Opracował Adam Masiak

Podejście oparte na ryzyku

Czyli jak określić odpowiednie techniczne środki ochrony danych w systemie informatycznym?

Agenda

- Czym jest podejście oparte na ryzyku i jakie elementy powinno obejmować?
- Jaką metodykę wybrać? – przegląd wybranych standardów analizy ryzyka.
- Analiza ryzyka w procesie projektowania systemu – na którym etapie opracować wymagania?
- Dokumentacja wymagań i inwentaryzacja technicznych i organizacyjnych środków ochrony.

Definicja

- Podejście oparte na ryzyku to zasada polegająca na uzależnieniu sposobu wypełnienia obowiązków ciążących na podmiocie będącym administratorem danych od charakteru, zakresu i celu przetwarzania, wpływu na podmiot danych i jego uprawnienia oraz zagrożenia atrybutów charakterystycznych dla zasobu informacyjnego i poddaniu tych czynników cyklicznej ocenie.

Artykuł 32

Bezpieczeństwo przetwarzania

1. Uwzględniając stan wiedzy technicznej, koszt wdrażania oraz charakter, zakres, kontekst i cele przetwarzania oraz ryzyko naruszenia praw lub wolności osób fizycznych o różnym prawdopodobieństwie wystąpienia i wadze zagrożenia, administrator i podmiot przetwarzający wdrażają odpowiednie środki techniczne i organizacyjne, aby zapewnić stopień bezpieczeństwa odpowiadający temu ryzyku, w tym między innymi w stosownym przypadku:

a) pseudonimizację i szyfrowanie danych osobowych;

b) zdolność do ciągłego zapewnienia poufności, integralności, dostępności i odporności systemów i usług przetwarzania;

c) zdolność do szybkiego przywrócenia dostępności danych osobowych i dostępu do nich w razie incydentu fizycznego lub technicznego;

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

Źródło: Rys.1 Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation), dostęp: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A32016R0679

Podejście oparte na ryzyku w RODO

- Bezpieczeństwo przetwarzania – art. 32 ust. 1 RODO
  - Stan wiedzy technicznej
  - Koszt wdrożenia zabezpieczeń
  - Charakter, zakres, kontekst i cele przetwarzania
  - Naruszenie praw lub wolności osób fizycznych
  - Prawdopodobieństwo i waga wystąpienia

Kontekst organizacyjny

Kontekst osoby fizycznej

Element systematycznej oceny

Podejście oparte na ryzyku

- Uwzględnienie odpowiednich rodzajów zagrożeń – art. 32 ust. 2 RODO:
  - Przypadkowego lub niezgodnego z prawem zniszczenia danych – utrata atrybutu dostępności
  - Nieuprawnionego ujawnienia lub dostępu do danych osobowych – utrata atrybutu poufności
  - Modyfikacji treści danych – utrata atrybutu integralności

Wybór metodyki szacowania ryzyka

ISO/IEC 27005:2014 Information security risk management

NIST SP 800-30 Guide for conducting risk assesment

ISO/IEC 31000:2009 Risk management – Principles guidelines

CIA triad

Identyfikowanie i wartościowanie aktywów

Przykładowe typy zagrożeń

Listy kontrole i listy podatności

Kontekst osoby fizycznej

Ocena wpływu na prawa i wolności

Określenie skali wpływu na jednostkę

Metodyka

Wykorzystanie list kontrolnych

TABLE D-1: INPUTS – THREAT SOURCE IDENTIFICATION

Description	Provi	
	Tier 1	Ti

From Tier 1: (Organization level)
- Sources of threat information deemed to be credible (e.g., open source and/or classified threat reports, previous risk/threat assessments). (**Section 3.1, Task 1-4**)
- Threat source information and guidance specific to Tier 1 (e.g., threats related to organizational governance, core missions/business functions, management/operational policies, procedures, and structures, external mission/business relationships).
- Taxonomy of threat sources, annotated by the organization, if necessary. (**Table D-2**)
- Characterization of adversarial and non-adversarial threat sources.
  - Assessment scales for assessing adversary capability, intent, and targeting, annotated by the organization, if necessary. (**Table D-3, Table D-4, Table D-5**)
  - Assessment scale for assessing the range of effects, annotated by the organization, if necessary. (**Table D-6**)
- Threat sources identified in previous risk assessments, if appropriate.
	No	

