POLITECHNIKA WARSZAWSKA

Analiza ryzyka jako podstawa zabezpieczenia danych osobowych

Maciej Byczkowski

Janusz Zawiła-Niedźwiecki

Centrum Informatyzacji

II Konferencja „Zabezpieczenie danych osobowych”
„Nowa rola ABI – aspekty organizacyjne i techniczne”
Politechnika Warszawska 24.06.2015

Niniejszy referat omawia analizę ryzyka związanego z przechowywaniem i przetwarzaniem danych osobowych oraz niezbędnych procedur dotyczących ich zabezpieczania, przy uwzględnieniu krajowych i międzynarodowych przepisów dotyczących ochrony danych osobowych.

Autorzy zwracają uwagę również na to, że do realizacji wymagań wynikających z przepisów prawa można wykorzystać związane z zarządzaniem bezpieczeństwem informacji normy ISO.

Wskazują również na praktyczne aspekty i etapy postępowania dotyczące procesu analizy ryzyka przetwarzania danych osobowych w organizacjach.

W 2010 r. na forum PTE sformułowano pogląd, że współcześnie właściwie należałoby mówić o społeczeństwie ryzyka i dlatego obecne zarządzanie we wszystkich dziedzinach aktywności ludzkiej musi opierać się na panowaniu nad kwestią ryzyka.

Ryzyko tak znacząco wpływa na nasze życie, nie tylko dlatego, że wiemy o nim coraz więcej, ale zwłaszcza dlatego, że w ostatnich 20 latach trendy liberalizacji i globalizacji w gospodarce światowej oraz w sposobach funkcjonowania społecznego doprowadziły do nieznanego dotąd zintensyfikowania konkurencji rynkowej, postępu technicznego, wymiany informacji.

Wobec takiego wyzwania naturalną reakcją jest wszechstronne badanie tego zjawiska oraz poszukiwanie podejść, metod, technik jego rozpoznawania i ograniczania jego wpływu.

W ogólnym ujęciu ryzyko polega na możliwości niezrealizowania zamierzeń w wyniku zajścia zdarzeń, które nie zostały przewidziane albo na które nie ma się wpływu.

Brzmi to przede wszystkim złowrogo, ale należy wskazać też atrakcyjny aspekt ryzyka. Jest ono bowiem nie tylko zagrożeniem, lecz kryje się też za nim szansa na powodzenie szczególnie trudnych zamierzeń, co jest motorem postępu cywilizacyjnego ludzkości i rozwoju efektywnego biznesu.

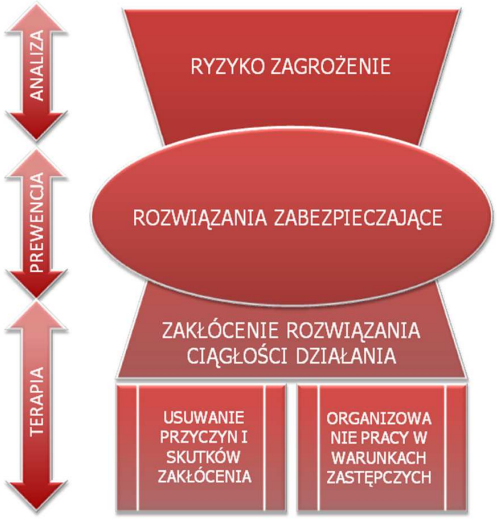
Zasadniczo ryzyko można podzielić na biznesowe (lub dla niektórych podmiotów ryzyko działalności statutowej), które jest kategorią rozpoznaną już dawno, oraz operacyjne, które wskazano pod koniec XX w.

Ryzyko biznesowe to możliwość poniesienia strat w wyniku niewłaściwych decyzji co do doboru klientów, kształtu produktów i usług lub zobowiązań wobec partnerów biznesowych albo w wyniku niesprawności lub niespójności systemu społeczno-gospodarczego państwa.

