mgr Agata ZIÓŁKOWSKA[1]

BIAŁY WYWIAD JAKO OGÓLNODOSTĘPNA FORMA CYBERINWIGILACJI A BEZPIECZEŃSTWO DANYCH UŻYTKOWNIKÓW URZĄDZEŃ MOBILNYCH

Słowa kluczowe: *biały wywiad, inwigilacja, cyberinwigilacja, bezpieczeństwo w cyberprzestrzeni*

STRESZCZENIE

Techniki informacyjne zdominowały XXI wiek. Szybki rozwój technologii i komunikowanie się za pomocą urządzeń mobilnych stwarza duże problemy związane z bezpieczeństwem ich użytkowników. Biały wywiad, który polega na pozyskaniu informacji z otwartych źródeł informacji (Open Source Intelligence), ma coraz większe znaczenie. Z tego powodu bezpieczeństwo danych użytkowników sieci online jest zagrożone. Autorka tekstu zwraca uwagę na źródła pozyskiwania informacji o użytkownikach urządzeń mobilnych z wykorzystaniem cyberprzestrzeni, które rzutują na ich bezpośrednie bezpieczeństwo w Internecie.

„W coraz bardziej rozbitym środowisku geopolitycznym punkt ciężkości wydaje się przesuwać od rządów w kierunku korporacji, a nawet jednostek prywatnych, które mają dostęp do większego potencjału wywiadowczego i informacyjnego, niż kiedykolwiek w historii miał jakiś rząd. Co będzie dalej? …”
Eamon Javers
[Agent Handlarz Prawnik Szpieg, 2010]

Wstęp

Rozwój Internetu radykalnie zmienił życie jego użytkowników doprowadzając do powstania nowych wyzwań dla ochrony prywatności. Możliwość dostępu do sieci z dowolnego miejsca na Ziemi sprawiła, iż podmioty (firmy, rząd, instytu-

[1] Agata Ziółkowska jest doktorantką Wydziału Bezpieczeństwa Narodowego Akademii Sztuki Wojennej.

cje) oraz prywatne osoby decydują się na przenoszenie codziennej aktywności do cyberprzestrzeni. Wielu użytkowników urządzeń mobilnych nie jest świadomych do jakich celów wykorzystywane są udostępniane przez nich informacje oraz w jaki sposób mogą one im zaszkodzić. Prywatność będąca niezbywalnym prawem każdego człowieka naruszana jest codziennie przez osoby trzecie, mimo iż to obszar, w który nie powinno się wkraczać bez pozwolenia. Każdy Internauta powinien sobie uświadomić, że w Internecie nie ma prywatności, a cała aktywność online może być rejestrowana i analizowana by skutecznie ich inwigilować. Prywatność jest cenną wartością, którą uregulowano zarówno w przepisach prawa krajowego, jak i na szczeblu międzynarodowym w tym unijnym. Zgodnie z art.49 Konstytucji RP z 1997 roku „Zapewnia się wolność i ochronę tajemnicy komunikowania się…", jednak ten przepis prawa niestety jest coraz częściej łamany. Wielu użytkowników nie wyobraża sobie życia bez ekspresowego dostępu do poczty elektronicznej, internetowej bankowości, portali społecznościowych, zakupów „online" czy najświeższych informacji. Niestety rzadko zapoznają się z polityką prywatności znajdującą się w regulaminach serwisów społecznościowych czy stron internetowych co wiąże się z brakiem anonimowości w sieci, kradzieżą danych wrażliwych oraz ogólną inwigilacją i infiltracją. Urządzenia mobilne umożliwiające śledzenie swoich użytkowników są dobrowolnie przez nich kupowane i noszone praktycznie cały czas przy sobie, a brak świadomości na temat cyberinwigilacji wpływa na bezpieczeństwo ich danych. Dlatego też, obecnie zwraca się szczególną uwagę na podstawowy cel strategiczny w obszarze bezpieczeństwa i ochrony internautów w cyberprzestrzeni. Zjawisko inwigilacji występowało od zawsze, natomiast obecnie do jej przeprowadzania nie wykorzystuje się tylko osobowych źródeł informacji a komputery w zaciszu domowym.

