1. Niefrasobliwość administratorów SDI.

Niewłaściwa polityka bezpieczeństwa TPSA może narazić uzytkowników usługi SDI na wyłączenie transmisji internetowej przez innego użytkownika SDI.

TPSA w wielu rejonach kraju ustawiała hasła uzytkownikom danej miejscowości w ten sam sposób. Co więcej w haśle jest wpisany login czyli nazwa użytkownika.

Dla przykładu:

Jeśli login to „marcin”, hasło miało postać „###marcin##” gdzie ciąg znaków ### i ## był identyczny dla wszystkich użytkowników.

W mojej miejscowosci stosowano dwa klucze.

Pierwszy własnie z ciągiem 1 (oznaczę go dla przykładu jak wyżej #) i drugi z ciągiem 2 (oznaczonym dla przykładu jako \*).

I tak hasło dla każdego uzytkownika brzmi „###login##” lub „\*\*\*\*login\*\*\*”.

Wystarczy znać login innej osoby i albo 1 albo drugi klucz da hasło.

Co można zrobić znając login i hasło ? Można się zalogować bez przeszkód na konto ofiary.

Oczywiście numer IP pozostanie nasz (jest przypisany prawdopodobnie do portu półki) ale gdy jesteśmy zalogowani na koncie ofiary, ona nie może się zalogować. Jej SDI nie zadziała – nie ma połączenia z internetem.

Co więcej, możemy zalogować się w trakcie sesji ofiary.

Wówczas co prawda nie uda nam się zalogować pomyślnie ale transmisja ofiary ustanie prawie do zera.

Temporyzacja czyli limit czasu w tym wypadku nie działa (nie wiem czemu) i możemy tak wisieć skutecznie wyłączając komuś transmisję.

Login często jest tożsamy z nazwą HOSTa (komputera).

Nazwę komputera możemy poznać odbierając od kogoś e-maila.

W mailu jest też IP po którym poznamy, że ofiara ma SDI w naszej miejscowosci.

Znowu niefrasobliwośc TPSA może być przyczyną kłopotów jej klientów.

2. Złośliwa aplikacja TPSA samowolnie ustawia przekierowania ?

Tak wynika z wniosków wyciągniętych z dostępnych faktów.

Kilkakrotnie w ciągu oststniego czasu dzwonilem pod numer konfiguracyjny i do odsłuchań poczty głosowej TPSA (9426).

Zmieniłem hasło, nagrałem powitanie. Nie aktywowałem żadnych przekierowań po tym połączeniu.

Jakież było moje zdziwienie, gdy po kilku dniach usłyszałem w słuchawce charakterystyczny sygnał świadcząsy o aktywnej usłudze przekierowania.

Okazało się, że „ktoś” bez mojej wiedzy i zgody dokonał przekuierowania warunkowego „gdy nie odbieram” (kod 61) na numer poczty głosowej.

Pełny oburzenia wyłączyłem przekierowanie i zapomniałem o sprawie.

Kilka dni później na innej linii też konfigurowałem sobie skrzynkę.

I znów po kilku dniach zauważyłem aktywne przekierowanie.

Z początku myślałem, ze to monterzy na polecenie TPSA włączają przekierowania (wszak TPSA zarabia na każdym odebranym w swojej sieci połączeniu (albo od innego abonenta albo w opłacie interconnectowej).

Jednak później przemyślałem fakty i wydaje mi się, ze TPSA wprowadziła do Centrum Kreowania Usług aplikację, mającą za zadanie włączać przekierowania na pocztę (wszak centrale są teraz zdalnie konfigurowane) gdy abonent niechcacynawet zadzwoni na numer poczty.

I tu podejrzanie brzmi ten tekst wygłaszany przez automat podczas konfiguracji skrzynki, ze aktywujac skrzynkę „zgadzasz się na świadczenie usługi Poczty Głosowej TP zgodnie z cennikiem i regulaminem usługi”.

A gdzie jest ten regulamin usługi Poczta TP ?

Widział go ktoś w internecie na przykład ? Jeśłi tak to proszę o info.

Takie działanie TPSA jest zdaje się nielegalne.

Znów TPSA panicznie próbuje ratować spadające przychody z usług telefoni stacjonarnej.

A ze nieuczciwie ? .....

3. Myślisz logicznie ? – Możesz więcej !

Otóż da się aktywować w TPSA (a właściwie deaktywować) rżne usługi mimo iż nie jest to ujęte w ofercie ani w cennikach.

Mnie udało się zamówić (i doczekać na wprowadzenie) takich usług jak wyłączenie mozliwości wybierania tonowego (DTMF) na jednej z linii lub wyłączenie mozliwości dokonywania przekierowań na innej linii.

