Załącznik nr X do OPZ

Wymagania w zakresie bezpieczeństwa

|  |  |  |
| --- | --- | --- |
| LP | Wymaganie | Model (roboczo) |
|  | System musi być tworzony zgodnie z zaleceniami standardu OWASP-ASVS poziom 2 (Open Web Application Security Project). | Standardy |
|  | System musi być tworzony zgodnie z zaleceniami standardu OWASP Testing Guide, a w szczególności OWASP - TOP 10 (Open Web Application Security Project). | Standardy |
|  | System musi spełniać wytyczne przedstawione w Rozporządzeniu Rady Ministrów z dnia 12 kwietnia 2012 r. w sprawie Krajowych Ram Interoperacyjności, minimalnych wymagań dla rejestrów publicznych i wymiany informacji w postaci elektronicznej oraz minimalnych wymagań dla systemów teleinformatycznych  (https://isap.sejm.gov.pl/isap.nsf/DocDetails.xsp?id=wdu20120000526). | Standardy |
|  | W zakresie bezpieczeństwa informacji system będzie spełniał wymagania normy PN-ISO/IEC 27001, PN ISO/IEC 27002, PN-ISO/IEC 27005. | Standardy |
|  | System musi mieć zsynchronizowany czas w oparciu o wiarygodny wzorzec czasu – serwer NTP wykorzystywany w Centrum. | Ogólne |
|  | System musi mieć możliwość ograniczenia korzystania tylko do jednej sesji jednocześnie dla danego użytkownika, chyba że używanie jednocześnie kilku lub więcej sesji dla danego pojedynczego użytkownika jest niezbędne w celu wykonania przypisanych mu zadań. | Sesje |
|  | System musi wymuszać zakończenie sesji po określonym czasie braku aktywności użytkownika | Sesje |
|  | Rozwiązanie powinno dostarczać mechanizmy związane z ochroną interfejsu WWW przed zakończeniem sesji oraz zewnętrznym dysponowaniem sesją Użytkownika (ataki typu „man in the middle"). | Sesje |
|  | System musi w odpowiedni sposób weryfikować błędy tak aby użytkownikowi końcowemu nie była prezentowana informacja o błędzie, zawierająca szczegóły techniczne wystąpienia tego błędu, ujawniające zastosowanie oprogramowania i jego konfigurację. Powinien być generowany standardowy, niezmienny komunikat o błędzie. | Weryfikacja danych |
|  | System musi w odpowiedni sposób weryfikować zawartość pól/formularzy aplikacji pod kątem wprowadzanych znak w (zastosowanej walidacji oraz kontroli poprawności składni zapytań), w celu zabezpieczenia przed atakami typu SQL Injection itd. | Weryfikacja danych |
|  | System musi zapewniać możliwość separowania uprawnień poprzez mechanizm aplikacyjny (logika aplikacji) uniemożliwiający realizację wybranych operacji przez jednego użytkownika. | Uprawnienia |
|  | System musi zapewniać udzielanie uprawnień użytkownik w poprzez profile/role grupujące pojedyncze uprawnienia. | Uprawnienia |
|  | System musi wspierać tryb pracy Mandatory Access Control (MAC) oparty na atrybutach bezpieczeństwa i politykach (na podstawie atrybut w i polityki udziela się bądź odmawia dostępu do obiektu). | Uprawnienia |
|  | System musi umożliwiać budowanie profili w oparciu o role użytkownik w uwzględniające:   1. dostęp do wskazanych funkcji w systemie; 2. rozdzielenia ról administracyjnych od biznesowych; 3. administratora bezpieczeństwa/audytora jako oddzielnego profilu; 4. zarządzanie prawami dostępu do danych na poziomie read/write/update/delete; 5. możliwość stworzenia unikalności identyfikator w użytkownika. | Uprawnienia |
|  | System musi w odpowiedni sposób weryfikować udostępnione przez daną aplikację usługi, tak aby dostępne były tylko niezbędne dla użytkownika zasoby, katalogi i pliki. | Uprawnienia |
