BEZPIECZEŃSTWO SYSTEMÓW KOMPUTEROWYCH

Wykład 4

Plan wykładu

4. Zarządzanie bezpieczeństwem systemów (wybrane zagadnienia)
   1. Zasady zarządzania bezpieczeństwem systemów
   2. Zarządzanie bezpieczeństwem systemów w kontekście ograniczeń występujących przy jego realizacji
   3. Zarządzanie bezpieczeństwem systemów – koszty czy zyski
      1. Poziom osiągniętego bezpieczeństwa a wydatki
      2. Struktura wydatków na bezpieczeństwo systemów
      3. Czy wydatki na bezpieczeństwo systemów się zwracają?
   4. Analiza stanu bezpieczeństwa systemów w świetle badań

4. Zarządzanie bezpieczeństwem systemów (wybrane zagadnienia)

Zarządzanie bezpieczeństwem systemów to bardzo rozległy temat. Na dzisiejszym wykładzie zostaną poruszone cztery zagadnienia uznane przeze mnie za podstawowe:

- Zasady zarządzania bezpieczeństwem systemów
- Zarządzanie bezpieczeństwem systemów w kontekście występujących ograniczeń przy jego realizacji
- Zarządzanie bezpieczeństwem systemów – koszty czy zyski
- Analiza stanu bezpieczeństwa systemów

4.1.1 Zasady zarządzania bezpieczeństwem systemów…

związane z użytkownikami systemu(-ów), to zasady:

- wiedzy koniecznej
- najsłabszego ogniwa
- koniecznych przywilejów
- dozwolonej obecności
- odpowiedzialności indywidualnej

4.1.2 Zasady zarządzania bezpieczeństwem systemów…

związane z polityką bezpieczeństwa, to zasady:

- **pełnej świadomości (bardzo ważna)**
- **niezbędnych usług**
- **niemożliwego do osiągnięcia stanu całkowitego bezpieczeństwa**
- **konieczności stosowania norm, standardów i tzw. „dobrych praktyk”**
- **równowagi kosztów zabezpieczeń i wartości zasobów**
- **równowagi pomiędzy zastosowanymi mechanizmami ochrony a zmianami w systemie(-ach)**

5

4.1.3 Zasady zarządzania bezpieczeństwem systemów…

związane z systemem ochrony, to zasady:

- **najsłabszego ogniwa w łańcuchu (zabezpieczeń)**
- **stałej gotowości mechanizmów bezpieczeństwa**
- **dublowania zabezpieczeń**
- **ochrony całościowej**
- **indywidualnego dopasowania**

6

4.2. Zarządzanie bezpieczeństwem systemów w kontekście ograniczeń występujących przy jego realizacji

W każdej chwili gdy zarządzamy bezpieczeństwem systemu(-ów) możemy trafić na przeszkody, które skutecznie utrudnią, ograniczą lub wręcz uniemożliwią jego realizację:

- **finansowe**
- **techniczne**
- **zasobów ludzkich**
- **prawne**
- **czasowe**
- **środowiskowe**
- **organizacyjne**
- **kulturowe i społeczne**

7

4.3. Zarządzanie bezpieczeństwem systemów – koszty czy zyski

Do udzielenia poprawnej odpowiedzi na to pytanie potrzebna jest wiedza o zależności pomiędzy już osiągniętym poziomem bezpieczeństwa a planowanymi wydatkami.

8

4.3.1. Zarządzanie bezpieczeństwem systemów – koszty czy zyski

Podstawowe relacje pomiędzy ponoszonymi wydatkami a poziomem bezpieczeństwa:

a) **w praktyce nigdy nie osiągniemy maksymalnego (całkowitego) poziomu bezpieczeństwa**

9

4.3.1. Zarządzanie bezpieczeństwem systemów – koszty czy zyski

Podstawowe relacje pomiędzy ponoszonymi wydatkami a poziomem bezpieczeństwa:

b) **jeśli chcemy osiągnąć tylko minimalny poziom bezpieczeństwa to i tak wymaga to wydatków** (W_P)

10

4.3.1. Zarządzanie bezpieczeństwem systemów – koszty czy zyski

Podstawowe relacje pomiędzy ponoszonymi wydatkami a poziomem bezpieczeństwa:

c) **w systemie o małym poziomie bezpieczeństwa, już niewielkie zwiększenie wydatków** (W_0 **do** W_1) **powoduje znaczny wzrost poziomu bezpieczeństwa** (z PB_0 do PB_1)

