Przepisy GIODO

- Najważniejsze wymagania dla systemów informatycznych

Ver 1.0, Autor: Bartosz Gędziorowski

Plan prezentacji

1. Przepisy GIODO – zastosowanie w systemach IT
2. Siedem zasad zapewnienia ochrony
3. Pozyskiwanie danych osobowych - formularz
4. Konta w systemie
   - Użytkownik
   - Administrator
5. Przechowywanie danych
6. Zabezpieczenia i wymagania
7. Przykłady rozwiązań technicznych

Przepisy GIODO zastosowanie w systemach IT

- Ustawa o ochronie danych osobowych (z dn. 29 sierpnia 1997) reguluje wymagania dot. bezpieczeństwa i funkcjonalności
- Zastosowanie: systemy informatyczne przetwarzające dane osobowe
- Prezentujemy najważniejsze wymagania wobec systemów mających połączenie z Internetem
- Szczegóły: www.giodo.gov.pl

7 zasad zapewnienia ochrony 1/2

- **Poufność** – informacja dostępna tylko dla uprawnionych
- **Integralność** – dane chronione przed nieautoryzowanymi zmianami
- **Dostępność** – dane osiągalne dla uprawinonych
- **Rozliczalność** – ograniczenie możliwych działań podmiotu do jego uprawnień

7 zasad zapewnienia ochrony 2/2

- **Autentyczność** – zapewnieniu tożsamości podmiotu z zadeklarowaną
- **Niezaprzeczalność** – braku możliwości wyparcia się swego uczestnictwa
- **Niezawodność** – zapewnienie spójności zamierzonych zachowań i skutków.

Pozyskiwanie danych osobowych poprzez formularz 1/2

- Zgoda na przetwarzanie danych w postaci checkbox (nie może być zaznaczony domyślnie)
- Osobna zgoda na przetwarzanie w celach marketingowych (nieobowiązkowa)
- Nie wolno łączyć w/w punktów
- Zbieramy minimum danych – tylko te faktycznie potrzebne

Pozyskiwanie danych osobowych poprzez formularz 2/2

- Obowiązek poinformowania osoby wypełniającej formularz
  - Kto jest administratorem (pełne dane, siedziba itd.)
  - W jakim celu dane są zbierane
  - W jaki sposób będą przetwarzane
  - O możliwości wglądu i zmieniania swoich danych
  - Wymienić wszystkich planowanych odbiorców danych
  - O dobrowolności podania danych lub o takim obowiązku ze wskazaniem podst. prawnej.

Konta w systemie - użytkownik

- Uwierzytelnianie użytkownika za pomocą loginu i unikalnego hasła (co najmniej 6 znaków)
- Hasło zmieniane nie rzadziej niż co 30 dni
- Możliwość dostępu użytkownika (tylko) do swoich danych i możliwość ich poprawiania
- Czytelnie opisane pola z danymi, najlepiej bez skrótów

Konta w systemie - administrator

- Osobne i unikalne konto dla każdego administratora
- Raz użyty login nie może być powtórnie wykorzystany
- Każdy login powiązany z imieniem i nazwiskiem
- Hasło zmieniane co 30 dni, min. 8 znaków (małe i wielkie litery oraz cyfry lub znaki specjalne)

Przechowywanie danych 1/2

- System powinien przechowywać informacje:
  - Kto i kiedy wprowadził dane
  - Kto i kiedy ostatnio edytował dane
  - Ewentualnie inne źródło danych (jakie)
  - Odbiorcy danych, zakres i data udostępnienia
- Regularne kopie zapasowe (zabezpieczone przed nieuprawnionym dostępem)
- Dane osobowe po osiągnięciu celu muszą zostać bezpowrotnie usunięte (także kopie).

Przechowywanie danych 2/2

- Numery porządkowe użytkowników mogą mieć zakodowane tylko następujące informacje:
  - Data urodzenia
  - Płeć
  - Nr nadania
  - Suma kontrolna

Zabezpieczenia i wymagania 1/2

- Hasła zaszyfrowane bez możliwości odczytu (hash and salt)
- Hasło nadane i dostarczone (np. drogą mailową) powinno być zmienione przez użytkownika
- Zabezpieczenie przed nadaniem zbyt prostych haseł
- Zabezpieczenie danych osobowych przed zindeksowaniem przez wyszukiwarki
- Zabezpieczenie systemu przed działalnością szkodliwego oprogramowania (wirusy)

Zabezpieczenia i wymagania 2/2

- Zabezpieczenie przed włamaniem
- Mechanizmy raportujące ew. ataki na system
- Należy usunąć dane z tych elementów systemu, które będą podlegały konserwacji lub naprawie przez osoby trzecie
- Musi powstać instrukcja opisująca sposób działania systemu i realizacji wymogów ustawy

Przykłady rozwiązań technicznych 1/2

- Mechanizmy bezpieczeństwa
  - fizyczne (zamykana serwerownia)
  - systemowe (firewalle, routery, DMZ, kryptografia SSL, szyfrowanie backupów)
  - aplikacyjne (firewall aplikacyjny, reguły bezpieczeństwa, RBAC)
  - testy penetracyjne (np. OWASP top 10)
- Monitoring dostępu:
  - fizyczny (karty dostępowe, CCTV)
  - systemowy (logi serwera, IDS, Snort)
  - aplikacyjny (logi aplikacji, rotator logów)

Przykłady rozwiązań technicznych 2/2

- Dodatkowe mechanizmy:
  - reverse proxy (separacja serwera od sieci Internet)
  - IPS, adaptacyjne firewalle bazujące na IDS i firewallach aplikacyjnych (automatyczne wykrywanie zagrożeń)
  - analiza logów real-time (wykrywanie nietypowych zachowań w logach)
  - Honeypot (pułapka; symuluje prawdziwy serwer, śledzi działania hakerów i je blokuje)

Dziękujemy za uwagę

3e Internet Software House
Centrala w Warszawie
ul. Podbipięty 51
02-732 Warszawa
tel/fax: (+48) 22 822 48 68
email: info@3e.pl

www.3e.pl