ZALECENIA BEZPIECZEŃSTWA SYSTEMU SEKAFI3 SQL

WYMAGANIA NA DZIEŃ 25/05/2018

Wydawca oprogramowania nie gwarantuje poprawności pracy oprogramowania, gdy nie jest ono aktualne. Ważność certyfikatu gwarancji zapewnia użytkownikowi dostęp do aktualnych wersji. Każda kopia programu opublikowana przez wydawcę jest podpisana kluczem cyfrowym. Certyfikat podpisu potwierdza autentyczność oraz gwarantuje, że aplikacja nie została zmodyfikowana przez kogoś innego.

W przypadku, gdy użytkownik nie posiada ważnego certyfikatu gwarancji, jego dane nie są bezpieczne, a oprogramowanie może posiadać wady, które nie były znane w czasie, w którym dana wersja programu została wydana. Aktualizacja oprogramowania jest możliwa tylko w okresie ważności certyfikatu gwarancji.

WYMAGANIA OGÓLNE

1. Wymagana wersja aplikacji minimum 3.0.632.1 z dnia 23-05-2018 lub nowsza
2. Stała aktualizacja oprogramowania do bieżącej wersji
3. System operacyjny Windows posiadający ważne wsparcie producenta. System operacyjny musi być aktualny (zainstalowane wszystkie aktualizacje krytyczne oraz opcjonalne dotyczące certyfikatów).
   Lista systemów nie wspieranych: Windows XP, Windows Vista (na tych systemach operacyjnych nie są testowane nowe wersje programu, a wcześniejsze testy wykazały braki zgodności w komunikacji z zewnętrznymi systemami).
4. Serwer bazy danych Firebird
   a. wersja tylko stabilna z serii 2.5.X minimum 2.5.7 (nie wolno używać wersji beta)
   b. nie należy używać wersji starszych: 1.X, 2.0 oraz 2.1 (grozi to uszkodzeniem bazy danych)
   c. nie wolno używać wersji nowszych, nieprzetestowanych, które nie zostały dopuszczone przez wydawcę (nowe wersje mogą nie posiadać aktualnie używanych funkcjonalności lub zostały one zmodyfikowane tak, że wymagają modyfikacji kodu programu bądź raportów)
   d. wersja klienta Firebird zainstalowanego na stacji roboczej powinna być zgodna z wersją na serwerze
   e. wersja klienta powinna być z narzędziami deweloperskimi – umożliwiająca wykonanie kopii bazy danych
5. Przy korzystaniu z systemu na kilkunastu stanowiskach wydawca zaleca wykorzystania w tym celu serwera na platformie Linux CentOS 7 (niskie koszty, bardzo duża stabilność i wydajność)

6. W przypadku serwera bazy danych opartego o środowisko OS Windows:
   a. zalecana wersja systemu Windows serwerowa lub PRO (nie zaleca się wersji Home)
   b. Wyłączona hibernacja systemu (tryb uśpienia)
   c. wyłączone usypianie dysków twardych
   d. niezalecana konfiguracja: laptop z zainstalowanym serwerem bazy danych i praca z baterii

7. Nie zaleca się aby serwerem bazy danych był zwykły komputer klasy desktop bez zabezpieczeń dostępnych dla platform serwerowych:
   a. Dyski twarde montowane wewnątrz obudowy bez sygnalizacji monitorującej stan dysku
   b. Brak HOT SWAP – możliwość wymiany uszkodzonego dysku na sprawny bez konieczności zatrzymywania systemu.
   c. Brak drugiego zasilacza, gdzie każdy z zasilaczy jest podłączony do innego UPS-a. W przypadku awarii zasilacza bądź UPS w takiej konfiguracji istnieje możliwość nieprzerwanej pracy oraz stosunkowo niskie prawdopodobieństwo utraty danych (nie zawsze musi być to duży wydatek, gdyż często serwer poleasingowy kosztuje tyle co nowa stacja robocza).

