizyczne środki bezpieczeństwa chroniące dane przed kradzieżą, czyli na przykład gospodarkę kluczami, system kontroli dostępu, alarm czy monitoring. Bardzo wiele zadań i zagrożeń wynika z użytkowania systemów teleinformatycznych. Te powinien identyfikować i nadzorować administrator systemu.

Identyfikacja ryzyka

Identyfikację ryzyka należy przeprowadzać nie rzadziej niż raz w roku. W przypadku istotnej zmiany warunków należy dokonać ponownej identyfikacji ryzyka. Zidentyfikowane rodzaje ryzyka należy poddać analizie mającej na celu określenie prawdopodobieństwa wystąpienia danego ryzyka i możliwych jego skutków.

Należy określić akceptowany poziom ryzyka. Jeśli więc np. w ciągu minionego roku nie doświadczyliśmy powodzi, pożaru czy włamania, to może prawdopodobieństwo wystąpienia takiego zagrożenia jest nieduże, ale jednak ewentualne skutki takiego zdarzenia mogą być katastrofalne.

Dlatego między innymi warto rozważyć możliwość bezpiecznego przechowywania zapasowych kopii bezpieczeństwa w zupełnie innej lokalizacji.

W stosunku do każdego istotnego ryzyka powinno się określić rodzaj reakcji (np.: akceptacja, przeniesienie, unikanie – wycofanie się, redukcja – ograniczanie). Należy określić działania, które trzeba podjąć w celu zmniejszenia danego ryzyka do akceptowalnego poziomu.

Przykład

Jeżeli ryzykiem jest wybuch niewypału znalezionego podczas prac przy drugiej linii metra, to musimy takowe zaakceptować, ale niech działaniem minimalizującym skutki będzie opracowanie odpowiedniego planu ewakuacji.

W stosunku do każdego istotnego ryzyka powinno się określić rodzaj reakcji. Zatem ryzyko możemy akceptować (tolerować), nie podejmując żadnych działań zaradczych.

Przy ochronie danych raczej nie można sobie pozwolić na taką reakcję. Można jednak się podzielić ryzykiem (przenieść je) – transfer ryzyka na inny podmiot, na przykład na firmę zewnętrzną, zwłaszcza taką, której powierzyliśmy przetwarzanie danych. Reakcją jest też unikanie (likwidacja ryzyka) – niepodejmowanie lub zaniechanie działań narażających na ryzyko.

Jednak większości zagrożeń związanych z przetwarzaniem danych nie unikniemy. Starajmy się więc je ograniczać (redukować) – podejmując działania zaradcze prowadzące do likwidacji lub ograniczania ryzyka do poziomu akceptowalnego.

Zarządzanie ryzykiem

W zarządzaniu ryzykiem bierze udział cały zespół, a konkretne zadania czy zagrożenia muszą być przypisane konkretnym osobom, tak zwanym właścicielom ryzyka. Do zadań właścicieli ryzyka należy w szczególności:

- identyfikacja i ocena rodzajów ryzyka związanych z realizacją przypisanych celów, zadań czy procesów,
- określenie reakcji w odniesieniu do poszczególnych rodzajów ryzyka,
- wdrażanie działań zaradczych w stosunku do zidentyfikowanych rodzajów ryzyka,
- gromadzenie, analiza i raportowanie informacji o incydentach.

Te formalne określenia wydają się skomplikowane, ale w praktyce chodzi o to, aby każdy wiedział, za co odpowiada, identyfikował zagrożenia i przekazywał uwagi.

Omówimy to na konkretnym przykładzie, analizując po kolei etapy i metodykę zarządzania ryzykiem, zaczynając od identyfikacji ryzyka, poprzez analizę ryzyka, czyli prawdopodobieństwo, wpływ, istotność. Ocenimy ryzyko, określimy mechanizmy kontroli, wdrożymy zabezpieczenia. Podejmiemy odpowiednie reakcje i monitoring.

Metodyka przeprowadzenia takiej analizy oraz skala ocen zagrożeń może być różna. Wskazane jest, aby była ona określona wcześniej i opisana w wewnętrznej procedurze zarządzania ryzykiem. Procedura taka jest bezwzględnie wymagana w jednostkach finansów publicznych i wynika z ustawy o finansach publicznych.

Dla naszego przykładu przyjmijmy, że analizujemy ryzyko w skali od 1 do 5, a obszarem będą zagrożenia związane z przetwarzaniem danych przy użyciu przenośnych urządzeń komputerowych.

