
UpGreat
we know-how to do IT
Wsparcie dla biznesu

UpGreat
we know-how to do IT

RODO – zmiana podejścia do ochrony danych osobowych

- Wprowadzenie do RODO
- Analiza ryzyka
- Metodyki analizy
- Kryteria akceptowalności
- Aktywa
- Zagrożenia
- Zabezpieczenia

Jakub Staśkiewicz
UpGreat Systemy Komputerowe Sp. z o.o.

ZMIANY W RODO W KONTEKŚCIE ZAPEWNIENIA BEZPIECZEŃSTWA

- Obowiązek zgłaszania naruszeń bezpieczeństwa organowi nadzorczemu, administratorowi danych oraz podmiotowi danych.
- Zapewnienie ochrony prywatności już w fazie projektowania systemów (Privacy By Design)
- Zapewnienie ochrony prywatności jako domyślnej cechy systemów (Privacy By Default)
- Art. 32 RODO nakłada obowiązek wdrożenia **odpowiednich** zabezpieczeń w celu ochrony przed zagrożeniami
- Wprowadzenie podejścia do zabezpieczeń opartego na **analizie ryzyka**

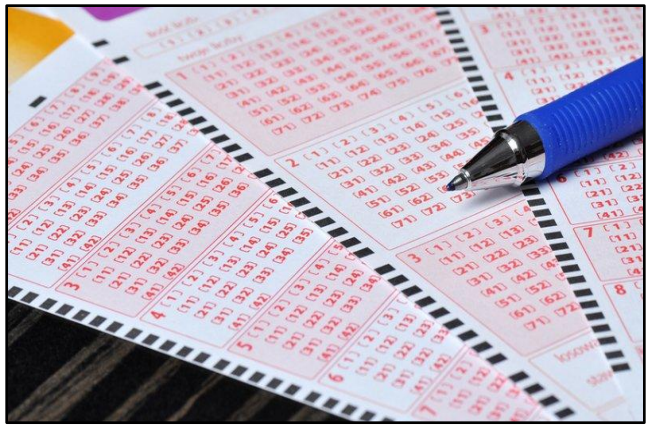
UpGreat
we know-how to do IT

Czym jest ryzyko?

RYZYKO

Potocznie to wskaźnik stanu lub zdarzenia
mogącego prowadzić do straty (obawa, niepewność).

1 / 22 000 000
1 / 776 000



1 / 14 000 000
1 / 176 000 000

Ryzyko to nie tylko prawdopodobieństwo, jest ono rzutowane na subiektywne poczucie wartości i straty

