Rola inspektora ochrony danych w zabezpieczeniu systemu informatycznego. Podejście oparte na ryzyku

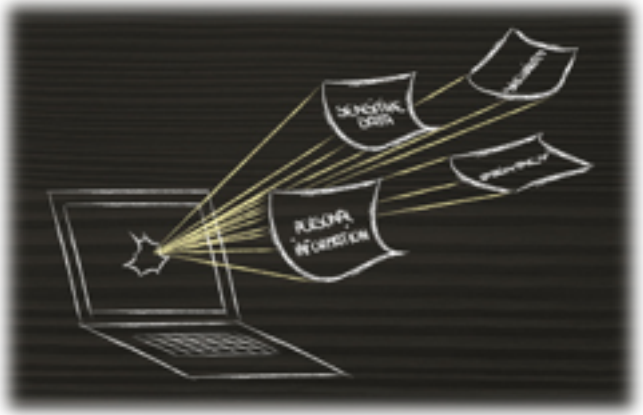
Mariola Więckowska

GIODO oraz INP PAN– 14 luty 2017

Agenda

1. UODO: Analiza ryzyka systemów IT
2. Przykłady ryzyk
3. RODO: co to jest Ryzyko Prywatności?
4. Stosowanie podejścia opartego na ryzyku w praktyce
5. Zwiększenie bezpieczeństwa systemów IT poprzez analizę ryzyka - rola Inspektora Ochrony Danych

Ryzyko przetwarzania danych określa miarę stopnia zagrożenia dla poufności, integralności i dostępności informacji, wyrażoną jako prawdopodobieństwa wystąpienia zagrożenie i szkodliwości jej skutków



Podejście oparte na ryzyku a ochrona przed cyber-zagrożeniami

- 4.3 miliarda rekordów zostało skradzionych przez hakerów w 2016, m.in. od takich gigantów jak Yahoo, LinkedIn czy MySpace
- Obawy konsumentów rosną, gdyż średni czas wykrycia wycieku danych to 201 dni.
- Ofiarami ransomware padają instytucje publiczne włączając policję, szkoły i szpitale
- 49% firm było przedmiotem ransomware. W pierwszych 3 miesiącach 2016 firmy zapłaciły ponad $209m - co w porównaniu z $24m w 2015 daje wzrost o 771%. FBI szacuje, że opłaty ransom przekroczą $1 miliard rocznie.
- Wdrożenie podstawowych zasad bezpieczeństwa już dawno nie wystarcza. Potrzeba znacznie bardziej zaawansowanych metod zabezpieczeń, jak przykładowo szyfrowanie, by ochronić się przed licznymi cyberatakami.
- IoT [Internet of Things] staje się znaczącym problemem

Inwentaryzacja zbiorów danych i powiązanych systemów IT

- Wykaz zbiorów danych osobowych wraz z programami służącymi do ich przetwarzania
- Ustalenie Właściciela Biznesowego i Właściciela Technicznego

Zasady ochrony danych osobowych

Przynajmniej raz w roku, osoba wyznaczona przez Właściciela Biznesowego systemu informatycznego przeprowadza przegląd i przygotowuje raport, który przedstawia ABI.

Raport w szczególności powinien zawierać:

- Zgodność uprawnień z listą osób upoważnionych do dostępu (przegląd praw dostępu użytkowników).
- Opis spełnienia przez system wymogów określonych w Instrukcji Zarządzania Systemami Informatycznymi (IZSI).
- **Ryzyka i kryteria ich oceny oraz zagrożenia dla danych wraz z ich prawdopodobieństwem i skutkami.**
- Ocenę adekwatności dokumentacji w odniesieniu do rodzaju przetwarzania danych oraz złożoności systemu informatycznego.

Atrybuty ryzyka

Kontrola zarządcza	Legalność	Poufność	Integralność	Dostępność	Bezpieczeństwo
Brak kontroli zarządczej w obszarze ochrony danych osobowych. Nie spełnianie wymagań zasad przetwarzania danych osobowych, w tym zasady bezpieczeństwa danych i wdrożenia procedur wymaganych przez UODO i związane akty prawne.	Brak spełnienie wymogów legalności przetwarzania w tym również transferu danych do państw trzecich (USA i kraje z poza UE) oraz powierzania przetwarzania danych osobowych wynikającego z UODO i powiązanych aktów prawnych.	Brak zapewnienia poufności danych osobowych, polegające na tym, że informacja jest dostępne lub wyjawiana nieupoważnionym osobom, podmiotom lub procesom.	Brak zapewnienia integralności danych - zapewnienie mechanizmów kontroli zmian danych oraz ich utraty w systemach IT.	Ryzyko związane z brakiem zapewnienia odpowiedniego poziomu dostępności do danych, m.in. opracowania i testowania BCP.	Brak adekwatnego poziomu stosowanych zabezpieczeń w zakresie ochrony danych osobowych, w tym zapewnienie środków technicznych i organizowanych wynikających z Polityki bezpieczeństwa, Instrukcji zarządzania systemami informatycznymi oraz wewnętrznych procedur.