Pierwsze musiałem zamówić na jednej z linii mojego znajomego, majacego pensjonat i centralę hotelową PBX.

Człowiek ten chciał mnieć pewność że goście nie będą ze swoich pokojów dokonywac przekierowań na dziwne numery linii miejskiej (niestety centrala hotelowa jest starego typu i nie umozliwia ograniczenie ruchu na cyfry \* i #).

Udało się.

Z kolei ja na jednej ze swoich linii w starym budynku gdzie kable telefoniczne idą wybebeszone w ogólno dostępnym miejscu, aktywowałem wyłączenie możliwości dokonywania przekierowań (kodem 21 , 61 i 67).

Też się udało. W ten sposób obce osoby podpiąwszy się do mojej linii, nie przekierują telefonu np. na numer telefonu komórkowego kolegi aby potem sobie na mój koszt ze swojego domu dzwonić.

Oczywiście na tej linii są aktywne też wszelkie ograniczenuia na numery których nie używam : międzynarodowe, wszystkie premium rate itp.

Wniosek jest z tego taki, że da się wynegocjować z Tepsą usługi niby nie świadczone przez ta firmę. Czasem trzeba przebrnąć przez słynne „nie ma takich mozliwosci” wygłaszane prze konsultantki z Błękitnej Linii , ale jeśłi da się przekonać panie konsultantki, ze się wie lepiej to się może udać.

Teraz już jest precedens i nie mogą się wymigiwać na przyszlość.

Przecież każda linia automatu ma taką usługę a niektóre pracują tylko pulsowo. Więc się da !

4. Podejrzane zachowanie centrali Alcatel S-12.

W Warszawie większość centrali telefonicznych to Alcatele S-12.

Dało tam się zauważyć dziwne zjawisko.

Mając telefon z DTMF ale taki bez spterowania procesorem (bezprzewodowe odpadają) należy zrobić taki eksperyment.

Wcisnąć dowolny klawisz cyfry (najlepiej pierwszej cyfry jakiegoś numeru lokalnego). Trzymając wciśnięty klawisz, podnieść słuchawkę. Telefon od razu wysyła DTMF ytej cyfry w linię. I tu dziwne zjawsko.

Puśmy ten klawisz. W słucawce dlaej sygnał ciągły. Wybieramy kolejne cyfry numeru. Dalej sygnał. Aż po ostaniej cyfrze znika ciągły sygnał a pojawia się sygnał wołania.

Niby o niczym to nie świadczy ale.... zadzwońmy w ten sposób na jakiś numer badaniowy (np. odzewnik na innej S-12). Nie dodzwonimy się !

To świadczy o jakimś błędzie wykraczającym poza blok rejestrów.

A jeśłi tak , to może się okazać, iż centrala na przykłąd nie zapisuje albo błednie zapisuje rekord bilingowy takiego połączenia!

Sprawdzcie i weźcie biling !

S-12 słyną z niestabilnej pracy i mnogości dziur.

5. Nowi operatorzy i nowe zakresy numeracji kryją skarby !

Mnie udalo się jakis czas temu odkryć numer dostępowy operatora VoIP, który dopiero testował swoje urządzenia.

Miał całą pulę numerów od operatora alternatywnego.

No i na niektó®ych z tych numerów system odbierał z.... dial-tonem J.

Numer wybierało się w dziwny sposób ale odkryłem jak.

Kilka miesięcy miałem dzwonienie na komórki jak lokalnie.

Skanujcie nowe zakresy numerów !

6. Wedlug donisień na grupach dyskusyjnych, TPSA wyłącza mozliwość dokonywania przekierowań na numery premium rate.

Nareszcie coś robią po fali krytyki gdy pajęczarze dokonywali przekierowań na słynny numer doładowań POP i po tej czynności omijali ograniczenie do dwóch dołądowań, dzwoniąc z co i rusz innego automatu na numer ofiary – abonenta.

7. Wieszające się eXanto.

Okazuje się, ze aparaty eXanto są bardzo niestabilne. Łatwo je zawiesić długo i szybko wciskając na zmianę przycisk nowej rozmowy i REDIAL.

Wpierw jednak trzeba wybrać jakiś numer.

Gdyby tak udało się do zawiesić na rozmowie....

A tak na marginesie. A gdyby zrobić na plytce drukowanej protezę karty CHIPowej z wyprowadzonymi sześcioma przewodami.

Te przewody powinny iść do kasety na oryginalną kartę ale trzymana poza aparatem. I teraz na każdym z tych sześciu przewodów dac wyłącznik ?

Czy aparat ma szansę zawiesić się, dgy jeden z PINów karty nagle okaże się być rozwartym ? I który ?

Zostawiam to przemysłeniom.

Pozdrawiam,

vari