**Załącznik nr 2 - Wymagania techniczne i proceduralne** **dla systemu**

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **Lp.** | **Wymaganie** | **System spełnia\*** | **System może spełniać\*** | **Nie ma możliwości dostosowana systemu do wymogu\*** | **Uwagi/Wycena\*\*** |
| **I.** | **Wymagania dla systemu** |  |  |  |  |
| 1. | System musi zapewniać ochronę przed aktualnie występującymi zagrożeniami dla serwisów internetowych oraz musi uwzględniać zalecenia konfiguracyjne i programistyczne, w szczególności producentów sprzętu i oprogramowania („best practice”) w tym wytyczne organizacji OWASP (Application Security Verification Standard 4.0.1 na poziomie minimum 1 (Level 1)). |  |  |  |  |
| 2. | Dostęp do systemu wyłącznie w oparciu o szyfrowane połączenia TLS 1.2 lub nowszy oraz zaufane certyfikaty SSL dostarczone przez zamawiającego lub wykonawcę. |  |  |  |  |
| 3. | Zasady dotyczące uwierzytelniania: |  |  |  |  |
| 3.1 | proces uwierzytelniania powinien być poprzedzony komunikatem o konsekwencjach nieautoryzowanego dostępu; |  |  |  |  |
| 3.2. | system powinien mieć możliwość definiowania granularnych uprawnień dostępu zarówno do modułów, jak i do danych; |  |  |  |  |
| 3.3. | brak możliwości pominięcia procesu uwierzytelniania do systemu; |  |  |  |  |
| 3.4. | wymuszenie użycia indywidualnych loginów i haseł (w przypadku zastosowania uwierzytelnienia jednoskładnikowego) oraz zapewnienia rozłączalności żądań dostępu do systemu; |  |  |  |  |
| 3.5. | wprowadzanie hasła do systemu w postaci uniemożliwiającej jego bezpośrednie odczytanie - hasło nie może być widoczne podczas wpisywania go na ekranie w formie jawnej; |  |  |  |  |
| 3.6. | realizacja procesu uwierzytelniania, powinna ujawniać jak najmniej informacji w trakcie swojego przebiegu, tak aby nie pozwolić nieuprawnionemu użytkownikowi na uzyskanie dodatkowych wskazówek, np. brak wyświetlania identyfikatora ostatniego zalogowanego użytkownika, brak informacji o typie błędu przy uwierzytelnianiu, czyli brak informacji, iż użytkownik podał błędne hasło - powinna być wyświetlana ogólna informacja, że nazwa użytkownika lub hasło są nieprawidłowe (dopuszcza się informowanie o wciśniętym klawiszu Caps Lock); |  |  |  |  |
| 3.7. | możliwość blokowania konta po określonej ilości nieudanych prób logowania do systemu; |  |  |  |  |
| 3.8. | brak możliwości pojawienia się hasła w postaci jawnej, zaszyfrowanej lub odcisku w logach procesu uwierzytelnienia; |  |  |  |  |
| 3.9. | możliwość wyboru i zmiany hasła oraz zawarcie mechanizmu pozwalającego na potwierdzanie zmiany hasła dla uniknięcia błędów przy ich wprowadzaniu; |  |  |  |  |
| 3.10. | możliwość okresowego wymuszania zmiany haseł, w tym wymuszanie zmiany haseł tymczasowych przy pierwszym zalogowaniu; |  |  |  |  |
| 3.11. | udostępnienie mechanizmu wymuszającego kontrolę złożoności haseł obejmujących:   * + - minimalną długość hasła;     - minimalny i maksymalny czas ważności hasła;     - historię haseł (zapobieganie ponownemu użyciu tych samych haseł);     - wymaganie istnienia w haśle znaków spośród następujących grup: małe litery, duże litery, cyfry, znaki specjalne;     - definiowanie odrębnych zasad dla zwykłych użytkowników i użytkowników z uprawnieniami administracyjnymi. |  |  |  |  |
| 4. | Dane osobowe (w zakresie uzgodnionym na wdrożeniu) i hasła na każdym etapie wykorzystania i przesyłania muszą być szyfrowane i nie mogą występować w postaci jawnej. Dla haseł należy zastosować algorytmy minimum SHA-2 z solą, BCrypt czy PBKDF2. |  |  |  |  |
| 5. | System powinien posiadać wbudowane dzienniki systemowe, w których zapisywane będą w pełni automatycznie, bez możliwości modyfikacji i zablokowania, wszystkie istotne działania użytkowników/systemu takie jak:   * + wszystkie udane i nieudane logowania;   + przyznanie/odebranie/zmianę uprawnień w systemie;   + rejestrację wszelkich zmian w parametrach/konfiguracji systemu;   + rejestrację działań administratora zgodnie z wymaganiami Rozporządzenia KRI (Dz.U. z 2017 r. poz. 2247),   + wyświetlanie określonych danych przez określonego użytkownika (np. zapisanie zapytania w taki sposób aby można było odtworzyć wynik);   + Minimum zapisywanych parametrów w dziennikach dla konkretnego zdarzenia:   + data, czas;   + nazwa użytkownik;   + rodzaj operacji;   + wskazanie danych/informacje o rekordzie. |  |  |  |  |
