DOI: 10.15199/13.2016.12.7

Zagrożenia cyberprzestrzeni

(Cyberspace threats)

mgr inż. OLGA PAWŁOWSKA

Instytut Maszyn Matematycznych, Warszawa

Streszczenie

Cyberprzestrzeń jest nieodzownym elementem współczesnego świata. Większość osób korzysta z dóbr dostarczanych przez cyberprzestrzeń i jednocześnie może paść jej ofiarą. Celem artykułu jest przedstawienie wybranych, najczęściej spotkanych zagrożeń, często pomijanych i niezauważanych.

Słowa kluczowe: Cyberprzestrzeń, zagrożenia, e-usługi

Abstract

Cyberspace is an integral part of the modern world. It is present in every area of human life. Most people use services supplied by cyberspace, but anyone can become victim of it. The aim of this article is to present selected and most often encountered cyberspace threats.

Keywords: Cyberspace, threats, e-services

Cyberprzestrzeń, jednoznaczna z pojęciem sieci Internet i jej zasobów, stanowi przedmiot zainteresowania badaczy wielu dziedzin, m.in. wojskowości (armia, organy zabezpieczające państwo), nauk społecznych i humanistycznych i innych. O ile pierwsi z nich skupiają się na szansach i zagrożeniach, jakie z cyberprzestrzeni wynikają dla państwa i jego instytucji, o tyle badacze nauk społecznych i humanistycznych koncentrują się na możliwościach, wartości tworzonej dla społeczeństwa i zagrożeniach, jakie z funkcjonowania w cyberprzestrzeni mogą płynąć dla pojedynczych osób oraz ich grup. W aspekcie zagrożeń dla użytkownika lub grup użytkowników zostaną dalej omówione realne niebezpieczeństwa ze strony wirtualnego świata – cyberprzestrzeni.

Wartości cyberprzestrzeni

Rozpatrując zagadnienia i problemy związane z cyberprzestrzenią nie można skupiać się na jej negatywnych stronach, na zagrożeniach, na które jesteśmy narażeni. Siła oddziaływania cyberprzestrzeni na człowieka wynika z jej pozytywnych stron, z wartości, które tworzy i możliwości, które oferuje. Atutem cyberprzestrzeni jest dostęp do e-usług, z dowolnego miejsca, w dowolnym czasie, przez 24 godziny na dobę, przez 7 dni w tygodniu.

Jednymi z ważniejszych e-usług oferowanych w cyberprzestrzeni są usługi związane z edukacją i pracą, umożliwiające stały rozwój wiedzy i kompetencji użytkownika oraz znalezienie i wykonywanie pracy, w pełni lub częściowo zdalnie. W cyberprzestrzeni studia i kursy dostępne są on-line, w trybie synchronicznym i asynchronicznym. Publikacje naukowe i inne niosące wiedzę, dostępne są w formie elektronicznych dokumentów. Praca może być świadczona zdalnie w uwarunkowanym prawnie systemie tele-pracy, poza stacjonarnym stanowiskiem pracy.

Zdalne kształcenie, jak i tele-praca charakteryzują się:

- dowolnością miejsca i czasu podejmowanych aktywności i związanym z tym brakiem konieczności dojazdu do miejsca pracy;
- elastycznym czasem zajęć dydaktycznych i pracy, pozwalającym na indywidualizację czasu wykonywania tych aktywności.

Użytkownicy zasobów oferowanych w cyberprzestrzeni z coraz większym zaufaniem korzystają z e-usług. Jednym z pierwszych, który zauważył potencjał cyberprzestrzeni, jest sektor bankowy. E-bankowość umożliwia zdalne prowadzenie osobistych finansów na kontach bankowych. Dzięki e-usługom bankowym miał szansę rozwinąć się inny obszar gospodarki – handel elektroniczny. W 2014 r. zanotowano 13,4 tys. e-sklepów, udział e-handlu w sprzedaży ogółem wynosił w Polsce w 2014 r. ok. 4–5% [1].

Cyberprzestrzeń stwarza także możliwość obcowania z kulturą – oferuje filmy, muzykę, wirtualne wystawy i muzea [2].