Celem artykułu jest krótkie przedstawienie przykładowych sposobów cyberinwigilacji z wykorzystaniem ogólnodostępnych źródeł informacji tj. białego wywiadu towarzyszącemu społeczeństwu informacyjnemu, wynikającemu z rozwoju technologii oraz błędów jakie popełniają użytkownicy urządzeń mobilnych w zakresie bezpieczeństwa informacji. Autorka dąży do wskazania głównych zagrożeń oraz możliwych działań, które pozwolą na ich zapobieganie.

Charakterystyka zagadnienia

Inwigilacja ludności występowała na długo przed szerokim udostępnieniem jej nowoczesnych technologii, dlatego nie jest zaliczana do nowego zjawiska. Pojęcie

inwigilacji, oznacza tajny nadzór[2], a także zespół czynności operacyjno-rozpoznawczych skupionych na śledzeniu i kontrolowaniu konkretnej osoby[3]. Reasumując inwigilacja to zakamuflowany sposób zorganizowanego zbierania informacji[4]. Służby wywiadowcze wraz z postępem technologicznym zaczęły rozwijać i wprowadzać nowe techniki inwigilacyjne, które doprowadziły do powszechnej inwigilacji w cyberprzestrzeni zwanej cyberinwigilacją.

W społeczeństwie informacyjnym inwigilacja elektroniczna obejmuje kontrolę rozmów telefonicznych, wiadomości tekstowych czy danych transferowych. Użytkownicy Internetu udostępniając swoje prywatne dane np. na portalach społecznościowych czy blogach takie jak: wykształcenie, aktualne miejsce zamieszkania, zawiązki, przyjaciół, zainteresowania i harmonogram swojego dnia, ułatwiają wywiadowcom czy firmom marketingowym tworzenie baz danych i predyspozycji każdego internauty, dlatego cyberprzestrzeń będąc idealnym otwartym źródłem informacji wykorzystywana jest nie tylko przez służby specjalne ale także przez agencje detektywistyczne, wywiadownie gospodarcze, przedsiębiorców czy małżonków[5]. W związku z tym biały wywiad, który polega na prowadzeniu czynności pozyskania informacji na podstawie źródeł powszechnie otwartych i dostępnych, jest tak samo wykorzystywany przez sektory prywatne jak i organy państwowe[6]. Sformułowanie biały wywiad czy otwarte źródła informacji na dzień dzisiejszy nie funkcjonuje w przepisach polskiego prawa, niemniej jednak wiele instytucji proponują własne definicje. Biały wywiad jest analizą informacji pozyskaną za pomocą legalnych źródeł uznawaną za najbardziej przyjazną i bezpieczną formę zdobywania tajemnic[7]. Charakter legalnego pozyskania informacji z sieci publicznej i odpowiednia analiza, umożliwia pionom operacyjnym reagować w odpowiednim czasie na potencjalne zagrożenia[8].

---

[2] *Słownik języka polskiego PWN*, witryna internetowa o nazwie www.sjp.pwn.pl [dostęp: 17.03.2017].

[3] T. Hanausek, *Kryminalistyka. Zarys wykładu*, Kraków 2005, s. 152.

[4] P. Wroński, *Czas nielegałów. Krótki kurs kontrwywiadu dla amatorów*, Fronda, Warszawa 2016, s. 78.

[5] W. Gogołek, *Komunikacja sieciowa. Uwarunkowania, kategorie, paradoksy*, ASPRA-JR, Warszawa 2010, s. 26.

[6] M. Minkina, *Gry wywiadów. Sztuka wywiadu w państwie współczesnym*, Rytm, Warszawa 2014, s. 41.

[7] K. Mroziewicz, *Czas pluskiew*, Wydawnictwo „Sensacje XX wieku", Warszawa 2007, s. 334.

