METODYKA SZACOWANIA RYZYKA

Akademia WSB

R E K T O R
dr Zdzisława Dacko-Pikiewicz, prof. AWSB

AKADEMIA WSB
ul. Cieplaka 1c
41-300 Dąbrowa Górnicza
Tel. 32 262 28 05
-1-

Spis treści

R E K T O R
dr Zdzisława Dacko-Pikiewicz, prof. AWSB

AKADEMIA WSB
ul. Cieplaka 1c
41-300 Dąbrowa Górnicza
Tel. 32 262 28 05
-1-

WSTĘP

Przyjęta przez autora metodyka analizy ryzyka, została oparta o dwie normy ISO. ISO 31000 – system zarządzania ryzykiem oraz ISO 27005 – system zarządzania ryzykiem w bezpieczeństwie informacji. Normy te posłużyły jako podstawa opracowania, niemniej ustalenia wag i opisy zagrożeń powstały jako opracowanie samodzielne.

Pierwsza z w/w norm określa sposób oceny ryzyka w oparciu o kontekst organizacji, zarówno związane z kontekstem zewnętrznym, jak i wewnętrznych. Za najbardziej istotne konteksty mające realny wpływ dla Akademii WSB przyjęto kontekst prawny, regulacyjny, techniczny i społeczny.

Analizując zagrożenia związane z wejściem w życie Rozporządzenia *Parlamentu i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych – w dalszej części informacji RODO,* wzięto pod uwagę kary za naruszenia.

TABELA KAR ZGODNA Z RODO:

Artykuł RODO	**Maksymalna kara**
Art. 25 Naruszenie zasad ochrony danych osobowych w fazie projektowania (privacy by design) oraz domyślna ochrona danych (privacy by default)	10 milionów euro lub do 2% wartości rocznego światowego obrotu przedsiębiorstwa
Art. 29 Przetwarzanie z upoważnienia administratora lub podmiotu przetwarzającego	10 milionów euro lub do 2% wartości rocznego światowego obrotu przedsiębiorstwa
Art. 30 Rejestrowanie czynności przetwarzania	10 milionów euro lub do 2% wartości rocznego światowego obrotu przedsiębiorstwa
Art. 31 Współpraca z organem nadzorczym	10 milionów euro lub do 2% wartości rocznego światowego obrotu przedsiębiorstwa
Art. 32 Bezpieczeństwo przetwarzania	10 milionów euro lub do 2% wartości rocznego światowego obrotu przedsiębiorstwa

Art. 5 Naruszenie zasad dotyczących przetwarzania danych osobowych	20 milionów euro lub do 4% wartości rocznego światowego obrotu przedsiębiorstwa
Art. 7 Naruszenie warunków wyrażenia zgody na przetwarzanie danych	20 milionów euro lub do 4% wartości rocznego światowego obrotu przedsiębiorstwa
Art. 15 Naruszenie wykonania prawa dostępu przysługującego osobie, której dane dotyczą	20 milionów euro lub do 4% wartości rocznego światowego obrotu przedsiębiorstwa
Art. 16 Naruszenie wykonania prawa do sprostowania i usuwania danych	20 milionów euro lub do 4% wartości rocznego światowego obrotu przedsiębiorstwa

W związku z powyższymi kontekst prawny, wynikający z RODO oceniono na maksymalną, zaproponowaną wagę - 5). Należy pamiętać, że RODO nie jest jedyną podstawą prawną, za którą przewiduje sankcje finansowe. Przykładem takiej sankcji może być brak umowy powierzania przetwarzania danych (art. 28 RODO – w kontekście praw osób fizycznych w związku z art. 5, art. 7, art. 15, art. 16, art 29, art. 30) na obsługę kadrową, prawną, finansową lub informatyczną co skutkować będzie karą 10 milionów euro lub 2% obrotów brutto (liczy się wyższa kwota).

Niedopełnienie w/w obowiązku jest naruszeniem a może stać się czynem zabronionym kodyfikowanym nie tylko poprzez RODO ale również ustawę kodeks karny.