ANALIZA RYZYKA - DEFINICJE

UpGreat
we know-how to do IT

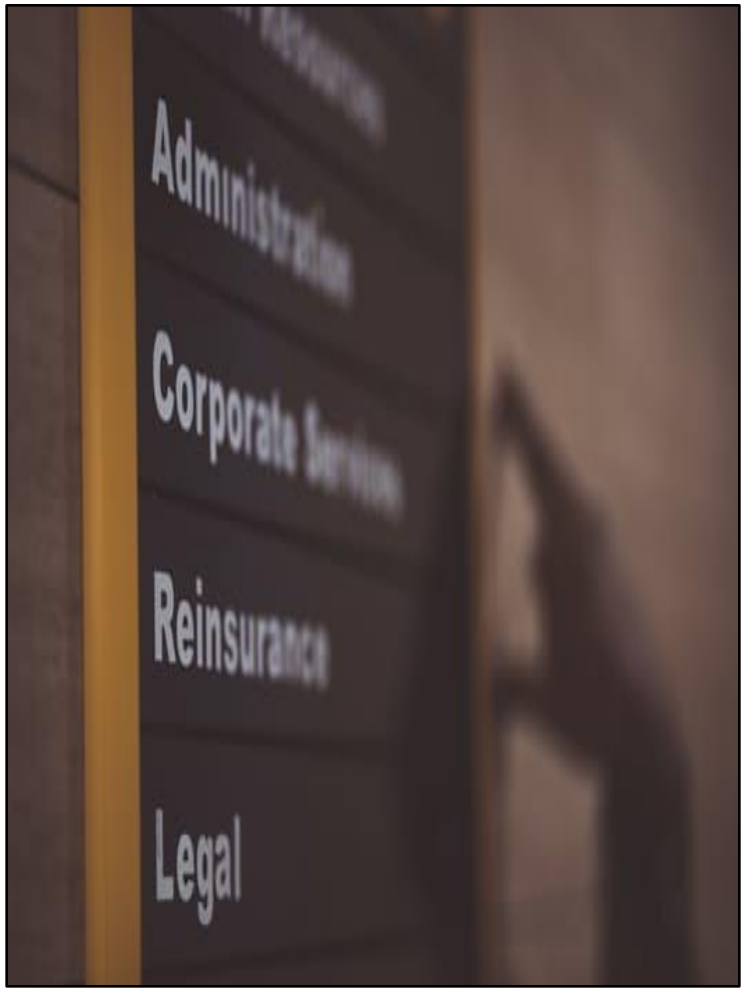
STRATA – nie tylko wymiar materialny

- Strata wizerunku lub zaufania
- Strata przewagi konkurencyjnej
- Strata spodziewanych przychodów lub klientów
- Strata przywilejów lub legalności
- Aktywa – również niematerialne

ANALIZA RYZYKA - DEFINICJE

AKTYWA – wszystko co stanowi wartość dla organizacji

- Wiedza, know-how
- Pracownicy
- Lokalizacja
- Dostawcy, kontrakty
- Dane
- Licencje
- Infrastruktura



AKTYWA – CHRONIONE WARTOŚCI

UpGreat
we know-how to do IT

Jakie wartości aktywów podlegają ochronie?

Przykład: co uznamy za stratę w przypadku bazy danych?

- Jeden rekord bazy na 1 tys.?
- Jeden rekord bazy na 1 mln?
- Wykradziony / ujawniony?
- Skasowany?
- Błędnie wprowadzony?

W kontekście ochrony danych stratą będzie każde naruszenie ich bezpieczeństwa.

Jak zatem precyzyjnie zdefiniować bezpieczeństwo?

- **C**onfidentality - poufność
- **I**ntegrity - integralność
- **A**vailability - dostępność

INCYDENT BEZPIECZEŃSTWA

INCYDENT - pojedyncze zdarzenie lub seria niepożądanych lub niespodziewanych zdarzeń, które stwarzają ZNACZNE prawdopodobieństwo zakłócenia działań biznesowych i zagrażają bezpieczeństwu informacji.

Jak zatem rozpoznać ZNACZNY wpływ na działania biznesowe?

Konieczna jest analiza wpływu na biznes (BIA)

BIA – BUSINESS IMPACT ANALYSIS

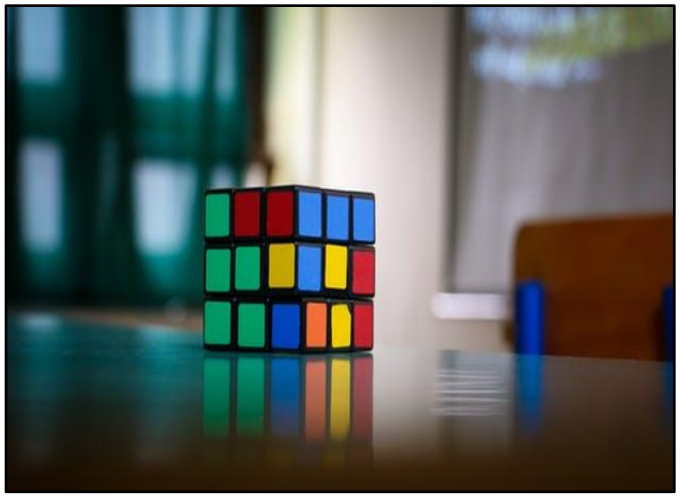
UpGreat
we know-how to do IT

BIA – ma na celu ustalenie jak niekorzystny wpływ na realizację celów biznesowych będzie miało zaistnienie określonego incydentu bezpieczeństwa.

W tym celu musimy zidentyfikować wszystkie krytyczne procesy biznesowe (np. przyjmowanie zamówień, produkcja, realizacja wysyłki).

Musimy też znać zasoby konieczne do realizacji krytycznych procesów (np. infrastruktura, ludzie, materiały).