[8] B. Sienkiewicz, *Historia pewnego złudzenia*, Przegląd Bezpieczeństwa Wewnętrznego, 20-lecie uop/abw, wydanie specjalne, s. 52, https://www.abw.gov.pl/pl/pbw/publikacje/przeg-

Rozwój Internetu przyczynił się do sformułowania definicji cyberprzestrzeni, jej bezpieczeństwa i postępu technologicznego w sektorze urządzeń mobilnych. W chwili obecnej pojęcie „cyberprzestrzeni" oznacza wirtualną przestrzeń, w której urządzenia mobilne, komputery czy media cyfrowe przesyłają pomiędzy sobą informacje wykorzystując do tego globalny system jakim jest Internet. Innymi słowy, cyberprzestrzeń to system powiązań internetowych z prężenie funkcjonującą przestrzenią komunikacyjną[9].

Z tego względu, że życie użytkowników Internetu zostało przeniesione do świata cyfrowego, zaczęto z większą precyzją dbać o bezpieczeństwo przesyłanych drogą elektroniczną informacji, czego konsekwencją było stworzenie terminu „cyberbezpieczeństwo". Zagadnienie to związane jest także z bezpieczeństwem narodowym. Definicji cyberbezpieczeństwa jest wiele, jednak większość określa bezpieczeństwo w cyberprzestrzeni w zakresie zabezpieczeń i działań, które mogą być wykorzystane do ochrony domen zarówno wojskowych jak i cywilnych. Chronione są przede wszystkim: oprogramowanie, dane firmy, sprzęt komputerowy, ludzie, dokumentacja oraz dane, które umożliwią konkurencji zdobycie wiedzy o kontrahentach czy informacjach handlowych.

Innym określeniem bezpiecznego przesyłania danych w Internecie jest bezpieczeństwo informacyjne. Według wielu definicji oznacza ono ochronę informacji przed niepożądanym dostępem, ujawnieniem czy zniszczeniem. Istotnymi zagrożeniami dla bezpieczeństwa w cyberprzestrzeni są także awarie technologiczne systemów czy sieci energetycznych[10].

Powszechny dostęp do Internetu z wykorzystaniem sieci bezprzewodowych wpłynął na rozwój technologii urządzeń mobilnych tj.: telefonów komórkowych, urządzeń nawigacji satelitarnej, przenośnych konsol, palmtopów, czytników e-booków, tabletów czy odtwarzaczy multimedialnych[11]. Pozwalają one na odbieranie, przetwarzanie a następnie wysyłanie danych bez konieczności podłączenia się do sieci przewodowych. Urządzenia te zaliczane do mini komputerów przenoszone są przez swoich użytkowników bez zaangażowania dodatkowych środków,

---

lad-bezpieczenstw-1/569,PrzegladBezpieczenstwaWewnetrznegoWYDANIESPECJALNE.html [dostęp: 20.02.2017].

[9] T. Szubrycht, *Cyberterroryzm jako nowa forma zagrożenia terrorystycznego*, Zeszyty Naukowe Akademii Marynarki Wojennej, nr 1, 2005, s. 173–175.

[10] M. Marczyk, *Bezpieczeństwo teleinformatyczne wobec ataków cyberterrorystycznych*, Difin, Warszawa 2014, s. 50.

[11] M. Szkotak, *Technologie mobilne*, iTst@rt Wydawnictwo Informatyczne, Piekary Śląskie 2011.

a ich wykorzystanie nie ogranicza się tylko do sprawdzenia poczty elektronicznej[12], dlatego w rzeczywistości użytkownicy urządzeń mobilnych są od nich coraz bardziej zależni[13]. Z powodu braku fizycznego ograniczenia dostępu do danej sieci cyberinwigilacja osób trzecich nie należy do skomplikowanych czynności[14].