KONTEKST ORGANIZACJI

Propozycje wag dla poszczególnych kontekstów (propozycja autora opracowania), gdzie
Waga – 1 (bardzo niska)

Waga – 2 (niska)

Waga -3 (średnia)

Waga – 4 (wysoka)

Waga - 5 (bardzo wysoka)

- Kontekst prawny (np. podstawa prawna – przepisy karne) – WAGA 5
- Kontekst regulacyjny (np. kary umowne wynikające z kontraktu) – WAGA 4

- Kontekst techniczny/ IT (wymagania producenta – wymagania gwarancji) – WAGA 5
- Kontekst społeczny – np. zaangażowanie osób niepełnosprawnych) - WAGA 3
- Kontekst finansowy – np. kara za nieprzestrzeganie RODO - WAGA 5
- Kontekst walutowy - WAGA 5
- Kontekst konkurencyjny - WAGA 5

W opracowaniu przyjęto, że określane ryzyko jest weryfikowane poprzez kontekst a do obliczeń przyjęto sumę wag kontekstów biorących udział w konkretnej sytuacji.

ZAKRES WAG – od 1 do 32 punktów

ZASADA PID

W analizie ryzyka uwzględniono również wagę ryzyk i ich związek z opisywanymi w ISO i RODO atrybutami: poufnością, integralnością i dostępnością

Aby oszacować ryzyka zaproponowano 3 stopniową wagę dla każdego z atrybutów

POUFNOŚĆ

Mały wpływ - 1

Średni wpływ - 2

Duży wpływ - 3

INTEGRALNOŚĆ

Mały wpływ - 1

Średni wpływ - 2

Duży wpływ - 3

DOSTĘPNOŚĆ

Mały wpływ - 1

Średni wpływ - 2

Duży wpływ - 3

ZAKRES WAG – od 1 do 9 punktów

SKUTKI NARUSZEŃ DLA ATRYBUTÓW INFORMACJI

Aby realnie oszacować ryzyka uwzględniono możliwość związaną z naruszeniem jednego z atrybutów i dla każdego określono 5 stopniową skalę, gdzie:

POUFNOŚĆ

Nieznaczny – 1

Niski – 2

Średni – 3

Wysoki – 4

Katastrofalny – 5

INTEGRALNOŚĆ

Nieznaczny – 1

Niski – 2

Średni – 3

Wysoki – 4

Katastrofalny – 5

DOSTĘPNOŚĆ

Nieznaczny – 1

Niski – 2

Średni – 3

Wysoki – 4

Katastrofalny – 5

ZAKRES WAG – od 1 do 75 punktów

WPŁYW NARUSZEŃ NA ORGANIZACJĘ

Dodatkowo zaproponowano wagi dla poszczególnych rodzajów naruszeń i ich związków z organizacją i jej prestiżem a także ciągłością działania oraz karami finansowymi.

Dla każdego z obszarów:

- skutki finansowe naruszenia

- skutki na ciągłość działania

- skutki na prestiż organizacji

zaproponowano określenie ewentualnych skutków i prawdopodobieństwo ich wystąpienia:

SKUTEK NARUSZEŃ NA FINANSE ORGANIZACJI:

- Nieznaczny – 1 (strata finansowa poniżej ..... zł)
- Niski – 2 (strata finansowa pomiędzy ..... zł a ..... zł)
- Średni – 3 (strata finansowa pomiędzy ..... zł a ..... zł)
- Poważny – 4 (strata finansowa pomiędzy ..... zł a ..... zł)
- Katastrofalny – 5 (strata finansowa powyżej ..... zł)

PRAWDOPODOBIEŃSTWO WYSTĄPIENIA

- Rzadkie – 1 (prawie się nie zdarza – nie odnotowano incydentów)
- Mało prawdopodobne – 2 (zdarzyło się w Polsce)
- Średnie – 3 (zdarzyło się w branży)
- Prawdopodobne – 4 (może zdarzyć się w kwartale – odnotowano jeden incydent)
- Pewne – 5 (zdarzy się przynajmniej raz w miesiącu – wielokrotne incydenty)