PODSUMOWANIE POJĘĆ:
ryzyko, strata, aktywa i ich wartość, incydent, bezpieczeństwo, wpływ na biznes…



ANALIZA:
Ocena ryzyka zaistnienia incydentu naruszającego bezpieczeństwo aktywów o określonej wartości i mogącego spowodować określone straty biznesowe.

Jaki jest ostatni, brakujący element układanki?

ZAGROŻENIE:
czynnik odpowiedzialny za powstanie incydentu

- naturalne (zjawiska przyrodnicze, ale też np. wyczerpanie zasobów)
- przypadkowe (awarie, wypadki, błędy ludzkie)
- zamierzone (kradzieże, ataki cyberprzestępców, akty wandalizmu, terroryści, hacktywiści)
- administracyjne (zmiana prawa)

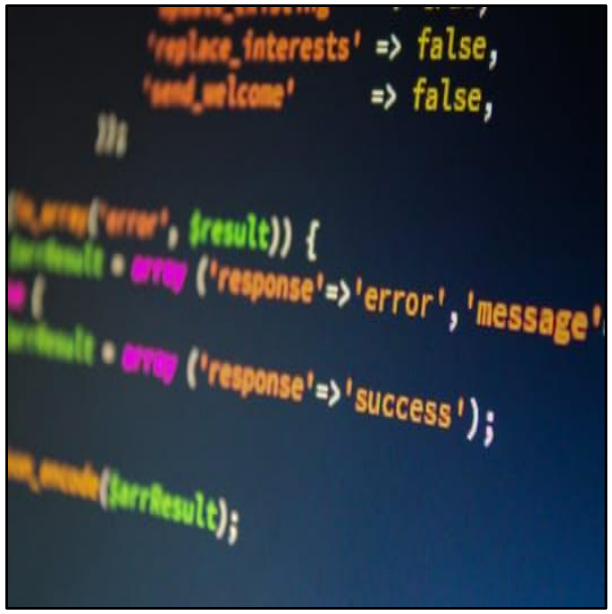
UpGreat
we know-how to do IT

PODATNOŚĆ

cecha sprzyjająca urzeczywistnieniu się potencjalnego zagrożenia.

Przykłady:

- Brak aktualizacji oprogramowania
- Częste awarie systemu zasilania
- Brak szkoleń dla pracowników
- Brak polityk bezpieczeństwa

