Polityka bezpieczeństwa usługi wirtualnych central na platformie CloudPBX

Poziom7

2017/11/14 08:06

Spis treści

Polityka bezpieczeństwa usługi wirtualnych central na platformie CloudPBX

Dokument określający zakres odpowiedzialności i poziom bezpieczeństwa pltformy CloudPBX

1. Wstęp

System telekomunikacyny CloudPBX oparty jest na publicznym dostępie do usługi, co oznacza możliwość korzystania z funkcjonalności centrali telefonicznej przy pomocy ogólnodostępnej sieci Internet. Zaletą takiego rozwiązania jest łatwość i szybkość wdrożenia, możliwość samodzielnej rekonfiguracji oraz niezależność terytorialna, jednak należy zwrócić uwagę, że otwartość rozwiązania może wpływać na próby nieautoryzowanego dostępu do zasobów centrali. Polityka bezpieczeństwa systemu CloudPBX została zaprojektowana tak, aby zmaksymalizować poziom bezpieczeństwa przy zachowaniu funkcjonalności systemu otwartego. W związku z tym użytkownik powinien mieć świadomość potencjalnych zagrożeń oraz podstawowych warunków zachowania bezpiecznie działającej usługi.

Terminy wykorzystane w dokumencie:

użytkownik - klient usługi CloudPBX posiadający imienne konto na platformie, uprawniony do zmian konfiguracyjnych centrali PBX,

terminal VoIP - urządzenie terminujące połączenia telefoniczne, dostępne zwykle pod numerem wewnętrznym centrali. Może to być telefon IP, bramka VoIP lub oprogramowanie typu softphone,

fraud - rodzaj oszustwa telekomunikacyjnego, polegającego na nieautoryzowanym wygenerowaniu dużej ilości połączeń na koszt użytkownika,

operator platformy CloudPBX - firma Poziom7, która realizuje i zarządza usługą CloudPBX. Zasady kontaktu określone są na stronie http://www.cloudpbx.pl

konto abonenckie - konto określające pojedynczego abonenta wewnętrznego centrali PBX. Identyfikowane telefonicznym numerem w numeracji skróconej. Jednoznaczne z kontem protokołu SIP

2. Opis zagrożeń

2.1 CloudPBX umożliwia tworzenie wirtualnych central telefonicznych oraz podłączanie do nich terminali VoIP przy pomocy protokołu SIP 2.0. W obszarze bezpieczeństwa oznacza to dostęp do aplikacji zarządzającej centralą CloudPBX, oraz autoryzację aparatów telefonicznych i zabezpieczenie transmisji głosowej. Przejęcie danych autoryzacyjnych do aplikacji lub terminali przez atakującego może skutkować wykonywaniem połączeń telefonicznych na koszt użytkownika. W skrajnych przypadkach może dojść do prób wywołania fraudów.

2.2 Aplikacja PBXVisor jest podstawowym narzędziem konfiguracyjnym centrali na platformie CloudPBX. Dostęp do aplikacji możliwy jest za pomocą przeglądarki internetowej na podstawie loginu i hasła konfigurowanego na etapie uruchomienia usługi. Uprawnienia dostępu do aplikacji powinny mieć tylko i wyłącznie osoby odpowiedzialne za konfigurowanie usługi po stronie użytkownika. Udostępnienie loginu i hasła osobom trzecim jest niedozwolone. Nieautoryzowany dostęp do aplikacji może skutkować nieprawidłowym działaniem centrali, a także możliwością wykonywania nieautoryzowanych połączeń telefonicznych.

2.3 Terminale VoIP rejestrują się w centrali telefonicznej za pomocą nazwy użytkonika i hasła, konfigurowanych podczas generowania linii telefonicznej w aplikacji PBXVisor.Informacje te należy wprowadzić w terminalu. Udostępnienie parametrów logowania terminala osobom trzecim może skutkować wykonaniem nieautoryzowanch połączeń telefonicznych. Użytkownik jest również odpowiedzialny za odpowiednie zabezpieczenie terminala VoIP przed nieuprawnionym dostępem do jego konfiguracji. Odczytanie konfiguracji terminala przez atakującego jest równoważne z odczytaniem parametrów autoryzacyjnych terminala, dlatego ważne jest prawidłowe zabezpieczenie terminali.