Źródła pozyskiwania informacji

Społeczeństwo informacyjne słysząc sformułowanie „wyszukiwanie informacji" wyobraża sobie główne okno podstawowej wyszukiwarki w sieci WWW i prawidłowo, ponieważ może ona służyć nie tylko do wyszukiwania informacji naukowych czy znalezienia adresu sklepu lecz także do początkowej fazy cyberinwigilacji. Potencjalny użytkownik przed swoim komputerem w zaciszu domowym, może wyszukać informację m.in. na temat: edukacji, w tym szkół jakie ukończyła osoba sprawdzana; zdjęć na których się znajduje; profili na serwerach społecznościowych, aukcyjnych czy sklepach internetowych a także jeżeli posiada adres e-mail może wyszukać powiązania między osobami, organizacjami, przedsiębiorstwami, domenami czy adresami IP. Dzięki mobilnej możliwości dostępu do sieci, każdy użytkownik może wyszukać interesujące go informacje lub dodać je do swojego konta na profilu społecznościowym. Smartfony jako minikomputery ułatwiają taką wymianę informacji. Aby móc opisać szczegółowo zagrożenie jakie czyha na potencjalnego Internautę, warto znać specyfikację najpopularniejszego urządzenia mobilnego jakim jest smartfon. Smartfony charakteryzują się dotykowym ekranem umożliwiającym rysowanie a nawet mającym funkcję elektronicznego podpisu. Przeważnie nowe urządzenia posiadają dwie wbudowane kamery z czego jedna zlokalizowana jest z przodu urządzenia, natomiast druga z tyłu. Jakość tych zdjęć jest na tyle dobra, że użytkownicy często wykorzystują telefon jako ksero. W połączeniu z bardzo dobrym mikrofonem można udźwiękowić film, a antena Wi-Fi, która umożliwia łączenie z Internetem, wykorzystuje smartfon jako router. Do połączenia ze sobą dwóch telefonów wykorzystuje się antenę Bluetooth, a do ustalenia przybliżonej lokalizacji anteny GPS (*Global Positioning System*)[15]. Te mini komputery umożli-

[12] M. Miłosz, *Systemy mobilne. Informatyka gospodarcza*, tom 4, C.H. Beck, Warszawa 2010.

[13] C. Sandvig, *An Initial Assessment of Cooperative Action in Wi-Fi Networking*, Telecommunications Policy, vol. 28(7/8), s. 579–602.

[14] B. Zieliński, *Bezprzewodowe sieci komputerowe*, Helion, Gliwice 2000, s. 142–160.

[15] A.Z. Wassilew, *Technologie „podłączenia" w społeczeństwie mobilnym*, Zeszyty Naukowe Uniwersytetu Szczecińskiego, Studia Informatica, Nr 28, s. 470–473.

wiają swoim użytkownikom stałą wymianę informacji a wywiadowcom dostarczają nieograniczony dostęp do aktualnych danych. Autorka w dalszym opracowaniu zwraca uwagę na źródła pozyskania informacji zamieszczonych w Internecie przez użytkowników urządzeń mobilnych, które mogą być wykorzystane do późniejszego opracowania raportu osobowego obserwowanego użytkownika.

Profesjonaliści pozyskujący informacje stają się coraz bardziej zależni od specjalistycznego oprogramowania oraz technik, bez których nabycie kluczowej dla odbiorcy wiedzy często byłoby niemożliwe. Większość sposobów pozyskiwania informacji należy do banalnych czynności, a każdy wywiadowca zaczyna od określania swoich potrzeb w celu zebrania odpowiedniego materiału. Kolejnym etapem jest skupienie się na: sprecyzowaniu kierunku i planowania swoich działań; gromadzeniu informacji i wyborze jego sposobu; przetwarzania pliku źródłowego na jednolitą formę przekazu np. tekst; opracowaniu dokumentu analitycznego oraz na doręczeniu raportu końcowego osobie upoważnionej do przetwarzania tych danych[16].