Dostępność i swoboda korzystania z e-usług spowodowała zmniejszenie czujności na ewentualne niebezpieczeństwa, jakie związane są z funkcjonowaniem cyberprzestrzeni.

Niebezpieczeństwa cyberprzestrzeni

Stwierdzenie R. Tadusiewicza wskazujące na źródła techniczne i ludzkie zagrożeń cyberprzestrzeni [3] jest o tyle prawdziwe, o ile weźmiemy pod uwagę także skutki wywołane przez funkcjonowanie cyberprzestrzeni. Pierwotnie źródłem zagrożeń jest człowiek - on konstruuje elementy technologii i nadzoruje prawidłowe ich wykonanie. Jeśli więc zawodzi technika, winny temu jest człowiek. Jeśli jednak rozpatrywać problem jako zagrożenia wynikające z techniki oraz zagrożenia wynikające z ludzkiego używania technologii, to zagrożenia cyberprzestrzeni, można ująć, na podstawie analizy literatury, w następujących grupach:

- zagrożenia dla zdrowia fizycznego,
- zagrożenia dla zdrowia psychicznego, w tym emocjonalne,
- zagrożenia związane z technologią,
- zagrożenia kryminalne.

Zagrożenia dla zdrowia fizycznego

Zagrożenia z grupy zagrożeń zdrowotnych to m.in. zaburzenia rozwoju fizycznego, otyłość i inne schorzenia (np. cukrzyca czy nadciśnienie tętnicze) silnie związane z brakiem ruchu. Zbyt długie przebywanie przed ekranem komputera może także powodować nerwice, ogólne zmęczenie i zaburzenie funkcji poznawczych, np. opóźnienia reakcji na różnorodne bodźce (zaburzenia percepcji), zachowania kompulsywne, roztargnienie, poczucie zagubienia, problemy z logicznym myśleniem – jego utrata lub ograniczenie, zaburzenia pamięci [4]. Długie, pozbawione ruchu, jednostajne wpatrywanie się w ekran komputera w sytuacji, gdy osoba np. ma aktywną lub utajnioną wersję padaczki, może doprowadzić do napadu lub aktywizacji tej choroby.

Zagrożenia dla zdrowia psychicznego

Drugą grupą zagrożeń są zaburzenia zdrowia psychicznego. Najczęściej spotykanym skutkiem korzystania z Internetu jest uzależnienie od niego. Uzależnienie od Internetu przejawia się [5]:

- tolerancją – osoba uzależniona potrzebuje wydłużać czas przebywania w sieci Internet, aby utrzymać stały poziom zadowolenia,
- zespołem abstynencyjnym, który pojawia się już w kilka dni od zaprzestania korzystania z sieci. Zespół abstynencyjny możemy diagnozować, gdy u osoby występują minimum dwa objawy spośród wymienionych poniżej:
  - o obsesyjne myślenie o Internecie i tym, co się w nim dzieje; traktowanie Internetu jako źródła rozwiązania wszystkich problemów,
  - o obniżenie nastroju w sytuacji niebycia w sieci,
  - o wybuchy złości w momencie ograniczania dostępu do Internetu,
  - o zaniedbywanie realnych kontaktów towarzyskich na rzecz prowadzenia życia towarzyskiego w sieci,
  - o pobudzenie psychoruchowe,
  - o stany lękowe związane z dostępem do sieci Internet,
  - o fantazje i marzenia związane z Internetem,
  - o dowolne bądź mimowolne poruszanie palcami w sposób charakterystyczny dla korzystania z klawiatury komputerowej,
  - o próby wymuszonego ograniczenia korzystania z sieci Internet.

Można stwierdzić, że oddziaływanie cyberprzestrzeni jest równie uzależniające, a więc także niebezpieczne dla człowieka, jak popularne używki kojarzone ze słowem „uzależnienie”- alkohol, narkotyki, czy też coraz bardziej popularne dopalacze.

Zaniedbywanie posiadanych obowiązków, pogorszenie kontaktów rodzinnych, osłabienie więzi międzyludzkich, tych ze świata rzeczywistego to kolejny, negatywny skutek uboczny korzystania z Internetu.