2.4 Połączenia telefoniczne w systemie CloudPBX realizowane są za pomocą protokołu SIP/RTP/SRTP. Protokół RTP odpowiada za przesył głosu poprzez sieć teleinformatyczną w podstawowej formie umożliwiającej podsłuchanie strumienia rozmowy przez atakującego. Bezpieczeństwo prywatności rozmowy zapewnia protokół SRTP zapewniający szyfrowanie strumienia głosowego. Aby wykorzystać tą funkcjonalność, terminal użytkownika musi umożliwiać włączenie szyfrowania SRTP.

3. Mechanizmy bezpieczeństwa autoryzacji zaimplementowane na platformie CloudPBX

3.1 Aplikacje zarządzające systemu CloudPBX, czyli „PBXVisor”, „Panel abonenta”, „OpenCC”, „Panel klienta” dostępne są za pomocą przeglądarki internetowej pod odpowiednimi adresami URL. Aplikacje

udostępnione są poprzez szyfrowany protoków HTTPS zabezpieczony certyfikatem SSL klasy 1. Gwarantuje to poufność przesyłania informacji autoryzacyjnych przez sieć Internet.

3.2 Autoryzacja terminali VoIP odbywa się na podstawie mechanizmu Digest access authentication (RFC 2069) gwarantującego przesył danych autoryzacyjncyh zakodkowanych algorytmami hashującymi uniemożliwiającymi odtworzenie par login/hasło

3.3 Polityka bezpieczeństwa wymusza stosowanie haseł terminali co najminej 16 znakowych, co w połączeniu z mechanizmami automatycznej ochrony wyklucza ataki typu BruteForce.

3.4 Platforma CloudPBX wspiera protokół SRTP (Secure RTP) szyfrujący strumień audio pomiędzy centralą a terminalem użytkownika. Warunkiem wykorzystania tej technologii jest wsparcie SRTP przez terminal VoIP

4. Mechanizmy automatycznej ochrony

Ochrona Pasywna

4.1 Polityka bezpieczeństwa dotycząca stosowania haseł terminali przewiduje konieczność stosowania haseł o długości 16 znaków z odpowednią kombinacją znaków specjalnych.

4.2 Możliwość ograniczenia dostępu terminala VoIP do rejestrowania się na wybranej linii. Ograniczenie to pozwala definiować adres lub podsieć IP, z której terminal może logować się do danego konta SIP.

4.3 Limit jednoczesnych połączeń z jednego terminala VoIP ograniczony do 2 połączeń.

4.4 Limit jednoczesnych połączeń międzynarodowych z jednego terminala VoIP ograniczony do 1 połączenia.

4.5 Limit jednoczesnych połączeń międzynarodowych dla centrali PBX ograniczony do 2 połączeń .

4.5 Blokada transferów połączeń na numery międzynarodowe.

4.6 Ochrona na poziomie telekomunikacyjnym w postaci dyskryminatorów ruchu wychodzącego, określającego zakres uprawnień do wykonywania połączeń wychodzących dla abonentów wewnętrznych.

Ochrona aktywna

4.7 Automatyczna blokada rejestracji SIP. Jeśli terminal abonenta dokona pięciokrotnej nieudanej próby rejestracji do centrali platformy CloudPBX, system zablokuje dostęp z adresu IP terminala na czas jednej godziny. Aby odblokować dostęp w krótszym czasie należy skontaktować się z operatorem platformy CloudPBX. UWAGA - jeśli terminal działa w sieci o adresacji prywatnej (NAT) i prezentuje się adresem IP bramy takiej sieci, dostęp zostanie zablokowany dla całej sieci lokalnej.

4.8 Automatyczna blokada logowania do aplikacji PBXVisor. Jeśli wykonane zostanie 10 nieudanych logowań w ciągu 5 minut, dostęp do aplikacji zostanie zablokowany dla adresu IP na jedną godzinę.

4.9 Limit kwotowy centrali. Każda centrala posiada domyślne ograniczenie kwotowe połączeń wykonywanych w bieżącym miesiącu rozliczeniowym. Limit domyślny ustalony jest na kwotę 500 zł netto. Jeśli kwota za połączenia zostanie przekroczona, połączenia zostaną zablokowane. Zmiana wysokośli limtu możliwa jest po złożeniu odpowedniej dyspozycji operatorowi platformy CloudPBX.