Praktyczne zastosowanie

Jednym z zadań w obszarze bezpieczeństwa informacji jest zapewnienie bezpiecznej pracy mobilnej, na odległość, z wykorzystaniem laptopów i innych urządzeń przenośnych. Ryzyko i zagrożenia, jakie temu mogą towarzyszyć to np.. utrata urządzenia, wyciek danych, instalacja nieautoryzowanego oprogramowania, nieuprawnione operacje użytkownika.

Załóżmy, że prawdopodobieństwo wystąpienia takiego ryzyka jest na poziomie 3 (powinno to wynikać z wcześniejszych doświadczeń w danej organizacji). Natomiast skutki wystąpienia takich zagrożeń i wpływ na bezpieczeństwo informacji, jeśli doszłoby np. do kradzieży laptopa, będzie zapewne wysoki i określimy go na poziomie 5. Mnożąc prawdopodobieństwo i skutki wystąpienia (3 × 5), otrzymamy istotność ryzyka. W tym przypadku będzie ona wysoka (15) i trzeba będzie takie zagrożenia na bieżąco monitorować.

Określamy też reakcję na ryzyko, którą będzie tu podjęcie odpowiedniego działania ograniczającego ryzyko. W tym konkretnym przypadku może to być szyfrowanie danych, odebranie użytkownikom uprawnień administratora, stosowanie regulaminów korzystania ze sprzętu i oprogramowania, protokoły przekazania sprzętu.

Właścicielem ryzyka, czyli osobą odpowiadającą za wydanie odpowiednio zabezpieczonego laptopa i odebranie od użytkownika stosownych oświadczeń będzie zapewne informatyk – administrator systemu, ewentualnie kierownik ds. administracyjnych.

Przykład

Elementy analizy ryzyka powinny być dokumentowane, najlepiej w formie odpowiedniej tabeli. Do śledzenia istotności zagrożeń stosuje się tak zwaną mapę ryzyka.

Wszystko po to, aby zapewnić przetwarzanym danym poufność, czyli bezpieczeństwo – właściwość zapewniającą, że informacja nie jest udostępniana lub wyjawiana nieupoważnionym osobom.

Dane i system, w którym są przetwarzane, muszą mieć zapewnioną integralność, co znaczy, że nie mogą być narażone na nieautoryzowane i nieuprawnione zmiany, modyfikacje. Muszą być dostępne zawsze kiedy trzeba, ale tylko dla uprawnionego podmiotu, osoby. Musimy też zawsze wiedzieć, kto, kiedy, gdzie i co robił z określonymi informacjami, czyli zapewnić rozliczalność, niezaprzeczalność i niezawodność.

Rzetelnie przeprowadzona analiza ryzyka pozwoli przewidzieć i zminimalizować zagrożenia związane z przetwarzaniem danych. Takiej analizie poddajemy też inne obszary naszej działalności. Czasami nawet nie zdajemy sobie sprawy, że na bieżąco to robimy.

Sprzątaczka zauważając, że po umyciu podłogi jest ryzyko upadku i wypadku, a nie ma wystarczającej ilości ostrzegających tabliczek „uwaga ślisko” i zgłaszając to przełożonej, właśnie dokonała analizy ryzyka i podjęła odpowiednie działania.

Czy i jak dokumentujemy takie szacowanie to już kwestia wtórna, lecz pewne wytyczne np. dla jednostek sektora finansów publicznych zostały określone w komunikacie nr 23 ministra finansów z 16 grudnia 2009 r. w sprawie standardów kontroli zarządczej dla sektora finansów publicznych.

Nasza szeroko rozumiana polityka bezpieczeństwa informacji nie może być jedynie „pułkownikiem", czyli teoretycznym dokumentem zalegającym na półce. Powinien to być praktyczny zbiór procedur, instrukcji czy regulaminów, dzięki którym dane osobowe i inne cenne informacje będą skutecznie chronione.

Piotr Glen,
administrator bezpieczeństwa informacji, audytor SZBI wg PN-ISO/IEC 27001

Stopka redakcyjna

Redaktor:	Wioleta Szczygielska
ISBN:	978-83-269-4725-4
E-book nr:	2HH0417
Wydawnictwo:	Wydawnictwo Wiedza i Praktyka sp. z o.o.
Adres:	03-918 Warszawa, ul. Łotewska 9a
Kontakt:	Telefon 22 518 29 29, faks 22 617 60 10, e-mail: *cok@wip.pl*
NIP:	526-19-92-256
Numer KRS:	0000098264 – Sąd Rejonowy dla m.st. Warszawy, Sąd Gospodarczy XIII Wydział Gospodarczy Rejestrowy. Wysokość kapitału zakładowego: 200.000 zł