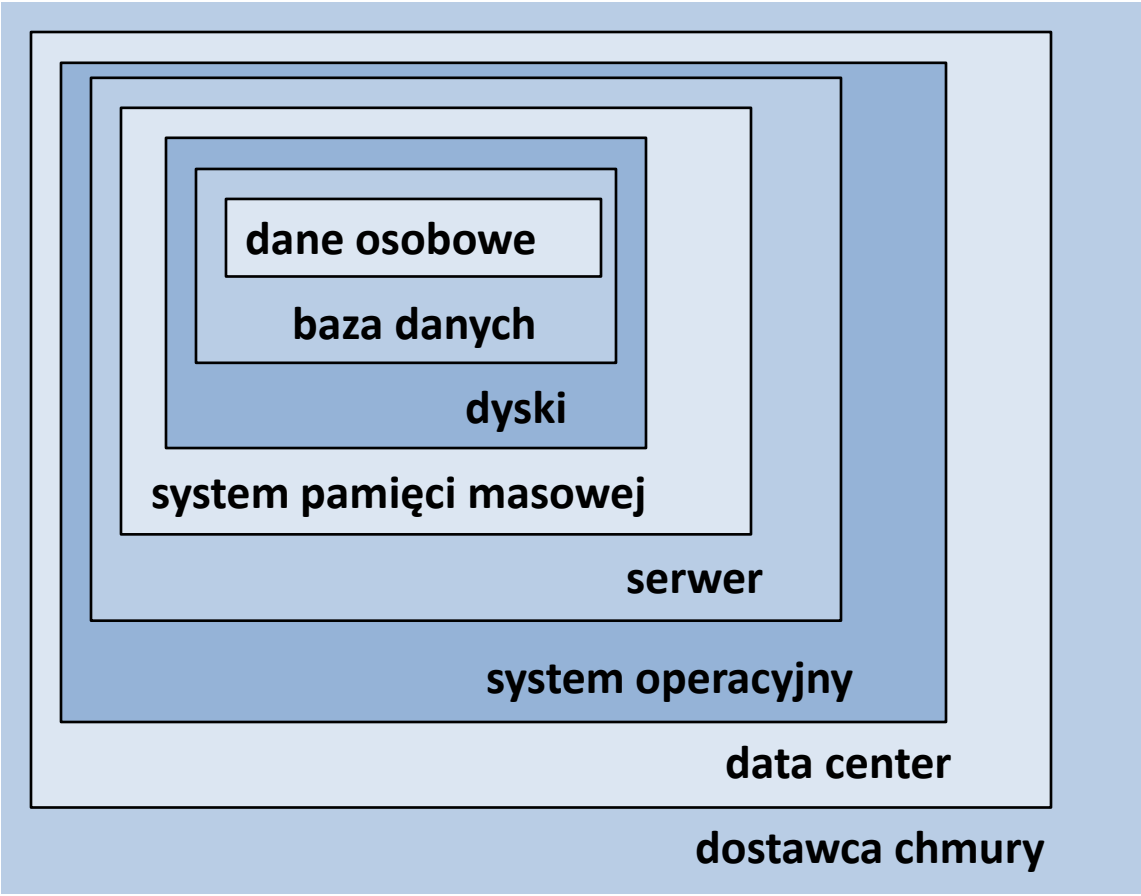


Ćwiczenie:

Jakie potencjalne podatności zagrażające bezpieczeństwu bazy danych osobowych jesteś w stanie wskazać?

POWIERZCHNIA ATAKU

całościowy zbiór elementów, w których mogą wystąpić podatności zagrażające danym aktywom.



W tym wypadku zagrożenia dla danych osobowych wynikają z sumy podatności wszystkich elementów mających na nie wpływ

UpGreat
we know-how to do IT

- Szacowanie skutków oraz prawdopodobieństwa odbywa się w skali 1 - 5

- Wytyczne dotyczące kwalifikacji następstw i prawdopodobieństwa do odpowiednich kategorii (1-5)

- Ryzyko jako iloczyn prawdopodobieństwa i skutków

R = P x S

R - Ryzyko
P - Prawdopodobieństwo
S - Skutki

UpGreat
we know-how to do IT

Szacowanie prawdopodobieństwa

Poziom	Opis	Prawdopodo-bieństwo	Częstotliwość wystąpienia
1	Prawie niemożliwe	< 0,01	1 x 100 lat
2	Mało prawdopodobne	0,01 – 0,1	1 x 10 lat
3	Umiarkowanie możliwe	0,1 – 0,2	1 x 5 lat
4	Prawdopodobne	0,2 – 0,5	1 x rok
5	Prawie pewne	> 0,5	1 x m-c

UpGreat
we know-how to do IT

Szacowanie następstw

Poziom	Skutek	Opis
1	Minimalny, pomijalny	Nikły wpływ na funkcjonowanie organizacji
2	Mało znaczący, niski	Brak poważnego wpływu na działanie organizacji
3	Znaczący, umiarkowany	Krótkotrwały, poważny wpływ na działanie organizacji
4	Poważny, wysoki	Poważny wpływ na działanie organizacji
5	Katastrofalny, krytyczny	Zagrożenie dla kontynuacji działania organizacji

UpGreat
we know-how to do IT

Szacowanie ryzyka

Macierz ryzyka		Prawdopodobieństwo				
		5	4	3	2	1
Następstwa	5	25	20	15	10	5
	4	20	16	12	8	4
	3	15	12	9	6	3
	2	10	8	6	4	2
	1	5	4	3	2	1

UpGreat
we know-how to do IT

Postępowanie z ryzykiem

Wartość	Rodzaj ryzyka	Opis działania
25	Krytyczne	Konieczna natychmiastowa poprawa, należy rozważyć wstrzymanie procesu
10 – 20	Nieakceptowalne	Konieczne niezwłoczne podjęcie działań obniżających ryzyko
5 – 10	Akceptowalne warunkowo	Konieczne działania zmniejszające ryzyko jeśli nie ma przeciwwskazań ekonomicznych
2 – 4	Akceptowalne	Nie ma konieczności podejmowania działań ale należy monitorować ryzyko
1	Pomijalne	Nie ma konieczności podejmowania jakichkolwiek działań