Dość istotnym zagrożeniem na które powinni zwracać uwagę użytkownicy urządzeń mobilnych są fałszywe tożsamości. Wielu użytkowników Internetu padło ofiarą przesłania prywatnych informacji do fałszywego odbiorcy. Fałszywą tożsamość może stworzyć każdy użytkownik sieci online. Dlatego bardzo ważna jest edukacja w tym zakresie, która będzie przestrogą dla Internautów. Fałszywą tożsamość można stworzyć w bardzo łatwy sposób. Wystarczy tylko poznać jej etapy tworzenia. Pierwszą czynnością jest określenie płci i wybranie unikatowego bądź ogólnego imienia i nazwiska, które pozwoli na ukrycie bądź łatwe odnalezienie swojej tożsamości w Internecie. Nazwisko takie powinno być nawiązaniem do poznanej w przeszłości osoby, w zależności od osoby będącej przedmiotem zainteresowania a wiek fałszywej tożsamości powinien być zbliżony do wieku osób, z którymi będziemy mieć kontakt. Należałoby aby zainteresowania i hobby pokrywały się z zainteresowaniami obserwowanego aby w razie konfrontacji była możliwość wymiany zdań i opinii na dany temat. Zdjęcia profilowe powinny przedstawiać zainteresowania, aby w żaden sposób nie naruszyć wizerunku osoby widniejącej na źródłowym zdjęciu pozyskanym z Internetu. Trzeba pamiętać o bieżącej aktualizacji nowej tożsamość. Jeżeli wywiadowca określił już podstawową legendę i posiada adres email, przeważnie tworzy fikcyjne konto na portalu społecznościowym jakim jest np. Facebook czy Twitter aby móc nawiązać znajomość online.

Użytkownicy Internetu rzadko zdają sobie sprawę, że wpisy dokonane na stronach www, nigdy nie znikną z sieci. Dlatego ważnym źródłem informacji są

[16] T.R. Aleksandrowicz, *Analiza informacji w administracji i biznesie*, WSHiP, Warszawa 1999, s. 55–56.

wyszukiwarki internetowe jak i specjalistyczne wyszukiwarki ludzi. Większość z nich oprócz swojej podstawowej funkcji posiada również możliwości korzystania z zaawansowanych zapytań użytkownika do których należą m.in.: możliwość wykluczenia terminów; wyszukania witryny zawierającej link do poszczególnych stron; wyszukania dokładnego terminu czy jego synonimu; znalezienie stron o podobnej treści, terminie w tytule czy w treści strony; wykluczenie określonej strony z wyszukiwania wyników; znalezienie określonego pliku w wybranym formacie i wiele innych. Dość istotnym udogodnieniem dla wywiadowcy jest opcja odtworzenia strony, która nie jest tymczasowo dostępna. W większości przypadków można ją wciąż otworzyć za pomocą wpisania odpowiedniej komendy tj. cache. Wyszukiwarki ludzi są także ogólnodostępne. Do zakresu ich działania zaliczamy wyniki, które obejmują m.in. profile społecznościowe, prywatne strony internetowe czy kontakty w branży.

Najważniejszym źródłem informacji są krajowe i zagraniczne portale społecznościowe. Dzięki nim, można pozyskać dane o charakterze adresowym, przeszłości zawodowej, kontaktowym, ukończonych szkołach a przede wszystkim sprawy prywatne tj.: związki, zdjęcia dzieci, miejsca podróż czy spędzanie wolnego czasu. Dzięki analizie danych można stworzyć schemat powiązań pomiędzy osobami jak i podmiotami gospodarczymi. Fora tematyczne także dostarczają wielu informacji na temat poglądów poszczególnych użytkowników. Z analizy wpisów, można często powiązać profile wzbogacone dokumentacjami fotograficznymi co skutkuje m.in. wykryciem pojazdów wraz z numerami rejestracyjnymi czy tablicami adresowymi[17].

Anonimowość w sieci w czasie nowych technologii zaliczana jest do niemożliwych. Oczywiście dostępne są programy i aplikacje zapobiegające śledzeniu potencjalnego użytkownika w Internecie, niemniej jednak nie wszystkie są skuteczne. W celu zweryfikowania społecznej świadomości użytkowników urządzeń mobilnych na temat cyberinwigilacji, autorka w roku 2016 przeprowadziła badania wśród studentów Akademii Obrony Narodowej. W badaniach wzięło łącznie udział 109 osób z I i V roku Bezpieczeństwa Narodowego. Poniżej przedstawiono najważniejsze wnioski pozyskane z analizy badań.