8. Na serwer bazy danych nie powinny mieć dostępu osoby nieuprawnione.

9. Nośnik danych (dysk), na którym przechowywana jest baza danych powinien być bezpieczny. Aby ochronić się przed utratą danych zaleca się stosowanie macierzy RAID, która w najprostszej wersji RAID 1 – mirror (kopia lustrzana dysku) pozwala stworzyć lustrzaną kopię dysku. W takiej sytuacji w przypadku awarii jednego dysku system nadal pracuje korzystając z kopii danych zawartych na drugim dysku.
   Nie jest także wskazane stosowanie dysków wyeksploatowanych wieloletnią pracą w innym miejscu. Zaleca się stosowanie nowych dysków gwarantujących bezpieczniejszą pracę.

WYMAGANIA DOTYCZĄCE BAZY DANYCH

1. Baza danych nie powinna znajdować się na stacji roboczej, na której uruchamiany jest program SEKAFI.

2. Folder zawierający bazę danych nie może być udostępniany w sieci, gdyż w wyniku działań niezamierzonych, mogłoby dojść do utraty danych, np. w wyniku działania szkodliwego oprogramowania bądź działania osób trzecich.

3. Hasło do bazy danych powinno być zmienione na inne niż domyślne.

4. Komunikacja z bazą odbywa się za pomocą protokołu TCP/IP poprzez port 3050, dlatego należy pamiętać, aby na serwerze, na którym znajduje się baza danych ten port był odblokowany w ustawieniach Zapory systemu. W celu poprawy bezpieczeństwa zaleca się, aby na serwerze ilość odblokowanych portów była ograniczona do minimum.

5. Metody zabezpieczenia programu:
   a. Klucz sprzętowy HASP lub NetHASP uniemożliwia łatwy dostęp do kopii bazy danych (niski poziom ryzyka dostępu osób niepowołanych do kopii danych), gdyż aby uruchomić program konieczne jest podłączenie klucza.

b. Metoda na numer NIP umożliwia łatwy oraz niczym nieograniczony dostęp do każdej kopii bazy (wysoki poziom ryzyka dostępu osób niepowołanych do kopii danych), gdyż do uruchomienia programu na kopii bazy niepotrzebna jest żadna dodatkowa metoda autoryzacji.

6. W konfiguracji połączenia klienta z bazą danych należy wskazać fizyczne miejsce bazy danych na serwerze.
   Zdarzało się w trakcie pomocy u niektórych klientów, że stacje robocze miały wpisaną lokalizację podmontowanego dysku zewnętrznego, a na stacji roboczej zainstalowany był serwer Firebird – takie zachowanie jest niedopuszczalne).

7. Serwer powinien posiadać stały adres w sieci.

8. Kopie bazy wykonywane z poziomu Sekafi są szyfrowane, dlatego za pomocą funkcjonalności SEKAFI należy:
   a. utworzyć własny klucz szyfrujący do szyfrowania kopii bazy
   b. zapisać klucz w postaci bezpiecznej (będzie potrzebny do odszyfrowania kopii bazy).
   Nikt, nawet dostawca oprogramowania, nie jest w stanie odszyfrować kopii bezpieczeństwa danych użytkownika bez znajomości klucza szyfrującego.

9. Kopia bazy danych powinna być wykonywana na koniec każdego dnia pracy i przechowywana na innym zewnętrznym nośniku niż dysk, na którym znajduje się baza danych.

10. Wszystkie wykonywane kopie bazy danych powinny być zaszyfrowane, aby osoby nieuprawnione nie miały możliwości ich wypakowania.

11. Należy przechowywać kopię bazy w innym bezpiecznym miejscu niż serwerownia.

12. Dla użytkowników Sekafi posiadających ważny certyfikat gwarancji został udostępniony bezpieczny zasób cloud.sekafi.pl, na którym mogą być przechowywane kopie bezpieczeństwa.

WYMAGANIA DOTYCZĄCE OPERATORÓW

1. Nie należy udostępniać możliwości logowania na koncie Administratora podczas normalnej pracy w systemie.

2. Zaleca się ustawienie wymuszania zmiany hasła co określoną ilość dni.

3. Hasło powinno być bezpieczne (system ma możliwość generowania odpowiednich ciągów znaków).

4. Użytkownik (każdy operator) ma możliwość wykonania kopii bezpieczeństwa na swojej stacji roboczej (kopia jest bezpieczna gdyż zawartość archiwum jest zaszyfrowana).

5. Powinno się wyłączać dostęp osobom, które już nie pracują bądź utraciły prawa dostępu do przetwarzania danych.