ZAKRES WAG – od 1 do 25 punktów

SKUTEK NARUSZEŃ NA CIĄGŁOŚĆ DZIAŁANIA DLA ORGANIZACJI:

1. Nieznaczny – 1 (krótkotrwałe zakłócenia w pracy organizacji,)
2. Niski – 2 (zakłócenie w pracy organizacji nie mające wpływu na działania innych organizacji)
3. Średni – 3 (zakłócenie w pracy organizacji mogące mieć wpływ na działania innych organizacji)
4. Poważny – 4 (brak możliwości realizacji celu strategicznego uczelni oraz działania przez długi okres czasu)
5. Katastrofalny – 5 (brak możliwości kontynuacji ciągłości działania uczelni)

PRAWDOPODOBIEŃSTWO WYSTĄPIENIA

1. Rzadkie – 1 (prawie się nie zdarza – nie odnotowano)
2. Mało prawdopodobne – 2 (zdarzyło się w Polsce)
3. Średnie – 3 (zdarzyło się w branży)
4. Prawdopodobne – 4 (może zdarzyć się w kwartale – odnotowano naruszenie lub incydent)
5. Pewne – 5 (zdarzy się prawie na pewno)

ZAKRES WAG – od 1 do 25 punktów

SKUTEK NARUSZEŃ NA WIZERUNEK ORGANIZACJI:

1. Nieznaczny – 1 (plotki nie będące informacjami)
2. Niski – 2 (informacje nie mające znaczenia dla działania uczelni)
3. Średni – 3 (doniesienia regionalne lub branżowe mogące mieć wpływ na działanie uczelni)
4. Poważny – 4 (doniesienia ogólnokrajowe mogące mieć wpływ na działanie uczelni
5. Katastrofalny – 5 (doniesienia ogólnokrajowe mogące mieć wpływ na działania uczelni)

PRAWDOPODOBIEŃSTWO WYSTĄPIENIA

1. Rzadkie – 1 (prawie się nie zdarza)
2. Mało prawdopodobne – 2 (zdarzyło się w Polsce)

3. Średnie – 3 (zdarzyło się w branży)
4. Prawdopodobne – 4 (może zdarzyć się w kwartale – odnotowano jeden incydent)
5. Pewne – 5 (zdarzy się prawie na pewno)

ZAKRES WAG – od 1 do 25 punktów

Z obszarów i ich wag tworzy się iloczyn z zakresem wag od 1 do 75

ZABEZPIECZENIA

Po obliczeniu ryzyk zgodnie z przyjętą i wyżej opisaną metodyką, określono dotychczas stosowane zabezpieczenia nadając im odpowiednie wagi. Miało to na celu zrealizowanie postulatu art. 32 RODO, gdzie określono proponowane zabezpieczenia:

a. pseudonimizację i szyfrowanie danych osobowych;

b. zarządzanie systemem w sposób zapewniający ciągłość poufności, integralności i dostępności przetwarzanych informacji;

c. zarządzanie systemem w sposób zapewniający zdolność do szybkiego przywrócenia dostępu do danych osobowych w razie wystąpienia incydentu fizycznego lub technicznego;

d. regularne testowanie, mierzenie i ocenianie skuteczności środków technicznych i organizacyjnych mających zapewnić bezpieczeństwo przetwarzania.

W określeniu zabezpieczeń wykorzystano ankiety, bezpośrednie audyty bezpieczeństwa, wywiady i wizje lokalne prowadzone w uczelni oraz doświadczenie audytorów.

Poniżej przedstawiono propozycję obliczeń dla zabezpieczeń.