|  | System musi zapewniać pełną identyfikowalność i rozliczalność wszystkich czynności użytkowników, administratorów Systemu:   1. udane/nieudane próby logowania z datą i czasem logowania/wylogowania, identyfikatorem użytkownika, nazwą stacji i adresem IP z którego nastąpiło logowanie; 2. próby nieautoryzowanego wejścia do systemu/aplikacji; 3. zmiany ustawień zabezpieczeń; 4. śledzenie działań użytkowników i administratorów, łącznie z śledzeniem działań w systemie/aplikacji. | Rozliczalność |
|  | Logi muszą zawierać informację o modyfikacjach związanych z zarządzaniem kontami i uprawnieniami, w szczególności dotyczące utworzenia, modyfikacji, zablokowania i usunięcia konta/grupy użytkownika oraz zmiany uprawnień użytkownika. | Rozliczalność |
|  | Dostęp do systemu musi być zabezpieczony kontem i hasłem. Hasła muszą spełniać poniższe wymagania:   1. hasła stosowane w systemie powinny być przechowywane w systemie zawsze w formie zaszyfrowanej, nie należy stosować haseł w postaci jawnej; 2. hasła muszą być budowane w sposób trudny do odgadnięcia i łatwy do zapamiętania, a jednocześnie utrudniać odszyfrowanie haseł za pomocą narzędzi do łamania haseł;   Hasła:   1. nie mogą zawierać ciągów znaków tworzących wyrazy słownikowe (np. imiona, nazwy roślin, zwierzęta itp.); 2. nie mogą zawierać ciągów znaków wynikających z układu znaków na klawiaturze (np. qwerty5, 2wsx#EDC, itd.); 3. nie mogą zawierać nazwy danego konta/loginu; 4. muszą się składać z co najmniej trzech grup znaków spośród następujących: wielkie litery A-Z, małe litery a-z, cyfry 0-9, znaki specjalne(!@#$ itd.); 5. minimalna zalecana długość hasła użytkowników - 8 znaków; 6. minimalna zalecana długość hasła kont specjalnych, technicznych 10 znaków; 7. hasła muszą być zmieniane okresowo.   Powyższe wymagania dotyczące haseł muszą być wymuszane przez oferowane rozwiązanie. | Hasła i konta |
|  | Wymagana częstotliwość wymuszenia zmiany haseł użytkowników wynosi 30 dni. Oferowane rozwiązanie musi umożliwiać definiowanie częstotliwości wymuszania zmiany haseł. | Hasła i konta |
|  | System musi pamiętać minimum 10 haseł wstecz, w tych systemach, które posiadają taką funkcjonalność, w celu uniemożliwienia zmiany hasła ponownie na to samo. | Hasła i konta |
|  | Rozwiązanie musi umożliwiać skonfigurowanie polityki blokowania kont (konto musi być zablokowane po max. 5 nieudanych pr bach logowania). Czas trwania blokady konta oraz ilość nieudanych prób po których następuje blokada konta musi być definiowalna przez administratora. | Hasła i konta |
|  | System musi wymuszać zmianę hasła przy pierwszym logowaniu oraz cyklicznie w trakcie eksploatowania. | Hasła i konta |
|  | Komunikacja z oprogramowaniem musi się odbywać z wykorzystaniem bezpiecznych protokołów tj. min. TLS 1.3 przy użyciu silnych algorytmów szyfrowania minimum AES 256 bits i długości klucza RSA 2048 bits.  Zamawiający dopuszcza wersję TLS 1.2 pod warunkiem poddania protokolu utwardzaniu po stronie Wykonawcy (wymagane jest  używanie szyfrów AES/GCM oraz ChaCha20-Poly130) | Komunikacja |
|  | Dane przesyłane do i z oferowanego rozwiązania muszą być przesyłane w sposób bezpieczny zapewniając przesyłanym danym integralność oraz poufność. | Komunikacja |
