Informacje wynikające z przepisów Ustawy z dnia 16 lipca 2004 r. Prawo telekomunikacyjne [Dz.U.2004.171.1800]

SPIS TREŚCI

I. WSTĘP 2

II. Informacje wynikające z art. 175e ust. 2 Prawa telekomunikacyjnego 2

III. Informacje wynikające z art. 175 ust. 2 Prawa telekomunikacyjnego. 3

IV. Informacje wynikające z art. 56 ust. 3 pkt 11 lit. e Prawa telekomunikacyjnego 3

V. Informacje wynikające z art. 56 ust. 3 pkt 12 i art. 63 ust.1 Prawa telekomunikacyjnego 4

VI. Informacje wynikające z art. 56 ust. 3 pkt 20 Prawa telekomunikacyjnego 4

1. ZAGROŻENIA 5

1.1. ZŁOŚLIWE OPROGRAMOWANIE 5

1.2. POŁĄCZENIA/SMS NA NUMERY PREMIUM 6

1.3. SPOOFING – podmiana nadawcy 6

1.4. KARTA SIM 6

1.5. KRADZIEŻ DANYCH 6

2. SPOSOBY OCHRONY URZĄDZEŃ KOŃCOWYCH I DANYCH 7

2.1. BACKUP DANYCH 7

2.2. HASŁO/PIN 7

2.3. OSOBY NIEUPOWAŻNIONE 8

2.4. AUTORYZOWANY SERWIS NAPRAWY 8

2.5. ANTYWIRUS/DODATKOWE OPROGRANOWANIE 8

VII. SPOSOBY OCHRONY DOSTĘNE W PLAY 8

I. WSTĘP

W niniejszym dokumencie prezentujemy informacje wynikające z wypełnienia obowiązku informacyjnego wynikającego z przepisów Ustawy z dnia 16 lipca 2004r. Prawo telekomunikacyjne [Dz.U.2004.171.1800].

II. Informacje wynikające z art. 175e ust. 2 Prawa telekomunikacyjnego.

Informacje o:

- potencjalnych zagrożeniach związanych z korzystaniem przez abonentów z usług telekomunikacyjnych;
- rekomendowanych środkach ostrożności i najbardziej popularnych sposobach zabezpieczenia telekomunikacyjnych urządzeń końcowych przed oprogramowaniem złośliwym lub szpiegującym;
- przykładowych konsekwencjach braku lub nieodpowiedniego zabezpieczenia telekomunikacyjnych urządzeń końcowych;

są dostępne na stronie internetowej UKE: http://www.uke.gov.pl/

Informacje o sposobach ochrony bezpieczeństwa, prywatności i danych osobowych podczas korzystania z publicznie dostępnych usług telekomunikacyjnych **są dostępne na stronie internetowej UKE:** http://www.bip.uke.gov.pl/

III. Informacje wynikające z art. 175 ust. 2 Prawa telekomunikacyjnego.

Informacje o wystąpieniu szczególnego ryzyka naruszenia bezpieczeństwa sieci, wymagającego podjęcia środków wykraczających poza środki techniczne i organizacyjne podjęte przez P4, a także o istniejących możliwościach zapewnienia bezpieczeństwa i związanych z tym kosztach, będą dostępne na niniejszej stronie internetowej P4, niezwłocznie po wystąpieniu tego ryzyka.

IV. Informacje wynikające z art. 56 ust. 3 pkt 11 lit. e Prawa telekomunikacyjnego

Operator monitoruje w sposób ciągły ruch we własnej infrastrukturze Sieci Telekomunikacyjnej. Pomiary te są wykorzystywane do wymiarowania niezbędnych zasobów sieciowych jak i ustalania sposobu kierowania ruchu w sposób umożliwiający obsłużenie ruchu zgodnie z założonymi parametrami jakościowymi. Pomiarów dokonuje się na podstawie danych statystycznych generowanych przez elementy sieciowe, systemu monitorowania sygnalizacji oraz systemu testów End 2 End.

Elementy sieciowe mają również zaimplementowane mechanizmy zapobiegające przeciążeniom w sytuacjach ponadnormatywnego ruchu oferowanego w sieci (overload protection). W sytuacji mogącej spowodować przeciążenie elementów sieciowych, ruch przekraczający maksymalną pojemność obsługiwaną przez sieć jest

odrzucany lub jest obsługiwany z opóźnieniem (kolejkowanie). Mechanizm taki pozwala na prawidłową obsługę znaczącej części ruchu, która może być obsłużona poprzez dostępne zasoby i zapobiega znacznej degradacji jakości świadczonych usług w sytuacjach ponadnormatywnego ruchu oferowanego. W procesie tym nie są stosowane żadne mechanizmy priorytetyzowania ruchu danego typu.

Operator zapewnia, na odpowiednim poziomie agregacji sieci, konfigurację zapewniającą redundancję zasobów dla podtrzymania ciągłości i jakości świadczonych usług. W razie wystąpienia awarii urządzeń lub zasobów sieciowych, następuje przekierowanie ruchu do obsługi przez urządzenie/zasób redundantne, do czasu usunięcia awarii urządzenia i przywrócenia zasobów podstawowych.

