INFORMACJA O ZAGROŻENIACH ZWIĄZANYCH ZE ŚWIADCZONYMI USŁUGAMI ORAZ O SPOSOBACH OCHRONY BEZPIECZEŃSTWA, PRYWATNOŚCI I DANYCH OSOBOWYCH W SIECI SOFT PRO 2

I. ZAGROŻENIA ZWIĄZANE ZE ŚWIADCZONYMI USŁUGAMI

Korzystanie z usług telekomunikacyjnych, oprócz niewątpliwych korzyści wiąże się z pewnymi zagrożeniami. Do największych zagrożeń związanych z korzystaniem z usług dostępu do sieci Internet należy działalność podmiotów (przestępców) wykorzystujących możliwości, jakie niosą za sobą usługi telekomunikacyjne. Wśród największych zagrożeń w cyberprzestrzeni należy wymienić ataki na przeglądarki internetowe, ataki na pocztę elektroniczną, ataki na systemy operacyjne i aplikacje komputerowe, ataki w sieciach i serwisach społecznościowych, ataki na urządzenia mobilne. Nie należy lekceważyć również zagrożeń, które mogą na siebie ściągnąć również sami użytkownicy, w szczególności związanych z naruszeniem autorskich praw majątkowych lub ze względu na przejawy mowy nienawiści, ksenofobii czy rasizmu.

1. **Ataki na przeglądarki internetowe** Do ataku na przeglądarkę internetową może dojść w sytuacji gdy użytkownik odwiedza niezaufane witryny internetowe lub otwiera linki, które będą odsyłały do takiej witryny. Niejednokrotnie same przeglądarki ostrzegają przed wystąpieniem zagrożenia. Takich ostrzeżeń nie można lekceważyć. Szkodliwe oprogramowanie za pośrednictwem przeglądarki może zostać zainstalowane na skutek kliknięcia w pojawiającą się reklamę. Popularnym zagrożeniem jest atak phisingowy, mający na celu podszycie się pod danego usługodawcę np. wirtualne biuro obsługi klienta dostawcy usług lub serwis bankowości internetowej. Atak taki polega na zarejestrowaniu przez oszustów domen internetowych, które służą do kradzieży loginów i haseł użytkowników. W razie zamiaru logowania do serwisów internetowych przy użyciu loginów i haseł użytkownicy proszeni są o szczególną uwagę przy wprowadzaniu danych gdyż witryny zarejestrowane przez oszustów często do złudzenia przypominają autoryzowane strony internetowe zarządzane przez dostawcę usług. W celu zmniejszenia prawdopodobieństwa wystąpienia wyżej wskazanych zjawisk zalecamy naszym Abonentom także częste zmiany haseł dostępu do stron bankowych, jak i innych witryn internetowych, z których korzystają, tworzenie haseł długich, zawierających wielkie i małe litery, cyfry oraz znaki specjalne takie jak ‘;</{}][, których przestępca nie będzie mógł się domyślić oraz nie zapisywanie ich, aby nie zostały wykradzione.
2. **Ataki na pocztę elektroniczną** Z uwagi na fakt, iż najczęstszym sposobem rozprowadzania nielegalnego oprogramowania jest poczta e-mail, zalecamy nie otwierać wiadomości od nieznanych nadawców oraz zawierających wzbudzające podejrzenia

SOFT PRO 2 Spółka z ograniczoną odpowiedzialnością
ul. Czarna 8/L.U.2
41-200 Sosnowiec

KRS: 0000375306
REGON: 241806185
NIP: 6443474728

Sąd Rejonowy Katowice-Wschód w Katowicach
Wydział VIII Gospodarczy Krajowego Rejestru Sądowego
Kapitał zakładowy 100.000,00 PLN

załączników. Rekomendujemy ponadto, instalację programów antywirusowych w znaczącym stopniu poprawiających bezpieczeństwo korzystania z sieci Internet. Szczególnie należy uważać na zawartość korespondencji e-mail, które w tytułach korespondencji wykorzystują elementy zachęcające do zapoznania się z treścią wiadomości. Wszelkie tytuły informujące o przyznaniu środków pieniężanach, bonów, nagród należy traktować z dużym stopniem podejrzliwości. Szczególnie jeżeli nie braliśmy udziału w żadnym wydarzeniu z jakim mogłaby się wiązać jakakolwiek wygrana.