| 6. | System powinien logować działania użytkowników pozwalające m. in. na:   * + ustalenie, który użytkownik dokonał zmiany danych osobowych (z pierwszym wpisem włącznie);   + ustalenie, jakie dane osobowe zostały zmienione przez użytkownika (zakres zmiany);   + ustalenie, jakie były poprzednie wartości danych osobowych (informacja historyczna);   + wygenerowanie raportu nt. zakresu przetwarzania danych osobowych;   + ustalenie źródła pochodzenia każdej danej osobowej;   + ustalenie daty pierwszego wprowadzenia danych osobowych do systemu oraz identyfikatora użytkownika wprowadzającego dane osobowe do systemu. |  |  |  |  |
| 7. | System powinien umożliwiać trwałe usuwanie danych osobowych albo ich anonimizację/pseudonimizację na żądanie lub po upływie okresu ich przechowywania. |  |  |  |  |
| 8. | System powinien umożliwiać wyszukanie wszystkich danych osobowych po zadanych parametrach. |  |  |  |  |
| 9. | System powinien posiadać możliwość eksportu logów w formacie umożliwiającym ich odczyt maszynowy np. txt, csv, CEF, JSON lub możliwość automatycznego przekazywania logów do zewnętrznych systemów monitorujących np. protokołem syslog. |  |  |  |  |
| 10. | System powinien zapewniać walidację wprowadzanych plików pod kątem ich typu i blokować pliki w formatach innych niż zdefiniowane w systemie. |  |  |  |  |
| 11. | System powinien być stworzony zgodnie ze standardami w oparciu o mechanizmy ułatwiające osobom z niepełnosprawnościami dostęp do publikowanych treści - zgodnie z ustawą z dnia 19 lipca 2019 r. o zapewnianiu dostępności osobom ze szczególnymi potrzebami (Dz. U. z 2022 r., poz. 2240 ) oraz ustawą z dnia 4 kwietnia 2019 r. o dostępności cyfrowej stron internetowych i aplikacji mobilnych podmiotów publicznych (Dz.U. z 2022 r. poz. 1002). |  |  |  |  |
| **III** | **Wymagania proceduralne** |  |  |  |  |
| 1. | Zadania muszą być realizowane zgodnie z wymaganiami SZBI, w szczególności w zakresie: |  |  |  |  |
| 1.1. | Zarządzania uprawnieniami – prowadzenie rejestru uprawnień, nadawanie uprawnień na podstawie wniosków o nadanie uprawnień. |  |  |  |  |
| 1.2. | Prowadzenie rejestru awarii, dziennika administratora systemu. |  |  |  |  |
| 1.3. | Bieżąca aktualizacja systemu, systemu operacyjnego serwera, baz danych, serwera www, aplikacji biznesowej, itp. – w razie wykrycia w nim błędów bezpieczeństwa lub innych nieprawidłowości oraz wydania nowych stabilnych wersji oprogramowania, poprawek do oprogramowania. |  |  |  |  |
| 1.4. | Podejmowanie działań mających zapobiegać incydentom bezpieczeństwa informacji w tym wdrażanie zaleceń zamawiającego (np. blokowanie złośliwego ruchu na podstawie przekazanych IoC), niezwłocznie, nie później niż w ciągu 4 godzin od jego wykrycia, informowanie zamawiającego na adres incydent@mrips.gov.pl o incydencie bezpieczeństwa mogącym mieć wpływ na działanie systemu. Zakres przekazywanych informacji w zgłoszeniu wynika z aktualnie obowiązujących przepisów prawa. |  |  |  |  |
| 1.5. | Wykonywanie backupów systemu zgodnie harmonogramem ustalonym z zamawiającym. |  |  |  |  |
| 1.6. | Wykonanie i aktualizacja dokumentacji technicznej systemu. |  |  |  |  |
| 1.7. | Gromadzenia i archiwizowania logów z systemów bezpieczeństwa, serwera i systemu za okres co najmniej 6 miesięcy wstecz oraz przesyłania ich raz dziennie na wskazany przez Zamawiającego serwer SFTP. Na żądanie Zamawiającego Wykonawca niezwłocznie zobowiązany będzie do przekazania logów z systemu UTM, serwera i systemu za wskazany okres. |  |  |  |  |
| 1.8. | Bieżący monitoring działania systemu. |  |  |  |  |
| 1.9. | Administrowanie wszystkimi serwerami powinno odbywać się zdalnie z siedziby Wykonawcy poprzez bezpieczne szyfrowane połączenie. |  |  |  |  |
| 1.10. | Czas skutecznej naprawy usterki, o której mowa w pkt 9 podpunkt 10 rozdziału XII zapytania ofertowego, będzie wynosić ……… godzin od momentu potwierdzenia zgłoszenia. |  |  |  |  |

\* Proszę wskazać wpisując znak „X” we właściwą kolumnę ( „system spełnia” lub „system może spełniać” lub „nie ma możliwości dostosowania systemu do wymogu”).

\*\* Proszę o uzupełnienie w przypadku, gdy dany wymóg może zostać spełniony, jednak wiąże się to z określonymi dodatkowymi warunkami lub kosztami. Jeżeli implikuje to dodatkowe koszty, proszę o orientacyjne ich określenie. Proszę również o wskazanie, jeżeli w przypadku określonego systemu nie ma konieczności spełnienia takiego wymogu i dlaczego.