|  | System musi posiadać dokumentację powykonawczą opisującą wszystkie zastosowane mechanizmy bezpieczeństwa. Pozytywna ocena udokumentowanych mechanizmów bezpieczeństwa będzie jednym z warunków dopuszczenia systemu do produkcji. | Dokumentacja |
|  | Wykonawca dostarczy Zamawiającemu dokumentację administratora bezpieczeństwa tj. Zestaw dokumentacji szczegółowo opisującej zastosowane rozwiązania dotyczące spełniania wymagań ogólnych (zgodnie z wymaganiami prawa) oraz specyficznych zamawiającego dotyczących bezpiecznej eksploatacji. Dokumentacja, w szczególności, powinna zawierać:   1. opis zastosowanych mechanizmów ochrony przed naruszeniem zasad dostępu (poufności), integralności, niezaprzeczalności, wiarygodności oraz opis mechanizmów udostępniania, autoryzacji w tym autoryzacji operacji szczególnych; 2. opis zastosowanych mechanizmów logowania zdarzeń, śladu audytowego oraz kontroli i monitorowania działań w aplikacji/systemie w tym wszelkich prób naruszenia zasad bezpieczeństwa; 3. dokumentacja administratora aplikacji i administratora środowiska systemu opisująca szczegółowo funkcjonalności, interfejs oraz zasady zarządzania kontami (użytkownikami) oraz uprawnieniami poszczególnych ról, uprawnień, obiektów, profili, użytkowników itp.; 4. dokumentacja opisująca sposób realizacji wymagań wynikających z przepisów ustawy z dnia 10 maja 2018 r. o ochronie danych osobowych (Dz. U. z 2018r. poz. 1000) jeśli aplikacja przetwarza dane osobowe; 5. opis zabezpieczeń interfejsów oraz opis metod zapewnienia poufności i rozliczalności tych kanałów przepływu informacji jeśli aplikacja wykorzystuje jakiekolwiek mechanizmy wymiany informacji z innymi systemami; 6. dokumentacja z testów bezpieczeństwa aplikacji wykonanych przez Wykonawcę lub wykonanych przez niezależną firmę specjalistyczną. | Dokumentacja |
|  | Zamawiający zastrzega sobie prawo do przeprowadzenia audytu bezpieczeństwa aplikacji przed jej produkcyjnym uruchomieniem. Warunkiem dopuszczenia systemu do działania produkcyjnego będzie uzyskanie pozytywnych wyników audytu bezpieczeństwa. | Audyt |
|  | Wszystkie elementy rozwiązania (systemy operacyjny, bazy danych jak i aplikacje) muszą posiadać zainstalowane wszystkie dostępne i aktualne poprawki bezpieczeństwa. | Ogólne wymagania |
|  | Środowiska produkcyjne, testowe, developerskie muszą się znajdować w odrębnych strefach bezpieczeństwa odseparowanych poprzez firewall. | Sieć |
|  | System musi uniemożliwiać modyfikowanie i usuwanie logów systemowych, także przez Administratora systemu | Logi |
|  | System musi umożliwiać administratorowi przeglądanie historii logowania użytkowników. | Logi |
|  | Rozwiązanie musi posiadać możliwość przeglądania w oferowanym systemie czynności z działań użytkowników i administratorów oraz logów audytowych. | Logi |
|  | System musi zapewniać bezpieczny mechanizm przechowywania logów audytowych. | Logi |
|  | System musi umożliwiać przesyłanie informacji/logów/zdarzeń do zewnętrznego systemu korelacji logów systemu SIEM (Splunk). | Logi |
|  | System musi umożliwiać przesyłanie informacji/logów/zdarzeń do zewnętrznego systemu logów (syslog) np. poprzez REST API. | Logi |
|  | System musi umożliwiać archiwizację i odtwarzanie repozytorium danych. Czas odtworzenia pełnego rozwiązania z archiwum nie może przekraczać 12 godzin. | Kopie zapasowe |
|  | System musi umożliwiać jego rozwój (rozbudowę zakresu informacyjnego oraz zmiany w strukturze i merytoryce procesów zasilania) i utrzymanie przy wykorzystaniu własnych zasobów Centrum | Ogólne |