ANALIZA RYZYKA - POSTĘPOWANIE

Postępowanie z ryzykiem – możliwe warianty działania:

- AKCEPTACJA: godzimy się z możliwością wystąpienia incydentu, jego skutki są ekonomicznie akceptowalne a koszt wdrożenia zabezpieczeń przewyższa wartość ewentualnych strat

- MIMINALIZACJA: wdrożenie rozwiązań zmniejszających poziom ryzyka (techniczne lub operacyjne środki zaradcze)

- UNIKANIE: unikanie i eliminacja działań powodujących występowanie ryzyka

- PRZENIESIENIE: przekazanie ryzyka innemu podmiotowi (np. ubezpieczyciel, dostawca, podwykonawca)

ŹRÓDŁA INFORMACJI O ZAGROŻENIAC

Testy penetracyjne i audyty bezpieczeństwa jako narzędzia identyfikacji zagrożeń oraz podatności:

- Ustawa o Ochronie Danych Osobowych (plan sprawdzeń)
- Krajowe Ramy Interoperacyjności (audyt bezpieczeństwa min. 1 x rok)
- ISO 27001 (audyt bezpieczeństwa jako narzędzie oceny skuteczności)

ZADANIA ZESPOŁU SECURITY

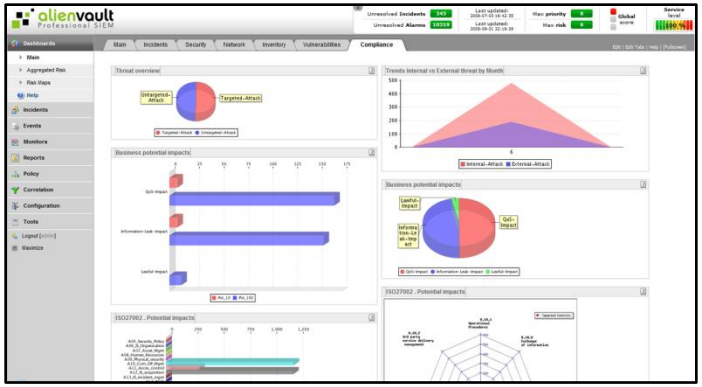
- Inwentaryzacja i klasyfikacja aktywów
- Polityki bezpieczeństwa
- Okresowe audyty bezpieczeństwa i testy penetracyjne
- Zarządzanie incydentami bezpieczeństwa
- Szkolenia pracowników
- Dokumentacja
- Szacowanie i analiza ryzyka
- Zarządzanie aktualizacjami
- Procedury disaster recovery
- Dobór i utrzymanie środków technicznych
- Filtrowanie ruchu
- Polityki AD
- Monitoring infrastruktury
- Archiwizacja i analiza logów

POTRZEBUJEMY SOC

- SOC – Security Operations Center
  Wydzielona jednostka do monitorowania, reagowania na incydenty i utrzymywania infrastruktury związanej z ochroną

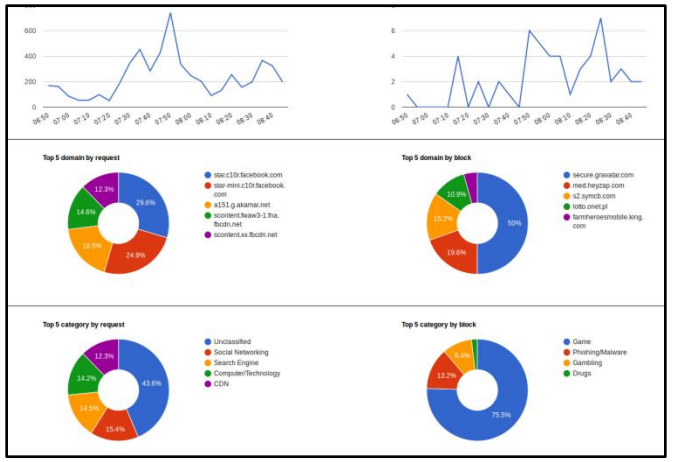
- Monitorowanie
  IDS/IPS, sondy sieciowe, monitoring sieci, monitoring środowiskowy, monitoring bezpieczeństwa stacji – AV, HIDS, bramki skanujące ruch smtp i http/https