5. Zasady bezpieczeństwa przy wykorzystaniu systemu CloudPBX

5.1. Dane autoryzacyjne do aplikacji zarządzających w systemie CloudPBX autentykują użytkownika w systemie. Udostępnienie danych osobom trzecim jest zabronione. Skutki działania w aplikacji ponosi użytkownik, na którego dane dokonana została autoryzacja. Należy pamiętać, że dysponując danymi autoryzacyjnymi do aplikacji PBXVisor, osoba nieautoryzowana może tworzyć nowe linie telefoniczne, przekierowywać rozmowy lub też pobierać nagrania rozmów telefonicznych.

5.2 Konfiguracja terminali VoIP wymaga poświęcenia uwagi w zakresie bezpieczeństwa działania aparatów. Zaleca się konfigurację aparatów w sieciach lokalnych z adresacją prywatną (NAT) lub chronioną firewallem. Szczególnie ważną kwestią jest zabezpieczenie samych terminali VoIP. Zwykle są to telefony lub bramy posiadające własne wbudowane aplikacje konfiguracyjne. Pozostawianie domyślnych danych logowania do takiego aparatu równoznaczne jest z udostępnieniem parametrów autoryzacyjnych do konta abonenckiego na centrali telefonicznej. Instalacja aparatu telefonicznego w sieci publicznej z fabrycznymi parametrami logowania może skutkować przejęciem konta abonenckiego przez osobę atakującą, a tym samym wygenerowanie kosztów obciążających użytkownika.

5.3 Jeśli terminal będzie pracował na publicznym adresie IP, należy dołożyć wszelkch starań, aby dostęp do jego parametrów konfiguracyjnych był chroniony. Należy pamiętać również o okresowej aktualizacji oprogramowania systemowego - firmware (jeśli producent udostępnia).

5.4 Dobrą praktyką w zakresie konfiguracji centrali telefonicznej jest narzucanie odpowiednich uprawnień dla abonentów do połączeń wychodzących - dyskryminatorów. Należy mieć na uwadze potrzeby abonenta i ewentualne ograniczanie usług nie wymaganych, np. blokada połączeń międzynarodowych dla abonentów komunikujących się tylko w obrębie połączeń lokalnych.

5.5 Wartym wykorzystania jest mechanizm ograniczenia dostępu do konta abonenckiego tylko z określonej sieci lub adresu IP. Jeśli abonent nie przemieszcza się dynamicznie wraz z terminalem logując się z niemożliwych do identryfikacji zakresów IP, wtedy dobrze jest ograniczyć dostęp do konta tylko dla znanej adresacji. Takie zabezpieczenie blokuje możliwość wykonania fraudu spoza lokalizacji użytkownika nawet w przypadku utraty parametrów autoryzacyjnych terminala.

6. Zakres odpowiedzialności.

6.1 Operator platformy CloudPBX oddaje użytkownikowi do dyspozycji usługę wirtualnych central PBX, posiadającą zestaw mechanizmów autoryzacyjnych i zabezpieczających. Operator odpowiedzialny jest za skutki działań nieautoryzowancyh, które wynikną z zaniedbań lub niedostatecznej ochrony platformy CloudPBX.

6.2 Operator platformy CloudPBX nie odpowiada za skutki naruszenia bezpieczeństwa platformy wynikłe z winy użytkownika, w szczególności z powodu zaniedbań zalecanej polityki bezpieczeństwa oraz podstawowych zasad bezpiecznego działania w sieci publicznej.

6.3 Użytkownik ponosi koszty połączeń wykonanych za pomocą zautoryzowanych połączeń, czyli takich w przypadku których terminal wykonał poprawną autentykację i autoryzację.

7. Podsumowanie

Mając na uwadze charakter działania platformy jako usługi publicznej, konieczne jest połączenie funcjonalności z wysokim poziomem bezpieczeństwa. Platforma CloudPBX zawiera zestaw mechanizmów, zabezpieczeń oraz ustandaryzowaną politykę bezpieczeństwa, gwarantującą maksymalny poziom zabezpieczeń przed nieautoryzowanym działaniem w zakresie zarządzania centralą, bezpieczeństwa danych, jak i w obszarze połączeń telekomunikacyjnych. Należy jednak pamiętać o podstawowych zasadach korzystania z usług publicznych poprzez sieć Intrernet i stosować się do zaleceń przewidzianych polityką bezpieczeństwa. W przypadku braku odpowiedniej wiedzy należy skonsultować się z operatorem usługi lub skorzystać z pomocy wyspecjalizowanej firmy.