From Tier 2: (Mission/business process level) - Threat source information and guidance specific to Tier 2 (e.g., threats related to mission/business processes, EA segments, common infrastructure, support services, common controls, and external dependencies). - Mission/business process-specific characterization of adversarial and non-adversarial threat sources.	Yes *via RAR*	
From Tier 3: (Information system level) - Threat source information and guidance specific to Tier 3 (e.g., threats related to information systems, information technologies, information system components, applications, networks, environments of operation). - Information system-specific characterization of adversarial and non-adversarial threat sources.	Yes *via RAR*	

Źródło: Rys.1 NIST SP 800-30 Guide for conducting risk assesment, appendix D, p. D-1

Rodzaj	Zagrożenie	Źródło
Zniszczenia fizyczne	Pożar	P, U, N
	Zalanie	P, U, N
	Zanieczyszczenie	P, U, N
	Poważny wypadek	P, U, N
	Zniszczenie urządzeń lub nośników	P, U, N
	Pył, korozja, wychłodzenie	P, U, N
Zjawiska naturalne	Zjawiska klimatyczne	
	Zjawiska sejsmiczne	
	Zjawiska wulkaniczne	
	Zjawiska pogodowe	
	Powódź	
Utrata podstawowych usług	Awaria systemu klimatyzacji lub dostaw wody[N5)]	
	Utrata dostaw prądu	
	Awaria urządzenia telekomunikacyjnego	
Zakłócenia spowodowane promieniowaniem	Promieniowanie elektromagnetyczne	
	Promieniowanie cieplne	
	Impuls elektromagnetyczny	
Naruszenie bezpieczeństwa informacji	Przechwycenie sygnałów na skutek zjawiska interferencji	
	Szpiegostwo zdalne	
	Podsłuch	
	Kradzież nośników lub dokumentów	
	Kradzież urządzenia	
	Odtworzenie z powtórnie wykorzystanych lub wyrzuconyc	
	Ujawnienie	
	Dane z niewiarygodnych źródeł	
	Manipulowanie urządzeniem	
	Sfałszowanie oprogramowania	
	Detekcja umiejscowienia	

Źródło: Rys.2 ISO/IEC 27005:2014 Information security risk management, appendix D, p. 54

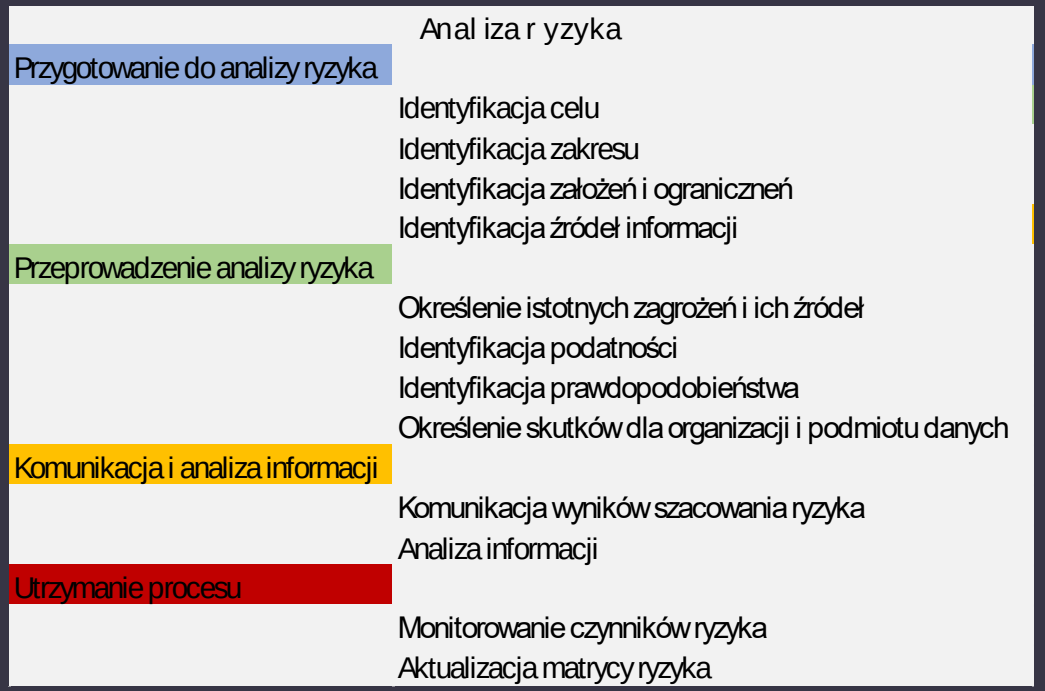
Źródło: Rys.3 NIST SP 800-30 Guide for conducting risk assesment, appendix E, p. E-1

