



mMedica

Dobre praktyki zabezpieczenia
dostępu do bazy danych

Spis treści

1. OPIS.....	3
2. SYSTEM OPERACYJNY.....	3
2.1. DEDYKOWANY SERWER BAZY DANYCH	3
2.2. DOPUSZCZALNE DODATKOWE USŁUGI.....	3
2.3. OGRANICZENIE DOSTĘPU SIECIOWEGO.....	3
2.4. REGULARNA AKTUALIZACJA SYSTEMU OPERACYJNEGO	3
2.5. ZASADA NAJMNIEJSZYCH UPRAWNIENÍ	3
2.6. SZYFROWANIE POŁĄCZEŃ	3
2.7. SILNE UWIERZYTELNIANIE I ZARZĄDZANIE HASŁAMI	4
2.8. REGULARNY PRZEGLĄD KONT I UPRAWNIENÍ	4
2.9. OGRANICZENIE DOSTĘPU ADMINISTRACYJNEGO	4
2.10. OCHRONA PRZED ATAKAMI TYPU BRUTE FORCE	4
2.11. SYNCHRONIZACJA CZASU.....	4
2.12. OCHRONA PRZED ZŁOŚLIWYM OPROGRAMOWANIEM.....	4
2.13. DOKUMENTOWANIE ZMIAN KONFIGURACYJNYCH.....	4
2.14. UWIERZYTELNIANIE WIELOSKŁADNIKOWE (MFA)	4
2.15. SZYFROWANIE DANYCH PRZECZOWYWANYCH	4
2.16. MONITORING INFRASTRUKTURY	5
2.17. AUDYTY BEZPIECZEŃSTWA I SKANOWANIE PODATNOŚCI.....	5
3. SIEĆ	5
3.1. SEGMENTACJA SIECI	5
3.2. OGRANICZENIE DOSTĘPU SIECIOWEGO.....	5
4. BAZA DANYCH	5
4.1. WYKONYWANIE I WERYFIKACJA KOPII ZAPASOWYCH	5
4.2. REPLIKACJA BAZY DANYCH	5
4.3. LOGOWANIE I ANALIZA ZDARZEŃ	5
4.4. TESTOWANIE PROCEDUR ODTWORZENIOWYCH.....	6
4.5. PLAN CIĄGŁOŚCI DZIAŁANIA I PLAN ODTWORZENIA PO AWARII	6
4.6. RETENCJA I ARCHIWIZACJA LOGÓW	6

1. Opis

Niniejszy dokument opisuje rekomendacje dotyczące zabezpieczeń bazy danych.

2. System operacyjny

2.1. Dedykowany serwer bazy danych

Serwer bazy danych powinien być zainstalowany na przeznaczonym wyłącznie do tego celu serwerze. Nie należy instalować na nim dodatkowych usług, takich jak serwer WWW, serwer pocztowy czy inne systemy niezwiązane z obsługą bazy danych. Należy pozostawić otwarty wyłącznie port przychodzący wykorzystywany przez PostgreSQL oraz niezbędne porty wychodzące służące do aktualizacji systemu operacyjnego i monitoringu. Konfiguracja powinna zostać wykonana na poziomie systemu operacyjnego i/lub zapory sieciowej. Brak odpowiedniej segmentacji zwiększa ryzyko nieautoryzowanego dostępu do serwera.

2.2. Dopuszczalne dodatkowe usługi

Dopuszcza się zainstalowanie na serwerze z bazą danych usługi mmService. W takim przypadku należy ograniczyć ruch wychodzący wyłącznie do systemów i usług wymaganych do prawidłowego działania mmService.