W obszarze kontekstów określono wagi zabezpieczeń, jako procentowy w obszarze 1 do 5, gdzie:

Brak zabezpieczeń - Waga 1 (0,2 wymaganego zabezpieczenia)

Słabe zabezpieczenia - Waga 2 (0,4 wymaganego zabezpieczenia)

Średnie zabezpieczenia - Waga 3 (0,6 wymaganego zabezpieczenia)

Dobre zabezpieczenia - Waga 4 (0,8 wymaganego zabezpieczenia)

Adekwatne zabezpieczenia - Waga 5 (1 wymaganego zabezpieczenia)

Ochrona przed naruszeniami dla PID

POUFNOŚĆ

Brak zabezpieczeń – 1 (0,2 - oczekiwanego zabezpieczenia)

Słabe zabezpieczenia – 2 (0,4 - oczekiwanego zabezpieczenia)

Średnie zabezpieczenia – 3 (0,6 - oczekiwanego zabezpieczenia)

Dobre zabezpieczenia – 4(0,8 oczekiwanego zabezpieczenia)

Bardzo dobre zabezpieczenia – 5(1 oczekiwanego zabezpieczenia)

INTEGRALNOŚĆ

Brak zabezpieczeń – 1 (0,2 - oczekiwanego zabezpieczenia)

Słabe zabezpieczenia – 2 (0,4 - oczekiwanego zabezpieczenia)

Średnie zabezpieczenia – 3 (0,6 - oczekiwanego zabezpieczenia)

Dobre zabezpieczenia – 4(0,8 oczekiwanego zabezpieczenia)

Bardzo dobre zabezpieczenia – 5(1 oczekiwanego zabezpieczenia)

DOSTĘPNOŚĆ

Brak zabezpieczeń – 1 (0,2 - oczekiwanego zabezpieczenia)

Słabe zabezpieczenia – 2 (0,4 - oczekiwanego zabezpieczenia)

Średnie zabezpieczenia – 3 (0,6 - oczekiwanego zabezpieczenia)

Dobre zabezpieczenia – 4(0,8 oczekiwanego zabezpieczenia)

Bardzo dobre zabezpieczenia – 5(1 oczekiwanego zabezpieczenia)

Określono również zabezpieczenia **w kontekście ich wpływu na finanse, ciągłość, działania i wizerunek uczelni**., gdzie dla:

Skutku finansowego przyjęto następujące wagi:

Brak zabezpieczeń – 1 (0,2 - oczekiwanego zabezpieczenia)

Słabe zabezpieczenia – 2 (0,4 - oczekiwanego zabezpieczenia)

Średnie zabezpieczenia – 3 (0,6 - oczekiwanego zabezpieczenia)

Dobre zabezpieczenia – 4(0,8 oczekiwanego zabezpieczenia)

Bardzo dobre zabezpieczenia – 5(1 oczekiwanego zabezpieczenia)

Ciągłości działania przyjęto następujące wagi:

Brak zabezpieczeń – 1 (0,2 - oczekiwanego zabezpieczenia)

Słabe zabezpieczenia – 2 (0,4 - oczekiwanego zabezpieczenia)

Średnie zabezpieczenia – 3 (0,6 - oczekiwanego zabezpieczenia)

Dobre zabezpieczenia – 4(0,8 oczekiwanego zabezpieczenia)

Bardzo dobre zabezpieczenia – 5(1 oczekiwanego zabezpieczenia)

Wizerunku przyjęto następujące wagi:

Brak zabezpieczeń – 1 (0,2 - oczekiwanego zabezpieczenia)

Słabe zabezpieczenia – 2 (0,4 - oczekiwanego zabezpieczenia)

Średnie zabezpieczenia – 3 (0,6 - oczekiwanego zabezpieczenia)

Dobre zabezpieczenia – 4(0,8 oczekiwanego zabezpieczenia)

Bardzo dobre zabezpieczenia – 5(1 oczekiwanego zabezpieczenia)

UWAGI KOŃCOWE

Różnica pomiędzy oszacowanymi ryzykami a zabezpieczeniami stanowią tzw. ryzyko szczątkowe lub rezydualne, czyli ryzyko pozostałe, które należy dobezpieczyć. Formą może być wdrożenie polityk, podpisanie stosowanych umów, zakup dodatkowego sprzętu, ubezpieczenie od następstw, etc.

Warto pamiętać, że istotnym elementem codziennej analizy ryzyka powinno być zarządzanie incydentami i naruszeniami .Każdy bowiem incydent i naruszenie może doprowadzić do czynu zabronionego co pomimo wdrożonych technicznych i organizacyjnych zabezpieczeń.