Ryzyko operacyjne to ryzyko strat w wyniku niewłaściwego lub błędnego działania procesu, ludzi i systemów albo wpływu wydarzeń zewnętrznych.

Właśnie ryzyko operacyjne, obejmujące także ryzyko niewypełniania obowiązków prawnych w działalności bieżącej, zostanie dalej omówione.

Triada: ryzyko – bezpieczeństwo – ciągłość działania



Całość działań panowania nad ryzykiem w sferze gospodarczej i administracyjnej nazywana jest zarządzaniem ryzykiem, a w sferze społecznej (funkcjonowania społeczności lokalnych lub całego kraju) zarządzaniem kryzysowym.

W obydwu przypadkach chodzi o poznanie istoty ryzyka i wyrażających je, w rozważanej lokalizacji i warunkach, konkretnych zagrożeń, podjęcie prewencji oraz przygotowanie gotowości do reagowania na zakłócenia.

Naruszenie bezpieczeństwa jest spełnieniem się potencjalnego dotąd ryzyka i zawsze polega na utracie jakichś kluczowych zasobów lub na utracie kontroli nad tymi zasobami.

W klasycznej działalności gospodarczej i klasycznych stosunkach społecznych, pomiędzy zakresem polegania na zapewnianiu bezpieczeństwa a zakresem polegania na planach reagowania, ustalana jest swoista równowaga wynikająca z ekonomicznej racjonalności wyboru między kosztami zabezpieczania a kosztami przewidywanych strat powstających w wyniku zajścia zakłóceń (z uwzględnieniem trudniej już policzalnych strat wizerunkowych związanych z zajściem zakłócenia).

Opracowując więc rozwiązania zapewniania bezpieczeństwa, bierze się pod uwagę rozwiązania zapewniania ciągłości działania i odwrotnie. Można nawet powiedzieć, że zabezpieczanie jako prewencja jest częścią zapewniania ciągłości działania, a ono z kolei jest zabezpieczeniem ostatniego poziomu.

Od takiej reguły racjonalności jedynym odstępstwem są obowiązki nakładane przepisami prawa.

Same w sobie nie zapewniają one pełnej skuteczności zabezpieczeń, ale w tym przypadku racjonalność polega tylko na statystycznie utrwalanej świadomości, że mimo zabezpieczeń jakiś procent zdarzeń zakłócających zajść musi. Wynika to i z prawa wielkich liczb, i świadomości zawodności materiałów, urządzeń czy technologii, i z ludzkiej niedoskonałości.

Nie są natomiast akceptowane ani niekompetencja (w tym nieznajomość prawa), ani błąd ludzki (w tym lekceważenie prawa), ani tym bardziej świadomie szkodliwe działanie.

Wymogi dotyczące przeprowadzania analizy ryzyka procesów przetwarzania danych osobowych są zawarte w przepisach ustawy o ochronie danych osobowych.

Chociaż nie występuje w przepisach sam termin „analiza ryzyka”, to z wymagań dotyczących zabezpieczenia danych osobowych określonych w art. 36 ust. 1 wynika obowiązek przeprowadzania takich działań.

Przepis ten wprost odnosi się do zagadnienia ryzyka operacyjnego, w ramach którego należy przeprowadzać analizę ryzyka, która obejmuje identyfikację i ocenę zagrożeń związanych z przetwarzaniem danych osobowych z podziałem na kategorie danych. Pod pojęciem kategorii danych należy rozumieć podział na tzw. dane osobowe „zwykłe” oraz dane osobowe „wrażliwe” wymienione w art. 27 ust. 1.

Celem tych działań jest poznanie istoty ryzyka i wyrażających je konkretnych zagrożeń, związanych z miejscem przetwarzania danych osobowych, systemami informatycznymi służącymi do przetwarzania danych oraz procesami ich przetwarzania, które są realizowane przez administratora danych lub procesora.