Zagrożenia związane z techniką

Kolejną wyróżnioną grupą zagrożeń są te związane z techniką. Zdarza się, że technika zawodzi, przestaje działać. O ile zjawisko to odbija się tylko w sposób emocjonalny na osobach, które nie mogą zrealizować swojej silnej potrzeby do przebywania w sieci, to nie jest to groźne, Gorzej, gdy przestaje działać sprzęt, od którego prawidłowego funkcjonowania zależy działalność instytucji czy przedsiębiorstwa ze skutkami wpływającymi na zyski finansowe. Niewłaściwe funkcjonowanie techniki może też mieć wpływ na ludzkie życie np. przy awarii systemu monitoringu medycznego. Sytuacje groźnych awarii technicznych nie występują często, gdyż właściwie wykonany system (infrastruktura sprzętowa) posiada zdublowane podstawowe elementy zabezpieczające jego właściwe funkcjonowanie zapobiegające przerwie w działaniu [6].

Zagrożenia kryminalne

Awarie techniczne mogą być wynikiem ataków hackerskiech, które należą do ostatniej omawianej grupy zagrożeń – przestępstw kryminalnych. Przykładami zagrożeń kryminalnych są:

- wspomniane ataki hackerskie,
- piractwo komputerowe,
- oszustwa handlowe (np. na aukcjach internetowych),
- phishing (podszywnaie się pod osobę lub instytucję),
- masowe wysyłanie wiadomości – spam,
- cyberprzemoc.

Ataki hakerskie to działania przestępcze wykorzystujące niedopracowania, luki bezpieczeństwa w systemach operacyjnych, programach komputerowych, sieciach komputerowych. Atakami mogą padać osoby prywatne, osoby znane publicznie jak i instytucje. Działalność hakerów polega na wykradaniu danych, podmianie elementów np. na stronach internetowych, kradzieżach i innych nielegalnych działaniach. Ataki te mogą być wykonywane dla żartu lub mogą być bardzo poważnym zagrożeniem, gdy skierowane są na serwery zarządzające procesami administracyjnymi lub gospodarczymi.

Piractwo komputerowe to sprzeczne z prawem działania polegające na posługiwaniu się wytworami autorskimi uiszczenia opłaty za korzystanie z nich (bez nabycia majątkowych praw autorskich na określonym polu eksploatacji utworu/ów). Działania te opierają się na kopiowaniu utworów i bezpłatnym przekazywanie ich między zainteresowanymi osobami lub na masowej produkcji fałszywych produktów i sprzedawania ich pod marką oryginalnych. Zainteresowaniem piratów komputerowych najczęściej padają filmy, programy komputerowe, muzyka, czy też zdjęcia udostępniane w sieci Internet. Osoby pobierające muzykę czy filmy z sieci powinny być świadome, czy robią to legalnie czy nielegalnie. Nie wszyscy jednak zdają sobie sprawę, że zdjęcia nieodpłatnie dostępne w cyberprzestrzeni także posiadają licencje i korzystanie z nich bez respektowania prawa autorskiego, jest przestępstwem.

Handel z wykorzystaniem Internetu (e-commerce, e-zakupy) jest narażony na oszustwa, które najczęściej dotyczą aukcji internetowych, i wiążą się z nieotrzymaniem kupionego przedmiotu lub otrzymaniem przedmiotu niezgodnego z opisem. Oszustwa w e-handlu również wiążą się z kradzieżami środków finansowych powodowanymi nieprawidłowym, nieuważnym korzystaniem z bankowości lub płatności elektronicznej.

Phishing jest metodą kradzieży danych polegającej na podszywaniu się pod osobę lub podmiot, bazującej na nieświadomości i nadmiernym zaufaniu użytkownika. Przestępcy

wysyłają wiadomości e-mail, bliźniaczo podobne do wiadomości oryginalnej, w której proszą o zalogowanie się na określonej stronie internetowej, także bliźniaczo podobnej do oryginalnej, i o zmianę hasła lub np. uaktualnienie swoich danych, czyli wykonania czynności z użyciem danych wrażliwych. W ten sposób użytkownik przekazuje wszelkie niezbędne informacje do pełnego zarządzania kontem.