11

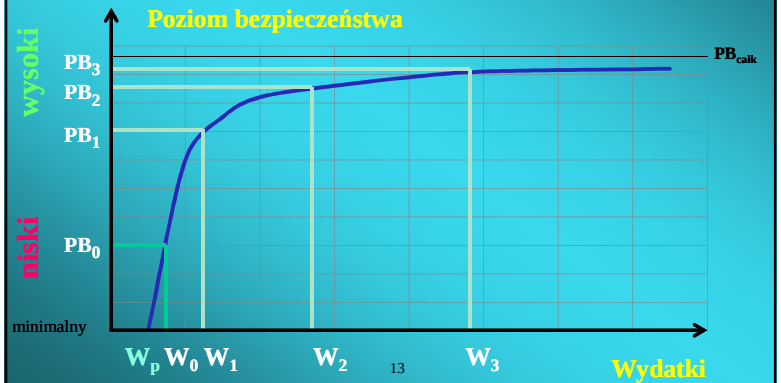
4.3.1. Zarządzanie bezpieczeństwem systemów – koszty czy zyski

Podstawowe relacje pomiędzy ponoszonymi wydatkami a poziomem bezpieczeństwa:

d) **w systemie o bardzo wysokim poziomie bezpieczeństwa, nawet bardzo duże** (W_2 **do** W_3) **zwiększenie wydatków powoduje niewielki wzrost poziomu bezpieczeństwa** (z PB_2 do PB_3)

12

4.3.1. Zarządzanie bezpieczeństwem systemów – koszty czy zyski



13

4.3.2. Zarządzanie bezpieczeństwem systemów – koszty czy zyski

Wydatki na bezpieczeństwo systemów:

- w europie stanowią około 5% kwot przeznaczonych na sektor IT(1)
- w USA stanowią około 7% kwot przeznaczonych na sektor IT

(1) Grzywak.A-Bezpieczeństwo systemów komputerowych (dane z 2000 roku)

14

4.3.2. Zarządzanie bezpieczeństwem systemów – koszty czy zyski

Jednocześnie badani twierdzą, że w ich przedsiębiorstwie:

- potrzeba dalszych inwestycji w bezpieczeństwo systemów – 63% badanych
- inwestycje są odpowiednie – 32% badanych
- wydatki na bezpieczeństwo można obniżyć – 5% badanych

(1) Grzywak.A-Bezpieczeństwo systemów komputerowych (dane z 2000 roku)

15

4.3.2. Zarządzanie bezpieczeństwem systemów – koszty czy zyski

Struktura wydatków na bezpieczeństwo:

- środki zabezpieczeń technicznych – 36%
- wynagrodzenie specjalistów ds. bezpieczeństwa – 23%
- usługi konsultingowe – 11%
- opracowanie strategii bezpieczeństwa – 9%
- szkolenia dla pracowników – 9%
- inne - 12%

16

4.3.3. Zarządzanie bezpieczeństwem systemów – koszty czy zyski

Czy wydatki na bezpieczeństwo systemów się zwracają?

a) **Ochrona systemu to inwestycja**
b) **Stosowanie najbardziej popularnego wskaźnika zwrotu z inwestycji ROI (return on investment) , ze względu na trudną do oszacowania wartość zysku jaką dadzą zabezpieczenia, jest niewykonalne**

17

4.3.3. Zarządzanie bezpieczeństwem systemów – koszty czy zyski

Możemy jednak zastosować wskaźnik zwrotu inwestycji w bezpieczeństwo ROSI (Return on Security Investment (MIT/Standford))

ROSI = R-(ALE)

*** -często stosowany dla narzędzi DLP**

Źródło www.cert.org

18

4.3.3. Zarządzanie bezpieczeństwem systemów – koszty czy zyski

ROSI = R-(ALE)

Aby określić nasz wskaźnik ROSI, należy po prostu odjąć od (R) rocznych kosztów poniesionych strat (np. utraty danych) to, co spodziewamy się stracić w ciągu roku (ALE – annual loss expectancy), gdzie

ALE = (R-E) + T

T – koszt inwestycji czyli koszt zabezpieczeń

E – oszczędności związane z wdrożeniem mechanizmów ochrony

19

4.3.3. Zarządzanie bezpieczeństwem systemów – koszty czy zyski

The Earlier You Invest in Security, the Greater the Return

* - Kevin Soo Hoo

20

4.3.3. Zarządzanie bezpieczeństwem systemów – koszty czy zyski

Więcej informacji o metodach liczenia wskaźnika ROSI:

