

Informacje i instrukcje dla użytkownika

Dokument jest przeznaczony dla administratorów, integratorów i operatorów systemów alarmowania. Określa zasady ochrony dostępu, utrzymania, aktualizacji i reagowania na problemy bezpieczeństwa. Należy używać go razem z instrukcją konkretnego produktu oraz dokumentacją instalacji.

1. Dane producenta

Informacja	Dane właściwe dla wydania
Producent	DIGITEX Sp. z o.o. sp.k.
Adres i kontakt	81-855 Sopot, Platanowa 2 • digitex@digitex.pl • www.digitex.pl
Zgłoszenia bezpieczeństwa	security@digitex.pl • https://www.digitex.pl/polityka-podatnosci/
Deklaracje zgodności UE	https://www.digitex.pl/strefa-klienta/

Dane do zgłoszenia odczytaj z tabliczki znamionowej, ekranu informacji o wersji lub protokołu odbioru. Nie umieszczaj w tej karcie haseł, kluczy kryptograficznych ani kodów dostępu.

Najważniejsza zasada bezpieczeństwa

Każdą zmianę mogącą wpłynąć na nadawanie alarmów uzgodnij z osobą odpowiedzialną za gotowość systemu. Zapewnij uzgodniony sposób alarmowania na czas prac. Nie wykonuj prób bezpieczeństwa przez wysyłanie nieuzgodnionych komend do działających syren.

2. Środowisko pracy i podział zadań

Produkty pracują w środowisku opisanym w dokumentacji danego wdrożenia. W przypadku digitexWAVE aplikacja jest zazwyczaj instalowana w infrastrukturze klienta. Utrzymanie serwera, sieci i kont wymaga wskazania administratora; dostarczenie oprogramowania nie oznacza automatycznie przejęcia tych zadań przez DIGITEX.

Rola	Podstawowe zadania
Właściciel systemu	Wyznacza administratorów i operatorów, zatwierdza prace oraz organizuje ciągłość alarmowania.
Administrator lub integrator	Konfiguruje środowisko, dostępy, kopie, aktualizacje i monitoring zgodnie z uzgodnionym zakresem.
Operator dyżurny	Korzysta z nadanych uprawnień, sprawdza stan systemu i zgłasza nieprawidłowości.
DIGITEX	Dostarcza informacje i poprawki dotyczące swoich produktów w określonym zakresie wsparcia; analizuje zgłoszenia bezpieczeństwa.

Wymagane warunki środowiskowe

Umieść urządzenia, routery i serwer w miejscach z kontrolą dostępu. Zabezpiecz szafy, porty serwisowe i nośniki kopii przed osobami nieuprawnionymi.

Wydziel sieć alarmowania i dopuść wyłącznie niezbędne połączenia pomiędzy jej elementami. Nie wystawiaj interfejsów administracyjnych bezpośrednio do Internetu.

Zdalny serwis dopuszczaj przez uzgodniony, uwierzytelniony kanał, na czas prac i z rejestrowaniem dostępu. Zakończ dostęp po wykonaniu zadania.

Zapewnij zgodne wersje systemu operacyjnego, bazy danych, przeglądarki i urządzeń komunikacyjnych oraz ich wsparcie bezpieczeństwa.

Utrzymuj zasilanie i tory komunikacyjne przewidziane w projekcie. Po zmianach w sieci sprawdzaj drogę komendy i powrotne potwierdzenie jej obsługi.

Parametry wymagające potwierdzenia dla produktu

Przed uruchomieniem dołącz zatwierdzoną specyfikację zawierającą:

- Wymagania systemowe,
- Interfejsy, porty, kierunki ruchu,
- Mechanizmy uwierzytelniania i szyfrowania,
- Role i zakres uprawnień,
- Wymagane usługi zewnętrzne.

Podaj również funkcje niedostępne i wymagane zabezpieczenia środowiska.

Prywatny APN nie jest sam w sobie potwierdzeniem szyfrowania transmisji ani uprawnień do wydawania komend. Zabezpieczenia toru IP, radia i dostępu serwisowego muszą wynikać z dokumentacji konfiguracji.