|  | System musi posiadać mechanizmy zabezpieczeń uniemożliwiające niepowołany dostęp do oferowanego rozwiązania oraz zabezpieczenia przed nieuprawnionym dostęp do danych oraz pozostałych moduł w aplikacji. | Ogólne |
|  | System musi umożliwiać zarządzanie kontami użytkowników co najmniej w zakresie:   1. zapewnienia unikalnych login w dla kont; 2. dodawania/edycji/zablokowania konta użytkownika (login, hasło, imię, nazwisko, email, telefon, adres); 3. spełnienia polityki bezpieczeństwa informatycznego Centrum, w tym polityki haseł; 4. wymuszenia natychmiastowej zmiany hasła; 5. przypisania użytkownika do struktury organizacyjnej i procesów. | Ogólne |
|  | System musi dawać możliwość pseudonimizacji, anonimizacji określonych danych oraz posiadać możliwość oznaczenia poszczególnych danych jako szczególne kategorie danych osobowych (dane wrażliwe) i dawać zróżnicowane możliwości dostępu do wskazanych danych. | Ogólne |
|  | System będzie zapewniać obsługę zapis transakcji wykonanych w bazie danych. | Bazy danych |
|  | Konfiguracja serwera webowego musi wymuszać ustawienie parametru httpOnly w cookies wysyłanych do użytkownika. | API |
|  | System musi posiadać udostępnione na zewnątrz interfejsy usług sieciowych.  W ramach wykorzystane powinny być wykorzystywane rozwiązania takie jak:   1. SOAP – w odniesieniu do przesyłania komunikatów, 2. OID – w odniesieniu do stosowania identyfikatorów, 3. XML – w odniesieniu do opisu struktur danych, 4. WSDL – w odniesieniu do opisu i specyfikacji usług, 5. SAML w wersji 2.0 lub wyższej – w odniesieniu do zarządzania tożsamością, 6. WS-Security – w odniesieniu do udostępnianych usług Web-Service, 7. WS-Policy – w odniesieniu do udostępnianych usług Web-Service, 8. WS-I Basic Profile – w odniesieniu do udostępnianych usług Web-Service, 9. WS-Addressing – w odniesieniu do udostępnianych usług web-service, 10. REST API - w odniesieniu do przesyłania komunikatów, 11. XACML w wersji 1.0 lub wyższej – w odniesieniu do polityki kontroli dostępu.   Ponadto system musi być gotowy na integracje przy użyciu standardowych mechanizm w integracji i komunikacji z systemami Zamawiającego:  - pliki w standardowych formatach (co najmniej CSV, JSON, XML, XLS, TXT),  - na poziomie baz danych (m.in. ODBC, JDBC, skrypty SQL),  - na poziomie wymiany poczty elektronicznej (protokół SMTP), | API |
|  | Integracja rozwiązania z użytkowanym przez Zamawiającego Active Directory umożliwiającą mechanizm SSO może odbyć się tylko za pośrednictwem rozwiązań takich jak ADFS lub inne narzędzie pośredniczące np. Keycloak. Zamawiający posiada wdrożoną usługę ADFS. | Logowanie |
|  | System musi zapewniać realizację w zakresie zasady rozliczalności w szczególności poprzez odnotowanie:   1. identyfikatora użytkownika wprowadzającego dane osobowe; 2. daty pierwszego wprowadzenia danych osobowych; 3. źródła danych, w przypadku zbierania danych nie od osoby, której one dotyczą; 4. nazwa i adres podmiotu, któremu przekazano dane ze wskazaniem charakteru przekazania (powierzenie, udostępnienie); 5. data udostępnienia/powierzenia danych; 6. zakres przekazywanych danych; 7. podstawa prawna przekazania; 8. nazwa komórki/jednostki/podmiotu przekazująceg dane; 9. numer pisma, na podstawie którego nastąpiło przekazanie; 10. imię i nazwisko osoby, która dane przekazała; 11. nazwa aplikacji, z której przekazano dane; 12. System musi zapewnić pełne zarządzanie danymi z uwagi na udzielanie zgodny na przetwarzanie danych osobowych; 13. numeru upoważnienia użytkownika do przetwarzania danych osobowych, przy czym numer upoważnienia musi być powiązany z zakresem uprawnień i ze zbiorem danych. | Dane osobowe |