V. Informacje wynikające z art. 56 ust. 3 pkt 12 i art. 63 ust.1 Prawa telekomunikacyjnego

Jakość usług w znacznej mierze zależy od zasięgu, który prezentowany jest w formie map zasięgu zgodnie z obecnymi informacjami na stronie: http://internet.play.pl/maps/map

VI. Informacje wynikające z art. 56 ust. 3 pkt 20 Prawa telekomunikacyjnego

Wypełniając obowiązek wynikający z art. 56 ust. 3 pkt 20 Prawa telekomunikacyjnego poniżej przekazujemy informację o zagrożeniach związanych

ze świadczonymi przez P4 usługami telekomunikacyjnymi, w tym o sposobach ochrony bezpieczeństwa, prywatności i danych osobowych. **Więcej informacji na temat sposobów i ochrony danych osobowych znajduje się na stronie http://www.bip.uke.gov.pl/**

1. ZAGROŻENIA

W niniejszym punkcie znajdują się informacje dotyczące zagrożeń, jakie mogą wystąpić używając telefonów komórkowych lub korzystając z Internetu za ich pośrednictwem. Zalecamy aby zapoznać się z przypadkami jakie mogą doprowadzić w szczególności do utraty cennych danych, które zawarte są w naszym telefonie czy też narazić nas na wysokie opłaty za realizację niezamierzonych przez nas drogich połączeń telefonicznych.

1.1. ZŁOŚLIWE OPROGRAMOWANIE

W przypadku instalacji złośliwego oprogramowania (czyli rozwiązania, aplikacji, które mogą powodować szkody w urządzeniach końcowych, niszczyć lub wykradać dane) na urządzeniu końcowym (np. telefon) może dojść (bez wiedzy użytkownika) do niezamierzonych operacji, w szczególności:

- samoczynny restart urządzenia końcowego (telefonu),
    - samoczynna wysyłka danych,
    - przekierowanie sms-ów bez wiedzy użytkownika,
    - przekierowanie na płatne numery bez wiedzy użytkownika.
- Instalowanie na urządzeniu końcowym aplikacji niewiadomego pochodzenia może spowodować utratę kontroli użytkownika nad urządzeniem oraz doprowadzić do utraty poufności danych osobistych.

1.2. POŁĄCZENIA/SMS NA NUMERY PREMIUM

Należy zwrócić szczególną uwagę na połączenia i SMS-y przychodzące z nieznanych numerów zachęcające nas do odesłania SMS-a czy też wykonania połączenia na wskazany numer. Nieświadomie na swój koszt wykonujemy wówczas kosztowne połączenie, a zarabia na tym nadawca.

1.3. SPOOFING – podmiana nadawcy

Zjawisko polegające na fałszowaniu, podmianie nadawcy tak aby zmylić odbiorcę i w konsekwencji wyłudzić dane, informacje wrażliwe, np. numer karty kredytowej, numery PIN, hasła, itp. Należy unikać przesyłania danych, informacji wrażliwych za pośrednictwem sms i/lub adresu e-mail.

1.4. KARTA SIM

Należy chronić swoją kartę SIM. Osoby trzecie mogą, z niezabezpieczonej karty SIM, skopiować informacje lub zadzwonić na nasz.

1.5. KRADZIEŻ DANYCH

Powszechnie dostępny z poziomu telefonu Bluetooth może okazać się skutecznym sposobem kradzieży danych z naszego urządzenia końcowego. Należy zwrócić uwagę na komunikaty pojawiające się w telefonie i wyłączać Bluetooth zawsze po zakończonej aktywności. Obecnie na rynku dostępne są również urządzenia/aplikacje, które wykorzystane w niewłaściwym celu mogą wykraść z pamięci urządzenia końcowego zawarte w nim dane (np. CSI Stick) – wystarczy

podpiąć się do urządzenia końcowego, dlatego nie należy pozostawiać urządzenia końcowego w zasięgu osób trzecich.

2. SPOSOBY OCHRONY URZĄDZEŃ KOŃCOWYCH I DANYCH

W niniejszym punkcie prezentujemy kilka z dostępnych na rynku sposobów ochrony zarówno telefonów jak i zawartych w nich cennych danych. Zachęcamy do zapoznania się z poniższymi informacjami.

2.1. BACKUP DANYCH

Zalecamy stosowanie dedykowanych aplikacji do backupu danych i ochrony urządzeń końcowych.
W urządzeniu końcowym należy robić backupy cennych dla użytkownika danych.
Numery telefonów (kontakty) i cenne informacje należy zapisywać na karcie SIM i/ lub karcie pamięci.

2.2. HASŁO/PIN

Zalecane jest, aby wprowadzić numer PIN/HASŁO do urządzenia końcowego. Ta 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.

2.3. OSOBY NIEUPOWAŻNIONE

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.
Urządzenia końcowe należy zostawiać poza zasięgiem osób nieupoważnionych.

2.4. AUTORYZOWANY SERWIS NAPRAWY

Naprawa urządzeń końcowych powinna być wykonywana w autoryzowanych serwisach naprawy. Pamiętaj aby oddając telefon do naprawy wyjąć kartę SIM.

2.5. ANTYWIRUS/DODATKOWE OPROGRAMOWANIE

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.

VII. SPOSOBY OCHRONY DOSTĘPNE W PLAY

Informujemy, że PLAY przygotował dla swoich klientów dedykowane usługi, które pozwolą podnieść poziom bezpieczeństwa w sieci. Poniżej prezentujemy opis poszczególnych usług.

PlayGuard – usługa która chroni smartfony i tablety przed złośliwym oprogramowaniem i zagrożeniami związanymi z korzystaniem z internetu oraz pozwala na zablokowanie, wyczyszczenie i namierzenie telefonu jeśli zostanie skradziony http://www.play.pl/obsluga-klienta/uslugi/play-guard/

Ochrona Internetu

Usługa, która chroni klienta (jego komputer) przed zagrożeniami związanymi z korzystaniem z Internetu http://www.play.pl/obsluga-klienta/uslugi/ochrona-internetu/

STOP SPAM i Blokady Premium

Udostępniamy klientowi możliwość zablokowania SPAMu wysyłanego do klienta z numerów Premium jak również różnego rodzaju blokady i limity związane z korzystaniem z usług Premium http://www.play.pl/obsluga-klienta/uslugi/numery-premium/