3. Bezpieczne uruchomienie i użytkowanie

Przed przekazaniem systemu do pracy

1. Sprawdź zgodność modelu, wersji i pakietów instalacyjnych z dokumentacją. Pobieraj pliki ze źródła wskazanego przez DIGITEX; weryfikuj podpis lub sumę kontrolną zgodnie z instrukcją produktu.
2. Utwórz indywidualne konta. Zmień hasła początkowe, usuń lub zablokuj zbędne konta i nadaj tylko uprawnienia potrzebne do wykonywania obowiązków.
3. Rozdziel codzienną obsługę od administracji. Włącz uwierzytelnianie wieloskładnikowe tam, gdzie jest dostępne; potwierdź je szczególnie dla zdalnego dostępu do infrastruktury.
4. Sprawdź reguły zapory, połączenia z serwerem i urządzeniami oraz ochronę kluczy i certyfikatów. Nie zapisuj danych dostępowych na obudowie ani we wspólnych notatkach.
5. Wykonaj kopię poprawnej konfiguracji i sprawdź możliwość jej odtworzenia. Zapisz wersje, uprawnienia i wynik testu w protokole uruchomienia.

6. W uzgodnionym oknie sprawdź adresowanie syren, grupy, uprawnienia do sterowania, statusy oraz tory zapasowe przewidziane w projekcie. Próbę dźwiękową wykonuj wyłącznie po wymaganych uzgodnieniach.

Podczas codziennej obsługi

Pracuj na własnym koncie, blokuj stanowisko po odejściu i nie udostępniaj hasła i PINu. Przed nadaniem komendy sprawdź odbiorców, obszar, treść i tryb alarmowania. Rozróżniaj wystanie komendy, jej przyjęcie i potwierdzenie wykonania — zgodnie z funkcjami dostępnej wersji systemu.

Nie instaluj niezgodzonych programów na serwerze i stanowiskach przeznaczonych do obsługi systemu. Nośniki używane podczas serwisu poddawaj kontroli w zatwierdzonym środowisku. Zmiany kont, grup syren, routingu i integracji dokumentuj z datą oraz osobą wykonującą.

Sygnaty wymagające sprawdzenia

Zgłoś nieznane konto, nietypową próbę logowania, niezgodną zmianę konfiguracji, niespodziewany restart, utratę potwierdzeń lub komendę, której operator nie wydał. Brak łączności może być zwykłą awarią, ale nie należy z góry wykluczać incydentu bezpieczeństwa.

4. Aktualizacje i wsparcie bezpieczeństwa

Okres wsparcia i jego zakres określa karta produktu lub dokumentacja powdrożeniowa. Wsparcie bezpieczeństwa obejmuje postępowanie z podatnościami i dostarczanie przewidzianych środków naprawczych. Nie jest to automatycznie okres gwarancji sprzętu, umowa serwisowa 24/7 ani termin wsparcia systemu operacyjnego dostawcy zewnętrznego.

Jak bezpiecznie wdrożyć aktualizację

1. Sprawdź komunikat producenta: wersje objęte zmianą, pilność, wymagania i wpływ na zgodność z innymi elementami instalacji.
2. Uzgodnij termin z właścicielem systemu. Przygotuj kopię, sposób odtworzenia oraz plan utrzymania alarmowania. Pilnej poprawki nie odkładaj bez oceny ryzyka i środków tymczasowych.
3. Pobierz właściwy pakiet z zatwierdzonego źródła i sprawdź autentyczność według instrukcji. Nie instaluj pliku wyłącznie dlatego, że otrzymałeś go w wiadomości e-mail.
4. Zastosuj instrukcję instalacji dla produktu. Uwzględnij kolejność aktualizacji i wymagania zasilania.
5. Sprawdź wersję po instalacji, logowanie, łączność, statusy i obsługę komend w kontrolowanym teście. Zapisz wynik. Przy błędzie wykonaj zatwierdzoną procedurę odtworzenia i skontaktuj się z serwisem.