|  | System musi zapewniać realizację zasad wynikających z rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (RODO)-przewidzianych w art. 5 RODO- np. jeżeli system przetwarza dane osobowe w więcej niż jednym celu, system musi umożliwiać przyporządkowanie danym osobowym celu przetwarzania | Dane osobowe |
|  | System musi umożliwiać realizację praw osoby, której dane dotyczą przewidzianych w RODO a w szczególności eksport danych osobowych dotyczących osoby, której dane są w systemie przetwarzane oraz informacji wynikających z art. 15 RODO w formie powszechnie i jednoznacznie zrozumiałej dla tej osoby (np. w postaci PDF) lub musi umożliwiać eksport danych osobowych dotyczących każdej osoby, której dane są w systemie przetwarzane, w powszechnie rozpoznawanym formacie (np. XML / XSD) – w przypadkach, gdy jest to uzasadnione celem przetwarzania. | Dane osobowe |
|  | System musi zapewniać możliwość definitywnego usunięcia danych osobowych. | Dane osobowe |
|  | System musi umożliwiać usunięcie całości danych dotyczących osoby. | Dane osobowe |
|  | System powinien rejestrować poniższe dane oraz udostępniać interfejs umożliwiający komunikację z innym systemami w zakresie danych dotyczących poszczególnych osób, w szczególności:   1. nazwa administratora danych; 2. cel przetwarzania; 3. zakres danych; 4. data wprowadzenia; 5. data importu danych oraz dane identyfikacyjne systemu źródłowego; 6. data i zakres eksportu danych oraz dane identyfikacyjne systemu docelowego; 7. data i zakres modyfikacji danych; 8. data wpływu żądania usunięcia danych; 9. data wpływu wycofania zgody na przetwarzanie; 10. data wpływu żądania sprostowania danych; 11. data i zakres sprostowania danych; 12. data wpływu żądania ograniczenia przetwarzania; 13. data i zakres ograniczenia przetwarzania; 14. data wpływu żądania dostępu do danych zgodnie z art. 15 RODO; 15. data realizacji żądania dostępu do danych zgodnie z art. 15 RODO; 16. data wpływu żądania przeniesienia danych; 17. data realizacji żądania przeniesienia danych; 18. dane podmiotu, do którego dane osobowe zostały przeniesione; 19. data wpływu żądania niepodlegania zautomatyzowanemu przetwarzaniu danych; 20. data realizacji żądania niepodlegania zautomatyzowanemu przetwarzaniu danych; 21. data i forma spełnienia obowiązków informacyjnych; 22. data wpływu sprzeciwu wobec przetwarzania danych; 23. data realizacji sprzeciwu wobec przetwarzania danych; 24. data cofnięcia zgody na przetwarzanie; 25. data wpływu i dane dotyczące skargi do organu nadzorczego; 26. data i zakres przekazania danych do państwa trzeciego lub organizacji międzynarodowej (jeżeli ma zastosowanie); 27. planowany termin usunięcia poszczególnych kategorii danych. | Dane osobowe |
|  | System powinien składować dane w postaci zaszyfrowanej. | Składowanie danych |
|  | Minimalnym akceptowanym algorytmem asymetrycznym jest RSA 2048. | Składowanie danych |
|  | Minimalnym akceptowanym algorytmem symetrycznym jest AES 128. | Składowanie danych |
|  | Minimalnym akceptowanym standardem funkcji skrótu jest SHA-2. | Składowanie danych |