

centrala

w centrum uwagi

czyli jak skutecznie
zadbać o jej
bezpieczeństwo



dla biznesu

krótka instrukcja dla administratora

Zadbaj o właściwe zabezpieczenie Twojej centrali telefonicznej. Nie pozwól, aby ktokolwiek posługiwał się nią na Twój koszt, w przeciwnym razie możesz narazić się na poważne straty finansowe. Jeśli posiadasz centralę na łączach tp i nie korzystasz z usług naszego administratora, zapoznaj się z **10 zasadami**, które decydują o jej właściwym zabezpieczeniu.

Jeżeli powierzyłeś komuś jej obsługę, przekaz mu niezbędną wiedzę. Proste działania, które wprowadzisz w życie, mogą być skutecznym zabezpieczeniem przed niepożądanymi użytkownikami Twojej centrali telefonicznej.

1. Wybierz silne hasło administratora

Stosuj algorytmy (reguły), które powszechnie są uznawane jako wystarczające do tworzenia silnych haseł.

Unikaj stosowania haseł „słownikowych”. Jeśli jest to konieczne, przechowuj hasła w bezpiecznym miejscu (zaszyfrowane).

Krótką instrukcją tworzenia bezpiecznego hasła

Używaj haseł długich, zawierających duże i małe litery, cyfry oraz znaki specjalne (!@#\$%^&*(){}[]?). Nie używaj haseł składających się z jednego słowa, które można znaleźć w słowniku, ponieważ można je łatwo złamać!

Dobrym sposobem jest wpisanie całej frazy (bez odstępów lub zrobienie odstępów w miejscach niegramatycznych, np. „niewi em”) składającej się ze znaków wymienionych powyżej. Jeżeli musisz wpisać tylko jedno słowo, wpisz je z błędem, np. „l@T0#81” zamiast „lato381”.

2. Szyfruj hasła

Jeśli to możliwe, stosuj opcję szyfrowania hasła w plikach konfiguracyjnych urządzenia.

3. Stosuj kontrolę systemu bazującą na kalendarzu

W miarę możliwości wykorzystuj usługi, które mogą definiować parametry pracy systemu w zależności od pory dnia, świąt etc. Przykładem takiej usługi może być night service.

4. Stosuj profile (grupy) nadające uprawnienia użytkownikom

Podziel użytkowników systemu na grupy z różnymi uprawnieniami.

Wykreuj odpowiednią konfigurację i zmień ustawienia określające uprawnienia konkretnego użytkownika. Staraj się nie wykorzystywać profili fabrycznych.

5. Sprawdź parametry konfiguracyjne usług głosowych

Sprawdź, w jaki sposób możesz modyfikować ustawienia dla takich usług jak np. call forward. Zwróć uwagę na tzw. zawijanie ruchu, czyli możliwość wykorzystania centrali do tranzytu ruchu w relacji PSTN-PABX-PSTN.

6. Nie wykorzystuj ustawień fabrycznych takich funkcjonalności jak DISA, IVR etc.

Sprawdź, czy funkcjonalności związane z interaktywnym sterowaniem centralką są wyłączone (ustawienia fabryczne). Jeśli zdecydujesz się na stosowanie tych funkcjonalności, postaraj się skonfigurować je z ustawieniami zapewniającymi wysoki poziom bezpieczeństwa. Należą do nich:

- hasła dostępne,
- ograniczenia przy przekierowaniu ruchu,
- uwierzytelnianie użytkowników.


7. Ograniczenia dostępu do systemu poprzez sieć IP/WiFi

Wykorzystaj kontrolę dostępu do systemu już na poziomie warstwy 2 modelu ISO. Będzie to możliwe poprzez stosowanie mechanizmów access-list na urządzeniach sieciowych. Staraj się budować ograniczenia bazujące na adresach MAC.

8. Ogranicz możliwości zdalnego dostępu do systemu

Na bieżąco staraj się monitorować uprawnienia swoich użytkowników. Stosuj monitoring systemowy w celu sprawdzenia ewentualnych nadużyć ze strony „zaufanych” użytkowników systemu. Jeśli zachodzi konieczność dostępu użytkowników do systemu z internetu, stosuj szyfrowaną transmisję danych (SSL, IPSec) oraz możliwie mocne uwierzytelnienie użytkowników.

9. Wymagaj od użytkowników systemu stosowania oprogramowania antywirusowego i antyspamowego
10. Regularnie dokonuj analizy zdarzeń systemowych (przeglądaj logi)



tylko centrale
zarządzane przez
Telekomunikację Polską
gwarantują pełne
bezpieczeństwo!

Sprawdź ofertę Central Diatonis w TP.

Więcej informacji na temat central zarządzanych przez Telekomunikację Polską dostępnych pod numerem Błękitnej Linii 19330.