Ustawienia automatycznych aktualizacji

Nie wyłączaj mechanizmu bez zapewnienia innego sposobu terminowego wdrażania poprawek. Jeżeli produkt nie obsługuje aktualizacji automatycznych, istnieje możliwość zlecenia aktualizacji zdalnej przez autoryzowany serwis DIGITEX.

Zmiany konfiguracji i koniec wsparcia

Wymiana routera lub radiotelefonu, zmiana APN, otwarcie portu, dodanie integracji albo zmiana certyfikatu mogą zmienić poziom ochrony i dostępność alarmowania. Przed zmianą sprawdź zgodność, zachowaj kopię i zaplanuj test. Nie obchodź uwierzytelniania ani kontroli integralności w celu przyspieszenia prac.

Przed końcem wsparcia uzgodnij aktualizację, migrację albo wymianę. Dalsza praca bez nowych poprawek zwiększa ryzyko; sama izolacja sieci nie usuwa podatności. Termin przeglądu planu migracji i osoba odpowiedzialna powinny znaleźć się w dokumentacji utrzymania.

5. Problemy bezpieczeństwa i wycofanie produktu

Gdy podejrzewasz atak lub podatność

1. Powiadom administratora i osobę odpowiedzialną za alarmowanie. Przy trwającym zagrożeniu zastosuj uzgodnioną procedurę ciągłości działania; nie czekaj na odpowiedź e-mail.
2. Zapisz czas zdarzenia, identyfikację produktu, wersję, objawy i ostatnie zmiany. Zabezpiecz dostępne logi w sposób, który nie zakłóci pracy systemu.
3. Nie kasuj danych ani nie przywracaj ustawień fabrycznych bez oceny administratora. Ograniczenie dostępu lub odłączenie elementu uzgodnij z osobą odpowiedzialną za ciągłość alarmowania.
4. Wyślij zgłoszenie na adres do zgłaszania incydentów. Wskaż, czy zdarzenie trwa i czy wpływa na syreny lub sterowanie. Informacje wrażliwe przekazuj wyłącznie uzgodnionym kanałem.
5. Zachowaj identyfikator sprawy i wykonuj uzgodnione działania. Zgłoszenie do DIGITEX nie zastępuje własnych obowiązków organizacji wobec właściwych organów.

DIGITEX przewiduje pierwszą reakcję na zgłoszenie w ciągu 24 godzin. Jest to termin kontaktu i rozpoczęcia obsługi, a nie obietnica naprawy w tym czasie. Szczegółowe zasady określa Polityka ujawniania podatności.

Bezpieczne wycofanie i przekazanie do serwisu

Przed wycofaniem urządzenia lub serwera potwierdź przejęcie jego zadań i zaktualizuj konfigurację systemu. Zachowaj tylko dane wymagane do odtworzenia, rozliczenia prac lub analizy incydentu, z kontrolą dostępu do archiwum.

- Usuń lub unieważnij konta, certyfikaty, klucze, tokeny i dostęp zdalny przypisany do wycofanego elementu. Wycofaj reguły zapory, VPN i integracje, których nie należy już używać.

- Usuń dane użytkowników, konfigurację i zapisane poświadczenia metodą właściwą dla modelu. Sam reset fabryczny nie musi bezpiecznie usuwać wszystkich danych.
- Postępuj zgodnie z instrukcją urządzenia lub oprogramowania. Jeżeli skutecznego usunięcia nie można potwierdzić, uzgodnij z DIGITEX obsługę nośnika przed przekazaniem sprzętu dalej.
- Usuń kartę SIM i uzgodnij dezaktywację zbędnej usługi. Dla modułów radiowych zastosuj zatwierdzoną procedurę usunięcia danych sieciowych i kryptograficznych.
- Zapisz numer urządzenia, zakres usunięcia danych, datę i osobę odpowiedzialną. Sprzęt elektryczny przekaz do właściwego procesu zagospodarowania.

Przy wysyłce do serwisu uzgodnij zakres danych potrzebnych do diagnozy. Nie przysyłaj aktywnych haseł administratora ani kluczy produkcyjnych bez wyraźnie ustalonej potrzeby i bezpiecznego sposobu przekazania.