3. **Ataki na systemy operacyjne i aplikacje komputerowe** Rekomendujemy instalację oprogramowania antywirusowego i jego bieżącą aktualizację. Dotyczy to również wszelkich zainstalowanych aplikacji i programów komputerowych, gdyż nieaktualne wersje mogą być podatne na zagrożenia zewnętrzne.
4. **Ataki w serwisach społecznościowych** Zalecamy również z należytą ostrożnością korzystać z portali społecznościowych. Zamieszczone w nich dane (przez samych użytkowników) mogą stanowić kopalnię wiedzy na temat samego abonenta a także członków jego rodziny, w tym osób nieletnich. Internet ułatwia poznawanie nowych ludzi, jednakże użytkownicy nigdy nie mają pewności, kto znajduję się po drugiej stronie sieci. Osoby poznawane za pośrednictwem Internetu mogą okazać się groźnymi przestępcami, dlatego zalecamy zachować szczególną ostrożność w kontaktach z ludźmi poznanymi przez Internet. W szczególności jeżeli te osoby proszą nas o udzielenie pomocy w postaci środków finansowych. W zakresie korzystania z serwisów społecznościowych aktualne pozostają postulaty związane z wykorzystaniem bezpiecznych i silnych haseł oraz unikania logowania się na urządzeniach, które łączą się do ogólnodostępnych sieci.
5. **Ataki na urządzenia mobilne** Jeżeli korzystasz np. ze smartfona staraj się unikać łączenia z siecią poprzez ogólnodostępne sieci WiFi. Jeżeli instalujesz aplikacje mobilne staraj się korzystać ze źródeł producenta danej aplikacji. Możliwe naruszenia praw osób trzecich przez użytkowników Internetu.
6. Kolejnym niebezpieczeństwem, jest możliwość naruszenia praw autorskich przez samych użytkowników. Przestępcy internetowi rozpowszechniają w sieci dokumenty i utwory chronione prawem autorskim. Użytkownicy korzystający z plików lub oprogramowania pochodzących z nielegalnych źródeł dopuszczają się przestępstwa, za co grozi odpowiedzialność karna. Użytkownicy powinni zdawać sobie sprawę z tego, że nie są w sieci anonimowi. Wszelkie ich działania pozostawiają w sieci trwałe ślady. Chodzi również o te działania, które dotyczą komentowania bieżących wydarzeń. Nie chcemy zniechęcać do udziału w wymianie myśli i poglądów, ale jednocześnie uczulamy, aby komentarze użytkowników nie nawoływały do nienawiści, ksenofobii, rasizmu. Odpowiedzialnością karną grozi również tworzenie materiałów dyskredytujące innych użytkowników sieci Internet. Kolejnym zagrożeniem dla użytkowników jest ryzyko zakupu rzeczy na odległość. Zalecamy, żeby sprawdzać sklepy internetowe, z których korzystamy oraz osoby, od których kupujemy. W tym celu pomocne są fora internetowe, dzięki którym możemy poznać opinię o naszych kontrahentach. Najczęściej już weryfikacja regulaminu sklepu internetowego pozwala przypuszczać, czy mamy do czynienia z wiarygodnym sprzedawcą.
7. **Inne zagrożenia** Należy zwrócić szczególną uwagę na zagrożenia jakie sieć Internet niesie dla dzieci. Każdy użytkownik sieci jest narażony na niechciane treści, szczególnie na materiały pornograficzne, zawierające przemoc, nawołujące do nienawiści, ksenofobii, rasizmu, popełniania różnego rodzaju przestępstw, zachęcające do hazardu. Wskazane

wyżej treści są szczególnie niebezpieczne dla kształtujących się dopiero umysłów dzieci i młodzieży, dlatego zalecamy rodzicom, aby zwracali szczególną uwagę na treści przeglądane przez ich podopiecznych. Zalecamy również zwracać szczególną uwagę na osoby, z którymi kontaktują się dzieci.

Następnym zagrożeniem ze strony przestępców jest możliwość wykorzystania danych Użytkowników w celu podszycia się pod nich, co w znaczący sposób może wpłynąć na ich życie i reputację. Nie należy również lekceważyć wpływu dostępu do sieci dla zdrowia psychicznego użytkowników, w szczególności w zakresie ryzyka uzależnienia się od korzystania z usług internetowych.

II. SPOSOBY OCHRONY BEZPIECZEŃSTWA, PRYWATNOŚCI, DANYCH OSOBOWYCH

W trosce o ochronę bezpieczeństwa, prywatności oraz danych osobowych Użytkowników dokładamy wszelkich starań, aby zabezpieczyć ich interesy. Dostęp do danych użytkowników posiadają tylko i wyłącznie upoważnieni pracownicy dokonujący czynności związanych ze świadczonymi przez nas usługami. Wszelkie dane naszych Klientów oraz hasła dostępu do tych danych dostępne są za pomocą szyfrowanych połączeń zabezpieczonych certyfikatem. Dane zabezpieczone są specjalistycznym oprogramowaniem, które praktycznie uniemożliwia ich przejęcie przez osoby trzecie, jak również zmianę ich treści przez osoby nieuprawnione. Ze względów bezpieczeństwa nie możemy wspominać o większości skomplikowanych metod i systemów stosowanych przez nas do ochrony bezpieczeństwa, prywatności oraz danych osobowych użytkowników. Aby zapewnić bezpieczeństwo użytkowników zalecamy odpowiednie, minimalizujące ryzyko negatywnych skutków, korzystanie z sieci Internet zgodnie z rekomendacjami określonymi w części I. Z informacjami o przetwarzaniu Państwa danych osobowych mogą się Państwo zapoznać za pośrednictwem dokumentów opublikowanych pod adresem iod@softpro2.pl