- http://www.iwar.org.uk/comsec/resources/infosec/roi.pdf
- http://www.infosecwriters.com/text_resources/pdf/ROSI-Practical_Model.pdf
- https://buildsecurityin.us-cert.gov/bsi/articles/knowledge/business/677-BSI.html
- http://net.educause.edu/ir/library/powerpoint/SPC0401.pps - na wesoło

4.4. Analiza stanu bezpieczeństwa systemów w świetle badań

Krótkie omówienie dwóch raportów:

a) raportu firmy PricewaterhouseCoopers „Global state of information security survey – 2012”

b) raportu firmy Ernst&Young „Światowe badania dotyczące bezpieczeństwa informacji”

4.4. Analiza stanu bezpieczeństwa systemów w świetle badań

a) Raport firmy PricewaterhouseCoopers

Ankietowani którzy odpowiedzieli “nie wiem” lub “nie znam odpowiedzi” na poniższe pytanie	2007	2008	2009	2010	2011
Ile incydentów bezpieczeństwa wystąpiło w Twoim przedsiębiorstwie w ciągu ostatnich 12 miesięcy ?	40%	35%	32%	23%	9%
Jakiego typu incydenty wystąpiły ?	45%	44%	39%	33%	14%
Co było źródłem tego incydentu ?	---	42%	39%	34%	22%

4.4. Analiza stanu bezpieczeństwa systemów w świetle badań

a) Raport firmy PricewaterhouseCoopers

Różnice w praktykach z zakresu bezpieczeństwo informacji	Azja		Ameryka Płn.	
	2009	2011	2009	2011
Wydatki na bezpieczeństwo będą wzrastać w ciągu najbliższych 12 miesięcy	53%	74%	29%	31%
Zwiększone ryzyko środowiskowe podniosło znaczenie funkcji bezpieczeństwa	62%	74%	50%	45%
Odpowiedź „nie wiem” na pytanie „Jaka jest liczba incydentów naruszenia bezpieczeństwa w ciągu ostatnich 12 miesięcy”	21%	3%	41%	17%
Odpowiedź „nie wiem” na pytanie „Jakie typy incydentów naruszenia bezpieczeństwa wystąpiły w ciągu ostatnich 12 miesięcy”	30%	6%	47%	20%
Odpowiedź „nie wiem” na pytanie „Jakie są prawdopodobne źródła incydentów naruszenia bezpieczeństwa które wystąpiły w ciągu ostatnich 12 miesięcy”	32%	17%	45%	37%
Czy masz wdrożoną w firmie kompleksową strategię bezpieczeństwa ?	66%	76%	73%	58%

4.4. Analiza stanu bezpieczeństwa systemów w świetle badań

a) Raport firmy PricewaterhouseCoopers

Różnice w praktykach z zakresu bezpieczeństwo informacji	Azja		Ameryka Płn.	
	2009	2011	2009	2011
Używam rozwiązań do zarządzania tożsamością	49%	62%	47%	33%
Czy posiadasz dedykowany personel bezpieczeństwa dla departamentów organizacji ?	48%	61%	42%	36%
Czy posiadasz narzędzia do wykrywania złośliwego kodu (malicious code detection tools) ?	70%	81%	78%	86%
Czy posiadasz narzędzia do wykrywania nieautoryzowanych urządzeń ?	54%	65%	57%	58%
Czy posiadasz narzędzia do skanowania i wykrywania podatności ?	55%	71%	59%	59%
Czy masz ustalone na piśmie zasady poufności ?	59%	70%	65%	57%

4.4. Analiza stanu bezpieczeństwa systemów w świetle badań

a) Raport firmy PricewaterhouseCoopers

Różnice w praktykach z zakresu bezpieczeństwo informacji	Azja		Ameryka Płn.	
	2009	2011	2009	2011
Czy zachowujesz należytą staranność ochrony danych osobowych ?	33%	43%	45%	27%
Czy używasz narzędzi DLP (data loss prevention) ?	44%	57%	49%	48%
Czy szyfrujesz bazy danych ?	65%	76%	59%	50%
Czy używasz bezpiecznych trybów przeglądarki ?	63%	78%	68%	77%
Czy masz wdrożone mechanizmy bezpieczeństwa serwisów internetowych ?	57%	71%	58%	58%

