Informacje o zagrożeniach związanych ze świadczonymi Usługami, w tym o sposobach ochrony bezpieczeństwa, prywatności i danych osobowych

Rodzaje zagrożeń telekomunikacyjnych:

- ZŁOŚLIWE OPROGRAMOWANIE – instalacja aplikacji niewiadomego pochodzenia może spowodować utratę kontroli użytkownika nad urządzeniem oraz utratę poufności danych osobistych ich niszczenie lub wykradanie do czego może dojść bez jego wiedzy. Złośliwe oprogramowanie może doprowadzić również do niezamierzonych operacji w telefonie w szczególności:
    - samoczynna wysyłka danych,
    - przekierowanie SMS-ów bez wiedzy użytkownika,
    - przekierowanie na płatne numery bez wiedzy użytkownika.
    - samoczynny restart urządzenia końcowego (telefonu);

- POŁĄCZENIA/SMS NA NUMERY PREMIUM – połączenia i SMS-y przychodzące z nieznanych numerów wskazujące na odesłanie SMS-a czy też wykonania połączenia na konkretny numer mogą powodować wygenerowanie wysokich kosztów za SMS lub połączenie;

- WANGIRI FRAUD – jest prowokowaniem do oddzwaniania na numery o wysokiej opłacie – abonent automatycznie oddzwania na numer „nieodebranego połączenia", który najczęściej jest podobny do numeru krajowego, ale w rzeczywistości jest to numer zagraniczny o znacznie podwyższonej opłacie;

- SMS PREMIUM wprowadzające w błąd użytkownika w celu uzyskania korzyści o treści sugerującej uruchomienie płatnej subskrypcji i informującej o możliwości wyłączenia usługi poprzez wysłanie zwrotnej wiadomości z określonym kodem (wysłanej na numer wysoko płatny bez podania kosztów lub przy zaniżeniu stawki za SMS zwrotny). W konsekwencji abonent/użytkownik odsyłający wiadomość, spodziewający się usunięcia subskrypcji, ponosi koszt korzystania z usług o podwyższonej płatności;

- SMS MT - wprowadzanie w błąd w celu akceptacji przez abonenta/użytkownika subskrypcji MT (płatne za otrzymanie SMS/MMS). Dotyczy osób chcących skorzystać z różnych serwisów internetowych, np.: obejrzeć film, doładować telefon, wysłać e-kartkę z życzeniami, podaje swój numer telefonu w celu otrzymania kodu dla wybranej usługi. Zamiast tego otrzymuje jednak SMS-a powiadamiającego o uruchomieniu SMS-ów wysokopłatnych przy odbiorze (nawet kilka razy w tygodniu). Ponadto ściąganie aplikacji z niezaufanego źródła, uruchamianie gier itp. również może spowodować nieświadome uruchomienie zamówienia na otrzymywanie SMS-ów MT. Sposobem ochrony jest szczegółowe zapoznawanie się z regulaminami usług oraz ich rodzajami a w przypadku braku dostępu do treści regulaminu – niekontynuowanie transakcji;

- SPOOFING – czyli podmiana na fałszywego nadawcę którego celem jest zmylenie odbiorcy i w konsekwencji wyłudzenie danych, informacji wrażliwych, np. numeru karty kredytowej, numeru PIN, hasła, itp. Należy unikać przesyłania danych, informacji wrażliwych za pośrednictwem sms i/lub adresu e-mail;

- KARTA SIM – niezabezpieczona kodem PIN jeżeli zostanie zgubiona, skradziona lub udostępniona nieumyślnie niepowołanym osobom, może zostać skopiowana i wykorzystana do połączeń/SMS-ów generujących wysokie koszty;

- KRADZIEŻ DANYCH PRZEZ BLUETOOTH – włączony cały czas może spowodować kradzieży danych z naszego urządzenia w związku z czym należy zwrócić uwagę na komunikaty pojawiające się w telefonie i wyłączać Bluetooth zawsze po zakończonej aktywności. Dane mogą również zostać skopiowane przez dostępne na rynku urządzenia/aplikacje, dlatego nie należy pozostawiać urządzenia końcowego w zasięgu osób trzecich.