2.3. Ograniczenie dostępu sieciowego

Konfiguracja PostgreSQL powinna umożliwiać połączenia wyłącznie z zaufanych hostów poprzez odpowiednią konfigurację pliku `pg_hba.conf`. Dodatkowo zaleca się filtrowanie ruchu przy pomocy zapory sieciowej lub mechanizmów systemu operacyjnego. Dostęp z niezaufanych hostów może umożliwić przeprowadzenie prób nieautoryzowanego dostępu.

hostssl	all	all	127.0.0.1/32	md5	clientcert=verify-ca
hostssl	all	all	:::1/128	md5	clientcert=verify-ca
hostssl	replication	all	192.168.1.123/32	md5	clientcert=verify-ca
hostssl	POZ	all	10.25.0.0/16	md5	clientcert=verify-ca
hostssl	AOS	all	10.26.0.0/16	md5	clientcert=verify-ca

2.4. Regularna aktualizacja systemu operacyjnego

System operacyjny powinien być utrzymywany w aktualnej, wspieranej wersji. Aktualizacje bezpieczeństwa powinny być wdrażane niezwłocznie po ich opublikowaniu i przetestowaniu. Brak aktualizacji może prowadzić do wykorzystania znanych podatności bezpieczeństwa.

2.5. Zasada najmniejszych uprawnień

Każdy użytkownik, aplikacja i usługa powinny posiadać wyłącznie uprawnienia niezbędne do realizacji swoich zadań. Konta administracyjne powinny być wykorzystywane jedynie do czynności administracyjnych. Ograniczenie uprawnień minimalizuje skutki ewentualnego przejęcia konta lub błędnej konfiguracji.

2.6. Szyfrowanie połączeń

Wszystkie połączenia z bazą danych są realizowane z wykorzystaniem protokołu SSL/TLS. Szyfrowanie transmisji chroni dane przed przechwyceniem podczas przesyłania przez sieć. W przypadku podejrzenia ujawnienia lub wykradzenia klucza prywatnego należy niezwłocznie wygenerować nową parę kluczy, wymienić certyfikat oraz zaktualizować konfigurację wszystkich systemów korzystających z danego połączenia.

2.7. Silne uwierzytelnianie i zarządzanie hasłami

Należy stosować silne hasła zgodne z polityką bezpieczeństwa organizacji. Hasła powinny posiadać odpowiednią długość i złożoność. Konta domyślne, nieużywane lub testowe powinny być usuwane lub blokowane.

2.8. Regularny przegląd kont i uprawnień

Należy okresowo przeprowadzać przegląd wszystkich kont użytkowników oraz nadanych im uprawnień. Konta nieużywane, tymczasowe lub należące do osób, które utraciły uprawnienia dostępu, powinny zostać niezwłocznie usunięte lub zablokowane.

2.9. Ograniczenie dostępu administracyjnego

Dostęp administracyjny do serwera powinien być możliwy wyłącznie z określonych adresów IP, sieci administracyjnych lub za pośrednictwem VPN. Wszystkie działania administracyjne powinny być rejestrowane i podlegać audytowi.

2.10. Ochrona przed atakami typu brute force

Należy wdrożyć mechanizmy wykrywania i blokowania wielokrotnych nieudanych prób logowania, zarówno na poziomie systemu operacyjnego, jak i infrastruktury sieciowej.

2.11. Synchronizacja czasu

Serwery powinny korzystać z zaufanych źródeł czasu (NTP). Prawidłowa synchronizacja czasu jest niezbędna do prowadzenia analizy logów, audytów bezpieczeństwa oraz diagnostyki incydentów.

2.12. Ochrona przed złośliwym oprogramowaniem

Serwer powinien być zabezpieczony przed uruchamianiem nieautoryzowanego oprogramowania. Zaleca się stosowanie mechanizmów typu EDR/XDR lub innych rozwiązań monitorujących aktywność systemu i wykrywających potencjalne zagrożenia.

2.13. Dokumentowanie zmian konfiguracyjnych

Wszelkie zmiany konfiguracji systemu operacyjnego, PostgreSQL, reguł sieciowych oraz uprawnień powinny być dokumentowane i podlegać procedurze zarządzania zmianą. Ułatwia to analizę incydentów oraz odtworzenie konfiguracji.