W treści art. 36 ust. 1 określone są szczególne sytuacje, które należy objąć analizą w celu zapewnienia bezpieczeństwa danych, minimalizacji ryzyka ich wystąpienia oraz przygotowania działań reagowania w sytuacji naruszenia bezpieczeństwa.

Wynikiem przeprowadzenia wymaganej analizy ryzyka jest zastosowanie przez administratora danych oraz procesora odpowiednich zabezpieczeń dla przetwarzanych danych osobowych oraz opracowanie odpowiedniej dokumentacji określającej właściwe stosowanie tych zabezpieczeń.

W rozporządzeniu MSWiA w sprawie dokumentacji przetwarzania danych osobowych oraz warunków technicznych i organizacyjnych, jakim powinny odpowiadać urządzenia i systemy informatyczne służące do przetwarzania danych osobowych – są określone:

a) podstawowe warunki techniczne i organizacyjne, jakim powinny odpowiadać urządzenia i systemy informatyczne służące do przetwarzania danych osobowych;

b) sposób prowadzenia i zakres dokumentacji opisującej sposób przetwarzania danych osobowych;

c) środki techniczne i organizacyjne zapewniające ochronę przetwarzanych danych odpowiednią do zagrożeń i kategorii danych objętych ochroną.

Wskazane w § 4 wymagania są podstawą do opracowania odpowiedniej dokumentacji „Polityki bezpieczeństwa” dla przetwarzanych danych osobowych, która powinna uwzględniać również zasady przeprowadzania okresowej analizy ryzyka przetwarzania danych. Aby móc zrealizować w praktyce ten wymóg, należy przeprowadzić analizę ryzyka przetwarzania danych w odniesieniu do wymienionych w § 4 pkt 5 atrybutów bezpieczeństwa informacji jakimi są: poufność, integralność i rozliczalność przetwarzania danych.

- **Wymogi dotyczące analizy ryzyka wynikające z przepisów dotyczących Krajowych Ram Interoperacyjności**
- **Planowane wymagania dotyczące zarządzania ryzykiem przetwarzania danych osobowych w projekcie Rozporządzenia PE i Rady UE**
- **Zarządzanie bezpieczeństwem danych osobowych z wykorzystaniem norm ISO serii 2700x**

Proces analizy ryzyka przetwarzania danych osobowych – podejście praktyczne:

- **identyfikacja zasobów danych osobowych, które będą podlegać ochronie oraz procesów ich przetwarzania przez ADO lub procesora**
- **określenie miejsc agregowania zidentyfikowanych zasobów danych osobowych**
- **rozpoznania procesów przetwarzania danych, które są realizowane przez danego ADO lub procesora**
- **identyfikacja zagrożeń oraz podatności na zagrożenia związane z przetwarzaniem danych osobowych**
- **sporządzenie „Mapy zagrożeń" związanych z przetwarzaniem danych**
- **identyfikacją podatności na zagrożenia w procesach przetwarzania danych osobowych**
- **plan postępowania z ryzykiem różnych rodzajów**

Referat jest oparty na

M.Byczkowski, J.Zawiła-Niedźwiecki, *Analiza ryzyka w zarządzaniu bezpieczeństwem danych osobowych*, Monitor Prawniczy 2014 (dodatek „Aktualne problemy prawnej ochrony danych osobowych")

Polecamy też:

M.Byczkowski, J.Zawiła-Niedźwiecki, *Information security aspect of operational risk management*, Foundations of Management nr 2/2009

F.Wołowski, J.Zawiła-Niedźwiecki, *Bezpieczeństwo systemów informacyjnych*, edu-Libri 2012

I.Staniec, J.Zawiła-Niedźwiecki, *Ryzyko operacyjne w naukach o zarządzaniu*, C.H.Beck 2015

Centrum Informatyzacji

dziękuję

maciej.byczkowski@ensi.net
j.zawila-niedzwiecki@wz.pw.edu.pl