4.4. Analiza stanu bezpieczeństwa systemów w świetle badań

a) Raport firmy PricewaterhouseCoopers

Różnice w praktykach z zakresu bezpieczeństwo informacji	EUROPA		Ameryka Płd.	
	2009	2011	2009	2011
Prawo stało się bardziej skomplikowane i uciążliwe	47%	53%	61%	58%
Wzrosło zagrożenia dla danych firmy z powodu zwolnienia pracownika	34%	42%	52%	48%
Działania na rzecz ograniczenia kosztów utrudniają osiągnięcie lepszych zabezpieczeń	42%	46%	61%	53%
Wzrosło zagrożenie dla bezpieczeństwa naszych zasobów	32%	38%	50%	44%
Nasi partnerzy biznesowi zostali osłabieni przez warunki ekonomiczne	33%	51%	53%	48%
Zredukowano budżet związany z nakładami na bezpieczeństwo	43%	57%	50%	66%

4.4. Analiza stanu bezpieczeństwa systemów w świetle badań

a) Raport firmy PricewaterhouseCoopers

Różnice w praktykach z zakresu bezpieczeństwo informacji	EUROPA		Ameryka Płd.	
	2009	2011	2009	2011
Czy masz wdrożoną w firmie kompleksową strategię bezpieczeństwa ?	59%	59%	56%	60%
Czy zatrudniasz Administratora Bezpieczeństwa Informacji ?	45%	51%	45%	53%
Czy masz wdrożony scentralizowany proces zarządzania bezpieczeństwem informacji ?	43%	34%	50%	38%
Czy monitorujesz postępowanie personelu ?	44%	44%	55%	53%
Czy zachowujesz należytą staranność ochrony danych osobowych ?	20%	18%	27%	25%
Czy wymagania strony trzeciej są zgodne z Twoją polityką bezpieczeństwo ?	31%	22%	32%	28%

4.4. Analiza stanu bezpieczeństwa systemów w świetle badań

a) Raport firmy PricewaterhouseCoopers

Różnice w praktykach z zakresu bezpieczeństwo informacji	EUROPA		Ameryka Płd.	
	2009	2011	2009	2011
Czy używasz narzędzi DLP (data loss prevention) ?	50%	58%	59%	57%
Czy posiadasz filtry zawartości stron internetowych ?	55%	72%	64%	72%
Czy jesteś przekonany, że ochrona bezpieczeństwa informacji w Twojej firmie jest skuteczna ?	73%	62%	89%	71%
Czy jesteś przekonany, że ochrona bezpieczeństwa informacji u Twoich partnerów/dostawców jest skuteczna ?	65%	62%	86%	70%

29

4.4. Analiza stanu bezpieczeństwa systemów w świetle badań

a) Raport firmy PricewaterhouseCoopers - pełna wersja raportu dostępna na stronie:

http://www.pwc.pl/pl_PL/pl/publikacje/global-state-of-information-security-survey-2012.pdf

30

4.4. Analiza stanu bezpieczeństwa systemów w świetle badań

b) Raport firmy Ernst&Young

- **znaczącą przeszkodą w osiągnięciu zadowalającego poziomu bezpieczeństwa są:**
  - **brak wystarczających środków finansowych - uzyskanie środków finansowych na bezpieczeństwo wymaga dokładnego uzasadnienia celowości wydatków**
  - **przekonanie zarządu o wadze bezpieczeństwa systemu**
  - **zmiany priorytetów wykorzystania zasobów**

31

4.4. Analiza stanu bezpieczeństwa systemów w świetle badań

b) Raport firmy Ernst&Young

- **pomimo uzyskania wysokich wskaźników co do wagi analizy ryzyka, zalecenia wynikające z analizy ryzyka, podczas rozpatrywania nowych rozwiązań wzięła pod uwagę niespełna 1/3 badanych**

32

4.4. Analiza stanu bezpieczeństwa systemów w świetle badań

b) Raport firmy Ernst&Young

- podejście do kwestii bezpieczeństwa ma charakter reakcji na zdarzenie, nadal zbyt mało firm podchodzi do bezpieczeństwa kompleksowo (analizując możliwości, zagrożenia i korzyści)
- największe nakłady przeznacza się na zakup technologii i narzędzi teleinformatycznych; zbyt małą wagę przywiązuje się do korzyści z nakładów w kapitał ludzki

33

4.4. Analiza stanu bezpieczeństwa systemów w świetle badań

b) Raport firmy Ernst&Young

- według raportu nadal największym zagrożeniem są wirusy komputerowe, są coraz bardziej złożone i specjalizowane
- z zagrożeń z wnętrza organizacji wymieniane jest najczęściej wykorzystanie systemów komputerowych niezgodnie z zasadami

34