Wymagania dla systemów informatycznych pozyskiwanych przez NCBR - wyciąg

1. Dostęp użytkownika do systemu odbywa się z wykorzystaniem indywidualnego konta. Uwierzytelnienie w systemie odbywa się za pomocą hasła.
2. System wykorzystuje uwierzytelnienie domenowe lub wymusza konfigurowalną politykę haseł zapewniającą minimalną długość haseł, złożoność, niepowtarzalność oraz ich okresową zmianę
3. System nie wyświetla haseł podczas ich wprowadzania przez użytkownika.
4. System nie udostępnia użytkownikowi informacji o przyczynie błędu logowania.
5. Każda operacja w systemie objęta jest autoryzacją.
6. W przypadku aplikacji w architekturze klient-serwer uwierzytelnienie i autoryzacja odbywają się po stronie serwera. Realizacja uwierzytelnienia i autoryzacji po stronie urządzenia użytkownika (komputera, urządzenia mobilnego itp.) jest dopuszczalna wyłącznie w przypadku aplikacji działających lokalnie.
7. System zapewnia możliwość zdefiniowania uprawnień użytkowników z zapewnieniem możliwości przestrzeganie zasad minimalnych uprawnień i wiedzy uzasadnionej.
8. System nie ujawnia funkcjonalności lub danych, do których użytkownik nie ma dostępu.
9. Operacje związane z eksportem lub wysyłką danych, o ile są zaimplementowane w systemie, wymagają oddzielnych uprawnień.
10. Operacje związane z realizację czynności administracyjnych wymagają oddzielnych uprawnień.
11. System zapewnia ochronę sesji użytkowników przed przejęciem, adekwatnie do dobrych praktyk dla wykorzystywanej w systemie technologii.
12. Użytkownik pozwala użytkownikowi na nawiązanie jednej sesji z systemem, chyba, że możliwość nawiązania większej ilości sesji wynika z założeń funkcjonalnych systemu.
13. System zapewnia wygaszenie sesji użytkownika w chwili jego wylogowania.
14. System zapewnia wygaszenie sesji w przypadku bezczynności użytkownika.
15. Okres bezczynności skutkujący wygaszeniem sesji jest konfigurowalny.
16. Wymagania dotyczące zarządzania sesjami nie dotyczą połączeń bezstanowych niewymagających uwierzytelnienia użytkownika.
17. System przetwarza dane w minimalnym zakresie niezbędnym do realizacji celu przetwarzania.
18. System umożliwia korygowanie danych, chyba, że korekta nie jest dopuszczalna z uwagi na cel przetwarzania danych, w szczególności z uwagi na regulacje prawne.
19. System umożliwia usunięcie danych, chyba, że usunięcie nie jest dopuszczalne z uwagi na cel przetwarzania danych, w szczególności z uwagi na regulacje prawne
20. System zapewnia odnotowywanie zdarzeń związanych z udanym i nieudanym dostępem.
21. System zapewnia odnotowywanie nieudanych prób wykonania operacji.
22. System zapewnia odnotowywanie błędów.
23. Sposób zapisu logu zapewnia możliwość jego odczytania przez niezależny od systemu proces posiadający odpowiednie uprawnienia.
24. Prezentowane użytkownikom komunikaty o błędach nie mogą ujawniać wewnętrznych informacji dotyczących systemu.

25. System powinien móc pracować w środowisku zwirtualizowanym. Dopuszcza się wyjątki w przypadku, gdy system wykorzystuje aktywa nie podlegające wirtualizacji.
26. Wskazanie innych systemów, z którymi system się komunikuje odbywa się w oparciu o nazwy (FQDN), a nie adresy IP.
27. Wskazanie innych systemów występuje w plikach konfiguracyjnych lub w innych danych możliwych do konfiguracji.
28. W przypadku komunikacji z innymi systemami wymaga się:
    a. Zapewnienia wzajemnego uwierzytelnienia i autoryzacji wykonywanych operacji.
    b. Możliwości zmiany danych wykorzystywanych do uwierzytelnienia przy dostępie do innych systemów.
    c. Zapewnienia ograniczenia uprawnień innych systemów przy dostępie do danych i funkcji przedmiotowego systemu.
    d. Wskazania wykorzystywanych protokołów sieciowych i portów.
29. Komunikacja z systemem jest szyfrowana, przy czym wymaga się możliwości stosowania szyfrowania AES256, a w przypadku wykorzystania TLS stosowania protokołu w wersji 1.2 i 1.3. Dotyczy to zarówno komunikacji użytkownika z systemem, jak i komunikacji z innymi systemami.
30. W przypadku stosowania certyfikatów x.509 system pozwala na zmianę certyfikatu.
31. System posiada mechanizmy walidacji wprowadzanych danych pod kątem poprawności semantycznej adekwatnej do treści danych.
32. System powinien zapewniać przetwarzanie danych w formatach zgodnych z przepisami o Krajowych Ramach Interoperacyjności.
33. System posiada mechanizmy walidacji wprowadzanych danych pod kątem znanych ataków, adekwatnych do zastosowanej technologii.
34. Walidacja dotyczy wszystkich danych dostarczanych do systemu, z dowolnego źródła.
35. Dane walidowane są po stronie serwera. Lokalna walidacja dopuszczalna jest wyłącznie w przypadku aplikacji działających lokalnie. Ponadto dopuszcza się dodatkową lokalną walidację danych w celu informowania użytkownika o błędach wprowadzanych danych, ale mechanizm ten nie zastępuje walidacji po stronie serwera.
36. System pozwala na skanowanie antywirusowe danych importowanych ze źródeł zewnętrznych, których wielkość i charakter przetwarzania pozwala na ich wykorzystanie jako nośnika złośliwego oprogramowania. W szczególności dotyczy to plików oraz obiektów typu BLOB.
37. System jest odporny na próby naruszenia jego logiki, w tym w związku z przepływem roboczym i sekwencją realizowanych zadań.
38. System wykorzystuje oprogramowanie wspierane przez producenta.
39. System wykorzystuje stabilne i sprawdzone rozwiązania. W szczególności komponenty systemowe, takie jak serwery aplikacyjne, systemy zarządzania bazami danych itp., są wspierane przez producenta i nie są wersjami eksperymentalnymi.
40. System zapisuje dane w sposób umożliwiający ich odczytanie przez niezależny od systemu proces posiadający odpowiednie uprawnienia.
41. System nie może narzucać ograniczeń co do aktualizacji wykorzystywanego przez niego oprogramowania systemowego.
42. System zapewnia skalowalność, zarówno z uwagi na ilość użytkowników jak i z uwagi na ilość przetwarzanych danych.

43. System nie wykorzystuje komponentów o znanych podatnościach.