Przykłady ryzyka dla systemów informatycznych

- Brak identyfikacji i analizy ryzyka w zakresie przetwarzania i ochrony danych osobowych.
- Zbieranie i przetwarzania danych osobowych niezgodnie z prawem: błędne określenie celu i zakresu przetwarzanych danych.
- Nieprzestrzeganie praw osób, które dane dotyczą.
- Przechowywanie danych po wygaśnięciu celu przetwarzania danych.
- Transfer danych do państwa trzeciego lub przetwarzania danych w chmurze publicznej niezgodnie z prawem - bez stosownych umów.
- Utrata lub uszkodzenie lub nieuzasadniona zmiana danych osobowych.
- Dostęp do zbioru danych osobowych przez osoby nieupoważniony.
- Przesyłanie danych drogę telekomunikacyjną bez stosownych zabezpieczeń wynikających z analizy ryzyka.
- Zabezpieczenie: hacking/phishing, wirusy, robaki, konie trojańskie.
- Błędne zarządzanie procesem obsługi incydentów. Niewłaściwa administracja i konfiguracja systemu informatycznego.
- Celowe lub przypadkowe uszkodzenie aplikacji, systemu operacyjnego lub urządzeń sieciowych skutkujące utratę, uszkodzeniem lub niewłaściwa modyfikacją danych.
- Utrata, uszkodzenie lub niewłaściwa modyfikacja danych spowodowana błędami powdrożeniowymi oprogramowania.
- System informatyczny nie spełnia wymagań z Instrukcji Zarządzania Systemami Informatycznymi.
- Brak rejestracji udostępnianych danych osobowych.
- Zniszczenie/zafałszowanie logów systemowych - dowodów audytowych
- Brak rozliczalności systemu - nie przydzielenie unikalnych identyfikatorów użytkownikom lub użycie konta współdzielonego.
- Prawidłowe odtwarzania usługi z Planu Ciągłości Działania.
- Trwałe usunięcie danych po wygaśnięciu celu przetwarzania danych.

Ryzyko w RODO

Ryzyka prywatności i ich potencjalne skutki można podzielić na 2 kategorie:

- **Ryzyko wiążące się z przetwarzaniem danych**, rodzące skutki finansowe, prawne i utraty reputacji w wyniku naruszenia prywatności oraz konsekwencje nieprzestrzegania przepisów w tym RODO.
- RODO wprowadza **ryzyko naruszenia praw lub wolności osób**, w tym braku wypełniania praw osób, możliwości kradzieży tożsamości, naruszenia dobrego imienia, dyskryminacji lub negatywnych skutków finansowych.

Ryzyka naruszenia praw do ochrony danych i ich mitygacja

Ryzyko

- Przypadkowego lub niezgodnego z prawem zniszczenia, utracenia, zmodyfikowania, nieuprawnionego ujawnienia lub nieuprawnionego dostępu do danych osobowych.
- Braku zapewnienia bezpieczeństwa przetwarzania danych na poziomie, który odpowiada ryzyku naruszenia praw i wolności osób fizycznych.
- Uznanie pseudonimizacji za równoważną ze zanonimizowanymi danymi
- Nieuwzględnienie możliwości profilowania – utrata prywatności osoby fizycznej

Mitygacja

Wdrożenie odpowiednich środków technicznych i organizacyjnych, które zapewnią odpowiedni stopień bezpieczeństwa, w tym:

- Pseudonimizację i szyfrowanie danych osobowych;
- Zdolność do ciągłego zapewnienia poufności, integralności, dostępności i odporności systemów i usług przetwarzania.
- Zdolność do szybkiego przywrócenia dostępności danych osobowych i dostępu do nich w razie incydentu fizycznego
- Regularne testowanie, mierzenie i ocenianie skuteczności środków technicznych i organizacyjnych mających zapewnić bezpieczeństwo przetwarzania.

Wysokie ryzyko: Ocena skutków dla ochrony danych (OSOD)

Jeżeli dany rodzaj przetwarzania – w szczególności z użyciem nowych technologii – ze względu na swój charakter, zakres, kontekst i cele z dużym prawdopodobieństwem może powodować wysokie ryzyko naruszenia praw lub wolności osób fizycznych to przeprowadza się OSOD, w szczególności w przypadku:

- systematycznej, kompleksowej oceny czynników osobowych odnoszących się do osób fizycznych, która opiera się na zautomatyzowanym przetwarzaniu, w tym profilowaniu, i jest podstawą decyzji wywołujących skutki prawne wobec osoby fizycznej lub w podobny sposób znacząco wpływających na osoby fizyczne;
- przetwarzania na dużą skalę szczególnych kategorii danych osobowych, o których mowa w art.9 ust.1 lub danych osobowych dotyczących wyroków skazujących i naruszeń prawa, o czym mowa w art.10;
- systematycznego monitorowania na dużą skalę miejsc dostępnych publicznie.