Cyberprzemoc jest rodzajem przemocy odbywającym się w sieci Internet, m.im. z wykorzystaniem telefonów komórkowych [7]. Problem ten dotyczy głównie dzieci i młodzieży, osoby dorosłe również padają jego ofiarą, z drugiej strony – stosują tego typu przemocy wobec innych. Do działań określanych mianem cyberprzemocy zalicza się m.in:

- obrażanie, wyzywanie, straszenie poniżanie kogoś w Internecie lub przy użyciu telefonu, rzadko pod własnym nazwiskiem, zazwyczaj w sposób anonimowy;
- robienie komuś zdjęć lub nagrywanie filmów z jego udziałem, ale bez jego zgody i późniejsze upublicznianie ich;
- upublicznianie w Internecie lub dystrybuowanie telefonem komórkowym zdjęć, nagrań filmowych lub tekstów, które są dla kogoś obraźliwe lub go ośmieszają;
- udawanie, podszywanie się pod kogoś w sieci Internet/z wykorzystaniem telefonu komórkowego.

Spam, czyli masowe wysyłanie listów elektronicznych zawierających wiadomości niechciane, niepotrzebne, nieważne, na tle innych zagrożeń cyberprzestrzeni nie wydaje się być zagrożeniem szczególnie niebezpiecznym, raczej jest dużą uciążliwością dla odbiorców spamu. Jest jednak działalnością szkodliwą, która:

- często zawiera złośliwe oprogramowanie, np. wirusy uniemożliwiające poprawne działanie komputerów,
- spowalnia działanie serwerów poprzez konieczność przetworzenia informacji,
- powoduje "zatykanie się" łączy.

Wiadomości spam, nawet mimo automatycznego umieszczania ich w specjalnym folderze „spam"/„niechciane wiadomości", powodują marnowanie czasu, gdyż wymuszają konieczność ich kasowania, a czasem także zapoznania się z nimi.

Po liczbie wymienionych przykładów widać, że przestępczość w cyberświecie jest rozwinięta na podobna skalę do przestępczości w realnym świecie. Warto wspomnieć, że kara za cyberprzestępczość ma swoje prawne umocowanie w realnym świecie i teoretycznie przestępcy nie powinni być bezkarni.

Wnioski

Cyberprzestrzeń stała się codziennością dla współczesnego człowieka. Elementem bez którego większość ludzi nie jest w stanie funkcjonować. Co więcej, współczesny człowiek pozytywnie przyjmuje stały rozwój technologii informacyjno-komunikacyjnych, które umożliwiają głębsze wpuszczenie cyberprzestrzeni do realnego życia. Warto pamiętać, że zagrożenia, jakie niesie cyberprzestrzeń, są jej drugim obliczem, na które użytkownicy zbyt często nie zwracają się uwagi.

Literatura

[1] Jakubik A,, *Zespół uzależnienia od Internetu*, „Studia Psychologica", nr 3 (2002), s. 133–142.

[2] Kłosiewicz-Górecka U., *Zmiany w handlu w okresie chwiejnego rozwoju gospodarczego Polski*, Warszawa 2015, www.ibrkk.pl/f/?Konferencja_IBRKK_U_K-G_02.03.2015.pdf [14.10.2015].

[3] Ordyńska O., Pawełczak M., *Wirtualne muzea. W poszukiwaniu edukacyjnych zastosowań*, [w:] „Prace naukowo-badawcze Instytutu Maszyn Matematycznych, Realny i wirtualny świat", 2/2009", s. 33–45.

[4] Tadeusiewicz R., *Zagrożenia w cyberprzestrzeni*, „NAUKA", 4/2010, s. 36.

[5] Tanaś M., *Medyczne skutki uboczne kształcenia wspomaganego komputerowo*, „Toruńskie Studia dydaktyczne" 1993, s. 107–109.

[6] Wolińska J. M., *Komputer (gry, Internet) – konieczność, pasja, zagrożenie, uzależnienie* [w:] Kwiatkowska G. E. (red.), *Wybrane zagadnienia psychologii współczesnej*, Wydawnictwo Uniwersytetu Marii Curie-Skłodowskiej, Lublin 2004, s. 185–196.

Netografia

[7] Kampania medialna Baw się w sieci bezpiecznie, http://www.saferinternet.pl/pl/kampanie-medialne/baw-sie-w-sieci-bezpiecznie [11.01.2015].