Sposoby ochrony urządzeń końcowych i danych:

- BACKUP DANYCH – dedykowane aplikacje do backupu danych i ochrony urządzeń końcowych pozwalają na bezpieczne przechowywanie cennych dla użytkownika danych. Ważne informacje i numery telefonów (kontakty) należy zapisywać na karcie SIM i/ lub karcie pamięci;

- HASŁO/PIN – prosta funkcjonalność, dostępna w każdym telefonie, zabezpiecza przed niepowołanym dostępem osób trzecich w przypadku kradzieży lub zagubienia. Wskazane jest, aby po kilku nieudanych próbach wprowadzenia nr PIN/HASŁA telefon był blokowany. Zaleca się sprawdzenie w instrukcji obsługi urządzenia, czy nie ma wbudowanych ono innych funkcji zabezpieczających przed nieautoryzowanym użyciem, pomagających w jego odnalezieniu lub kasujących wszystkie dane w urządzeniu w przypadku jego zagubienia lub kradzieży;

- Ochrona aparatu przed OSOBAMI NIEUPOWAŻNIONYMI - nie należy zostawiać telefonu bez kontroli i udostępniać go osobom nieupoważnionym (w tym dzieciom), gdyż istnieje potencjalne zagrożenie braku kontroli nad urządzeniem i jego zawartością;

- NAPRAWY W AUTORYZOWANYM SERWISIE – zaleca się wyczyszczenie danych (przywrócenie ustawień fabrycznych) przed oddaniem urządzenia do naprawy lub jego utylizacją oraz wyjęcie karty SIM;

- PROGRAM ANTYWIRUSOWY - aplikacje do ochrony telefonów powinny być właściwie zainstalowane, tj. poziom ustawień powinien być adekwatny do wartości informacji na telefonie oraz do możliwości zainstalowanej aplikacji bezpieczeństwa, a także aktualizowane na bieżąco

- SKANOWANIE URZĄDZENIA - w celu wyeliminowania obecności szkodliwego oprogramowania zaleca się częste skanowanie zawartości urządzenia;

- Stosowanie BEZPIECZNYCH HASEŁ w sieci – nie powinno się używać takiego samego hasła do wszystkich aplikacji i powinny się one składać z kombinacji liter, cyfr i znaków specjalnych;

- Nieoddzwanianie lub niewysyłanie komunikatów na NIEZNANE NUMERY;

- NIEPODAWANIE POUFNYCH DANYCH, w szczególności danych osobowych, identyfikatorów, haseł, kodów dostępu, numerów kart płatniczych/kredytowych nieznanemu rozmówcy lub w miejscach publicznych, na portalach internetowych czy drogą mailowa;

- SYSTEMATYCZNA AKTUALIZACJA systemu operacyjnego aparatu telefonicznego lub innego urządzenia elektronicznego umożliwiającego za pośrednictwem karty SIM korzystanie z usług świadczonych przez operatora;

- NIEPRZECHOWYWANIE W PAMIĘCI WEWNĘTRZNEJ aparatu telefonicznego lub na karcie pamięci niezabezpieczonych (niezaszyfrowanych) poufnych danych, w szczególności danych osobowych, identyfikatorów, haseł lub kodów dostępu, numerów kont lub kart kredytowych;

- Wyłączanie przez abonenta/użytkownika łączności bezprzewodowej Wi-Fi, Bluetooth i NFC niezwłocznie po zakończeniu korzystania z tego typu połączeń;

- BEZPIECZNE KORZYSTANIE Z APLIKACJI mobilnych , w tym:
    - instalowanie lub aktualizacja aplikacji mobilnych tylko z zaufanych źródeł, najlepiej producenta danej aplikacji;
    - zwracanie szczególnej uwagi na wymagania instalowanego programu w zakresie dostępu do poszczególnych funkcjonalności urządzenia podczas jego instalacji;
    - dokładna analiza w trakcie instalacji lub aktualizacji aplikacji mobilnych, jakie mają one uprawnienia oraz do jakich usług lub danych abonenta/użytkownika mają one dostęp,
    - systematyczna aktualizacja aplikacji mobilnych poprzez instalowanie poprawek i aktualizacji systemowych;

- ZABEZPIECZENIE urządzenia, za pomocą którego korzysta się z HOT-SPOTU przed nieuprawnionym dostępem z zewnątrz