2.14. Uwierzytelnianie wieloskładnikowe (MFA)

Jeżeli jest to technicznie możliwe, dostęp administracyjny do serwerów, systemów zarządzania oraz rozwiązań VPN powinien być zabezpieczony uwierzytelnianiem wieloskładnikowym (MFA), co znacząco ogranicza ryzyko przejęcia kont uprzywilejowanych.

2.15. Szyfrowanie danych przechowywanych

W przypadku przetwarzania danych wrażliwych zaleca się stosowanie szyfrowania dysków, woluminów oraz kopii zapasowych. Zabezpiecza to dane przed odczytem przez osoby nieuprawnione w przypadku utraty lub kradzieży nośników.

2.16. Monitoring infrastruktury

Należy monitorować stan serwera, wykorzystanie procesora, pamięci operacyjnej, przestrzeni dyskowej, wydajność PostgreSQL oraz dostępność usług. Monitoring powinien generować automatyczne alerty w przypadku wykrycia nieprawidłowości.

2.17. Audyty bezpieczeństwa i skanowanie podatności

Zaleca się regularne przeprowadzanie audytów bezpieczeństwa oraz skanów podatności serwera, systemu operacyjnego i PostgreSQL. Wykryte podatności powinny być analizowane i usuwane zgodnie z przyjętą procedurą zarządzania ryzykiem.

3. Sieć

3.1. Segmentacja sieci

Serwer bazy danych powinien znajdować się w wydzielonej strefie sieciowej, do której dostęp mają wyłącznie autoryzowane systemy aplikacyjne i administratorzy. Ogranicza to możliwość przemieszczania się atakującego pomiędzy segmentami sieci.

3.2. Ograniczenie dostępu sieciowego

Serwer powinien mieć ograniczony dostęp również na poziomie sieci. Zarówno ruch przychodzący jak i wychodzący powinien być filtrowany.

4. Baza danych

4.1. Wykonywanie i weryfikacja kopii zapasowych

Należy regularnie wykonywać kopie zapasowe bazy danych oraz przechowywać je na odrębnym nośniku lub w odseparowanej lokalizacji. Zmniejsza to ryzyko utraty danych w wyniku awarii sprzętu, błędów administracyjnych, ataków ransomware lub celowego uszkodzenia danych. Kopie zapasowe powinny być regularnie weryfikowane pod kątem poprawności wykonania i możliwości odtworzenia.

4.2. Replikacja bazy danych

Zaleca się wdrożenie replikacji PostgreSQL. Serwer replikacyjny stanowi kopię serwera podstawowego i może zostać wykorzystany w przypadku jego awarii. Pozwala to ograniczyć przestoje systemu oraz zminimalizować ryzyko utraty danych.

4.3. Logowanie i analiza zdarzeń

Należy włączyć logowanie zdarzeń PostgreSQL, w szczególności logowanie połączeń, rozłączeń, błędów, nieudanych prób logowania oraz wolno wykonywanych zapytań. Logi powinny podlegać regularnej analizie automatycznej lub ręcznej w celu wykrywania anomalii, prób nieautoryzowanego dostępu oraz problemów wydajnościowych.

```
log_connections = on
log_disconnections = on
log_min_duration_statement = 500
```

4.4. Testowanie procedur odtworzeniowych

Należy regularnie przeprowadzać testy odtwarzania kopii zapasowych oraz procedur awaryjnego przełączenia na serwer replikacyjny. Pozwala to potwierdzić skuteczność planów ciągłości działania.

4.5. Plan ciągłości działania i plan odtworzenia po awarii

Dla środowiska bazodanowego powinien zostać opracowany oraz okresowo testowany plan ciągłości działania (BCP) oraz plan odtworzenia po awarii (DRP). Dokumentacja powinna określać maksymalny dopuszczalny czas niedostępności usługi oraz akceptowalny poziom utraty danych.

4.6. Retencja i archiwizacja logów

Logi systemowe, bazodanowe oraz bezpieczeństwa powinny być przechowywane przez okres zgodny z polityką organizacji lub wymaganiami prawnymi. Powinny być zabezpieczone przed modyfikacją i nieautoryzowanym usunięciem.