TABLE E-1: INPUTS – THREAT EVENT IDENTIFICATION

Description	Provided To		
	Tier 1	Tier 2	Tier 3
From Tier 1: (Organization level) - Sources of threat information deemed to be credible (e.g., open source and/or classified threat reports, previous risk/threat assessments. (**Section 3.1, Task 1-4**.) - Threat event information and guidance specific to Tier 1 (e.g., threats related to organizational governance, core missions/business functions, external mission/business relationships, management/operational policies, procedures, and structures). - Exemplary adversarial threat events, annotated by the organization, if necessary. (**Table E-2**) - Exemplary non-adversarial threat events, annotated by the organization, if necessary. (**Table E-3**) - Assessment scale for assessing the relevance of threat events, annotated by the organization, if necessary. (**Table E-4**) - Threat events identified in previous risk assessments, if appropriate.	No	Yes	Yes *If not provided by Tier 2*
From Tier 2: (Mission/business process level) - Threat event information and guidance specific to Tier 2 (e.g., threats related to mission/business processes, EA segments, common infrastructure, support services, common controls, and external dependencies). - Mission/business process-specific characterization of adversarial and non-adversarial threat events.	Yes *Via RAR*	Yes *Via Peer Sharing*	Yes
From Tier 3: (Information system level) - Threat event information and guidance specific to Tier 3 (e.g., threats related to information systems, information technologies, information system components, applications, networks, environments of operation). - Information system-specific characterization of adversarial and non-adversarial threat events. - Incident reports.	Yes *Via RAR*	Yes *Via RAR*	Yes *Via Peer Sharing*

Analiza ryzyka w procesie projektowania

- Przygotowanie do analizy ryzyka – ustalenie wymagań i warunków brzegowych
- Przeprowadzenie analizy ryzyka – zasilenie opracowanego modelu danymi
- Komunikacja i analiza informacji – krytyczna ocena wyników analizy oraz przygotowanie planów postępowania
- Rozwój i utrzymanie – zapewnienie ciągłości procesu dla rozwijanych systemów



Analiza ryzyka w procesie projektowania

	Analiza ryzyka	Projektowanie w modelu kaskadowym	Projektowanie w modelu spiralnym	Projektowanie w modelu zwinnym
Przygotowanie do analizy ryzyka		Planowanie systemu	Planowanie	Ustalenie celów
	Identyfikacja celu	Analiza systemu	Projektowanie	Rozpoznanie i redukcja zagrożeń
	Identyfikacja zakresu	Projekt systemu	Programowanie	Tworzenie i zatwierdzanie
	Identyfikacja założeń i ograniczneń	Implementacja	Testowanie	Ocena i planowanie
	Identyfikacja źródeł informacji	Testowanie	Implementacja	
		Wdrożenie	Informacja zwrotna	

	Analiza ryzyka	Projektowanie w modelu kaskadowym	Projektowanie w modelu spiralnym	Projektowanie w modelu zwinnym
Przeprowadzenie analizy ryzyka		Planowanie systemu	Planowanie	Ustalenie celów
	Określenie istotnych zagrożeń i ich źródeł	Analiza systemu	Projektowanie	Rozpoznanie i redukcja zagrożeń
	Identyfikacja podatności	Projekt systemu	Programowanie	Tworzenie i zatwierdzanie
	Identyfikacja prawdopodobieństwa	Implementacja	Testowanie	Ocena i planowanie
	Określenie skutków dla organizacji i podmiotu danych	Testowanie	Implementacja	
		Wdrożenie	Informacja zwrotna	

	Analiza ryzyka	Projektowanie w modelu kaskadowym	Projektowanie w modelu spiralnym	Projektowanie w modelu zwinnym
Komunikacja i analiza informacji		Planowanie systemu	Planowanie	Ustalenie celów
	Komunikacja wyników szacowania ryzyka	Analiza systemu	Projektowanie	Rozpoznanie i redukcja zagrożeń
	Analiza informacji	Projekt systemu	Programowanie	Tworzenie i zatwierdzanie
		Implementacja	Testowanie	Ocena i planowanie
		Testowanie	Implementacja	
		Wdrożenie	Informacja zwrotna	

Dziękuję za uwagę.
Pytania?