Polityka Bezpieczeństwa EZD

Opracowanie Podlaski Urząd Wojewódzki w Białymstoku

I. Cel dokumentu

Celem dokumentu jest przedstawienie rekomendacji w zakresie zarządzania bezpieczeństwem funkcjonowania systemu Elektronicznego Zarządzania Dokumentacją (EZD) autorstwa Podlaskiego Urzędu Wojewódzkiego w Białymstoku.

Dokument stanowi wyłącznie rekomendację i jest dokumentem uzupełniającym Politykę Bezpieczeństwa Informacji (PBI) funkcjonującą w poszczególnych urzędach. PB EZD nie zastępuje PBI i powinien być adoptowany do specyficznych uwarunkowań urzędów, będąc w pełnej synchronizacji z PBI.

II. Zastosowane skróty i pojęcia

Nazwa	Objaśnienie
ŁUW	Łódzki Urząd Wojewódzki w Łodzi
EZD PUW	System Elektronicznego Zarządzania Dokumentacją autorstwa Podlaskiego Urzędu Wojewódzkiego w Białymstoku
ePUAP	Elektroniczna Platforma Usług Administracji Publicznej
Portal	Portal wsparcia EZD Support (portal.bialystok.uw.gov.pl)
RM	Patrz *Portal*
PBI	Polityka Bezpieczeństwa Informacji
PB EZD	Polityka bezpieczeństwa systemu EZD

III. Polityka bezpieczeństwa systemu informatycznego EZD

1) Infrastruktura sieci musi stanowić wydzieloną część dostępną tylko użytkownikom systemu.
2) Każda jednostka (stacja robocza, serwer) powinna posiadać oprogramowanie typu anty-wirus zabezpieczające przed wirusami i innymi atakami. Oprogramowanie anty-wirus powinno być aktualizowane na bieżąco.
3) Jednostka posiadająca system EZD powinna przestrzegać instalacji wszelkiego rodzaju oprogramowania w całej infrastrukturze. Jednostka powinna kontrolować i zezwalać na instalację tylko dozwolonego oprogramowania. Instalacja innego oprogramowania jest zabroniona.

4) Infrastruktura serwerów i stacji roboczej powinna być kontrolowana przez kontroler domeny.
5) Infrastruktura sieci instalacji EZD musi być wydzielona poza inne możliwe punkty dostępu przez osoby niepowołane. W szczególności powinna być wydzielona poza strefy bezpłatnego dostępu do internetu.
6) System EZD wymusza, aby proces logowania do systemu odbywał się tylko przez protokół HTTPS. Generowanie haseł przez inny protokół niż https narusza bezpieczeństwo i stwarza możliwość nieuprawnionego dostępu do haseł.
7) Dostęp do serwerów bazy danych musi być wydzielony tylko dla serwerów aplikacyjnych.
8) Dostęp do macierzy dyskowej, w której zapisywane są dane musi być ograniczony tylko do serwerów aplikacyjnych. Dostęp do macierzy dyskowej, w której zapisywane są załączniki dla systemu EZD musi posiadać dostęp tylko do operacji ZAPISu oraz ODCZYTu bez możliwości kasowania plików.
9) Uprawnienia na bazie danych dla systemu EZD powinny zostać ograniczone tylko do dostępu do bazy EZD.
10) Hasła dostępu do systemu EZD (poprzez kontroler domeny, bądź bezpośrednio w zależności od zastosowanych w urzędzie rozwiązań) muszą spełniać wymogi, co najmniej, Rozporządzenia Ministra Spraw Wewnętrznych i Administracji z dnia 29 kwietnia 2004 r. w sprawie dokumentacji przetwarzania danych osobowych oraz warunków technicznych i organizacyjnych, jakim powinny odpowiadać urządzenia i systemy informatyczne służące do przetwarzania danych osobowych. System EZD wymusza stosowanie silnych haseł. Wymogi silnego hasła stosowane w systemie EZD:
    1. Długość hasła min. 8 znaków
    2. Znaki z co najmniej 3 grup:
        a. Cyfry
        b. Duże litery
        c. Małe litery
        d. Znaki specjalne (! @ # $ % ^ & * ? _ ~ - ( ) { } ; :)
    3. Hasło musi być zmieniane co 30 dni.
    4. Hasło nie może być takie same jako poprzednio używane.
11) System zapisu załączników musi zapisywać na dwóch oddzielnych fizycznie nośnikach danych. Odpowiednie ustawienia administracyjne wskazują na podstawowe miejsce zapisu oraz na dodatkowe miejsca zapisu załączników z ostatnich 48 godzin.

12) System zapisu załączników wymusza, aby system backupów załączników uruchamiał się maksymalnie, co 48 godzin.
13) System backupów powinien archiwizować bazę danych raz na 24 godziny. Rekomenduje się, aby system backupów archiwizował logi transakcyjne, co godzinę. Zapewnia to utratę danych maksymalnie z ostatniej godziny funkcjonowania systemu.
14) Należy ograniczyć dostęp do plików konfiguracyjnych systemu EZD, w których przechowywane są, jawnym tekstem, informacje dostępowe do bazy danych (np. hasło, login, adres serwera bazy danych).
15) Dostęp do bazy danych wszystkich komponentów systemu EZD należy skonfigurować w trybie zintegrowanego uwierzytelniania (Integrated Security) w środowiskach, w których możliwe jest zastosowanie takiej autoryzacji, w celu pozbycia się przechowywania jawnie danych dostępowych (login, hasło) w plikach konfiguracyjnych.
16) Naturalne dokumenty elektroniczne doręczane do urzędu przez elektroniczne skrzynki podawcze powinny być dodatkowo zabezpieczane tak, by utrata tych plików była niemożliwa w przypadku awarii bazy danych plików.
17) System EZD zapisuje adresy IP przy każdej wykonywanej operacji.
18) Wykrycie potencjalnego wstrzykiwania/modyfikowania aplikacji może skutkować cofnięciem licencji na użytkowanie systemu EZD.
19) Należy poinformować użytkowników systemu EZD, że wszelkie próby naruszenia bezpieczeństwa systemu będą traktowane, jako atak na system EZD.
20) Należy poinformować użytkowników o konsekwencjach posiadania loginu i hasła dostępu do systemu. Należy zachować wszelkie formy bezpieczeństwa w przechowywaniu informacji o dostępie do systemu EZD.
21) Użytkownik systemu nie może wykonywać lub próbować wykonywać ataku na system EZD. Wprowadzanie niedozwolonych znaków oraz kombinacji znakowych świadczących o próbie złamania systemu jest zabronione.
22) Należy zabezpieczyć (ograniczyć) dostęp do kluczy prywatnych certyfikatów autoryzujących wykorzystywanych przez system EZD w komunikacji z ePUAP tylko dla aplikacji EZD oraz odpowiednio zabezpieczyć otrzymane pliki certyfikatów z Centrum Certyfikacji Ministerstwa Spraw Wewnętrznych, aby uniemożliwić ich wykorzystanie przez osoby nieuprawnione. Dostęp do kluczy prywatnych certyfikatu autoryzującego powoduje jednoczesny dostęp do kontekstu bezpieczeństwa podmiotu urzędu na ePUAP.