Analiza ryzyka w Ocenie skutków dla ochrony danych

Analiza ryzyka naruszenia praw lub wolności osób fizycznych przy uwzględnieniu wiedzy technicznej, kosztu wdrożenia, charakteru, zakresu, kontekstu i celów przetwarzania powinna rozważyć poniższe obszary:

1. Cel i zakres zbierania danych osobowych
2. Źródło danych osobowych
3. Informowanie podmiotu o zbieraniu danych osobowych
4. Sposób zbierania danych osobowych
5. Przechowywanie i bezpieczeństwo danych osobowych
6. Dostęp do danych
7. Sprostowanie danych
8. Poprawność i adekwatność przetwarzanych danych
9. Okres przechowywania danych
10. Wykorzystanie danych zgodnie z celem
11. Ujawnienie i przekazywanie danych
12. Użycie unikalnych identyfikatorów

Przykładowe obszary analizy ryzyka

Obszar ryzyka	Opis ryzyka	Wpływ ryzyka na przetwarzającego i podmiot danych	Istniejące zabezpieczenia mogące ograniczyć ryzyko	Ocena obecnego ryzyka rezydualnego	Rekomendowane dodatkowe działania dla ograniczenia ryzyka	Rezydualne ryzyko pozostałe mimo wprowadzenia środków zapobiegawczych
Zakres danych zbieranych przez aplikację	Aplikacje będzie zbierać więcej danych niż wynika to z polityki prywatności	Aplikacja będzie posiadać lepszą funkcjonalność i prowadzić do zwiększonych zysków, ale użytkownicy mogą sprzeciwić się zbieraniu danych wykraczających poza zakres wskazany w polityce prywatności i zbieranie może być niezgodne z prawem	Business ma adekwatny cel pozwalający na zbierania większego zakresu danych osobowych, ale polityka prywatności tego nie uwzględnia	Prawdopodobieństwo: Średnie Wpływ: Średni	Wdrożenie procesu dla zarządzanie powiadomieniem o rozszerzeniu celu i w związku z tym uzyskaniem zgody dla zwiększonego zakresu zbierania danych przez aplikację	Prawdopodobieństwo: Niskie Wpływ: Minimalny Niektórzy istniejący klienci mogą ciągle nie zdawać sobie sprawy, że zmiana nastąpiła

Przykłady mitygacji

Dla każdego zdefiniowanego ryzyka określić działania i możliwości jego wyeliminowania lub zmniejszenia, m.in.:

- Podjęcie decyzji o rezygnacji ze zbierania, wykorzystywania lub ujawniania poszczególnych rodzajów danych osobowych.
- Przechowywania danych tylko tak długo, jak to konieczne i zaplanowanie bezpiecznej likwidacji informacji.
- Wdrożenie odpowiednich technologicznych, procesowych i fizycznych środków zabezpieczeń.
- Opracowanie sposobów na bezpieczne utajnianie lub/i de-identyfikację informacji.
- Przeszkolenie i przygotowanie instrukcji dla personelu, jak używać bezpiecznie nowy system.
- Transparentność w kontakcie z podmiotami danych.
- Wybór dostawców oferujących większy stopień bezpieczeństwa.

Rola Inspektora Ochrony Danych

- Aktywnie uczestniczy w analizie ryzyka oraz rekomenduje środki pozwalające na jego mitygację.
- Wspomaga w wyborze adekwatnych środków zaradczych najbardziej korzystnych dla podmiotów danych, projektu i administratora danych.
- Poprzez odpowiednio przeprowadzoną analiza ryzyka wykazuje stosowanie ochrony danych w fazie projektowania oraz domyślną ochronę danych.
- Dla każdego rekomendowanego środka zaradczego ograniczającego ryzyko pomaga określić konkretne działania, osobę odpowiedzialną i termin realizacji.
- Dba, aby wszelkie decyzje dotyczące prywatności i wybranych działań zostały odpowiednio udokumentowane i zaakceptowane.
- Dokłada starań, aby informacje przedstawione były w sposób prosty i zrozumiały dla odbiorcy, który nie posiada wiedzy na temat technologii, prawa lub danego systemu.
- Monitoruje postęp działań związanych z ochroną prywatności, aby upewnić się, że są odpowiednio zakończone.
- Wspiera ocenę zmiany w realizacji projektu, procesów biznesowych, przepływu informacji, ról i zadań, aby upewnić się, że nie powstaje nowe ryzyko prywatności.

Dziękuję!
Zapraszam do dyskusji!

mariola.wieckowska@allegrogroup.com

Mariola Więckowska