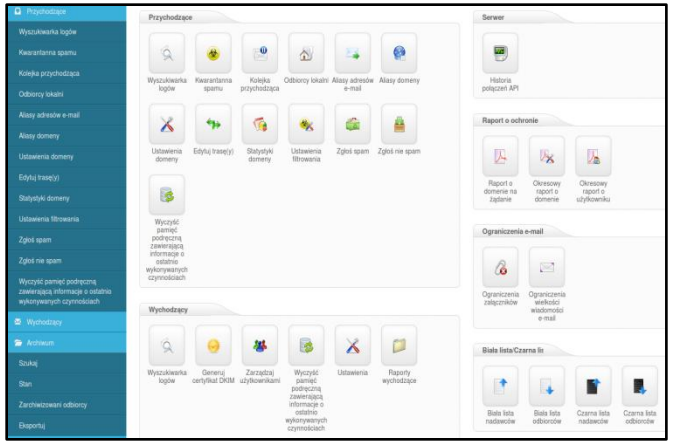
- Zarządzanie logami
  Centralne gromadzenie, archiwizacja i kompresja. Korelacja zdarzeń i ich ocena pod kątem zagrożeń – systemy typu SIEM



SOC – CLEAN PIPE

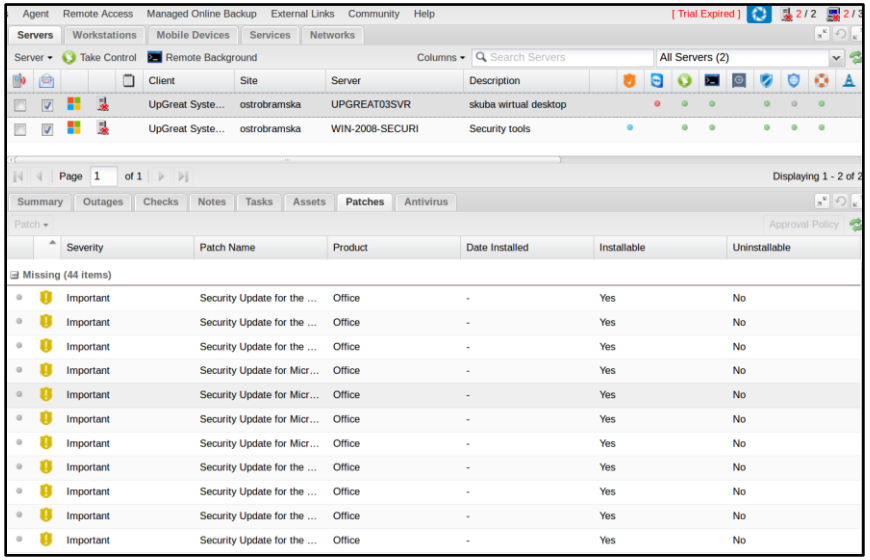
- Filtrowanie poczty
  ochrona antywirusowa i antyspamowa
- Filtrowanie WWW i DNS
  ochrona na podstawie treści, kategorii, bazy reputacji
- Ochrona usług webowych
  anty DDOS, web application firewall





SOC – ENDPOINT SECURITY

- Ochrona antywirusowa
- Skanowanie podatności
- Zarządzanie aktualizacjami
- Backup i archiwizacja
- Zdalny dostęp
- Inwentaryzacja sprzętu i oprogramowania
- Monitoring usług i parametrów systemowych
- Ochrona urządzeń mobilnych (BYOD)



SOC – USŁUGI DODATKOWE

- Polityki i audyty bezpieczeństwa
- Testy penetracyjne i próby socjotechniczne
- Szkolenia użytkowników
- Usługi ABI
- Konsultacje z zakresu bezpieczeństwa

UpGreat
we know-how to do IT

Dziękuję za uwagę

- http://www.upgreat.pl/blog
- http://www.facebook.com/upgreat.poznan

Jakub Staśkiewicz
UpGreat Systemy Komputerowe Sp. z o.o.

Dziękuję za uwagę

Jakub Staśkiewicz
tel.: 667 768 452
mail: jakub.staskiewicz@upgreat.pl

UpGreat Systemy Komputerowe Sp. z o.o.
60-122 Poznań, ul. Ostrobramska 22
http://www.upgreat.com.pl