Według badań respondenci mają małą świadomość o braku zachowania anonimowości podczas korzystania z Internetu co skutkuje możliwością ich permanentnej inwigilacji. Kierunkiem spodziewanego zagrożenia według badanych są nadużycia ze strony władz państwowych i organów ścigania a ataki w Internecie należą do codzienności. Badani raczej nie otwierają załączników od nieznanych nadawców e-mail. Jako zabezpieczenie się przed niechcianym dostępem do prywatnych danych podczas korzystania z Internetu, stosują różne loginy i hasła oraz

[17] K. Turaliński, *Wywiad gospodarczy i polityczny. Podręcznik dla specjalistów ds. bezpieczeństwa, detektywów i doradców gospodarczych*, Artefakt, Warszawa 2015, s. 119–122.

aktualne programy antywirusowe. Należy jednak pamiętać, że ich posiadanie nie daje gwarancji zachowania bezpieczeństwa. Respondenci mimo zagrożenia korzystają bez ograniczeń z publicznych sieci bezprzewodowych, gdzie nieodpowiednie ich zabezpieczenie może skutkować nieautoryzowanym dostępem do sieci. Pozytywnym zaskoczeniem była natomiast informacja o korzystaniu przed studentów z szyfrowanych komunikatorów. Świadczyć to może o świadomości w zakresie inwigilacji telefonii komórkowej. Przeciwieństwem natomiast były wyniki na temat użytkowania telefonu komórkowego w zakresie robienia i udostępniania zdjęć na portalach społecznościowych. 75% badanych codziennie udostępnia zdjęcia z zapisanymi metadanymi w Internecie, czego konsekwencją jest min. możliwość ustalenia miejsca zamieszkania takiego użytkownika.

Dla respondentów bezpieczeństwo przesyłu informacji nie jest tak istotne jak bezpieczeństwo bankowe, dlatego większość badanych nie korzysta z mobilnych aplikacji płatniczych. Na niekorzyść użytkowników urządzeń mobilnych wpływa: sporadyczne czytanie regulaminów serwisów internetowych, wykorzystywanie w hasłach słów związanych z życiem prywatnym oraz brak znajomości stron informujących o bezpieczeństwie w sieci. Portale społecznościowe, najczęściej użytkowane przez respondentów to: Facebook, Instagram, Twitter i Nasza Klasa a największe ryzyko związane z ich użytkowaniem to brak umiejętności ochrony własnej prywatności. Studenci jednogłośnie zgadzają się, że Internet jest istotnym narzędziem w działalności zorganizowanej przestępczości i terrorystów.

Badani nie darzą zaufaniem władz państwowych i organów ścigania mających dostęp do informacji na temat ich aktywności telekomunikacyjnej. Powodami ograniczonego zaufania są kompetencje i zasięg działań osób wykonujących kontrolę danych treści. Respondenci aby zwiększyć swoje bezpieczeństwo w sieci bardzo rzadko korzystają z programów i aplikacji zwiększających bezpieczeństwo danych[18].

Powód braku zapewnienia odpowiedniego bezpieczeństwa przesyłanych danych oraz dostępu do prywatnych profili internetowych wynika z coraz większych wymagań serwisów czy aplikacji w celu weryfikacji użytkownika. Sieci i aplikacje zabezpieczane są przed próbami włamań przez hakerów i późniejszym manipulowaniem posiadanymi danymi.

Z tego względu mnożone są procedury polityki bezpieczeństwa, które wymagają niemałego zaangażowania dla potencjalnego użytkownika. Ludzie aplikacji muszą pamiętać hasła do: konta użytkownika podczas logowania się do komputerów służbowych czy prywatnych; konta poczty służbowej, prywatnej; konta bankowego; numeru PIN do karty bankomatowej, kredytowej, SIM (telefonu służ-

[18] Opracowanie własne na podstawie przeprowadzonych badań.

bowego, telefonu prywatnego); dane do logowania do portali społecznościowych w tym forum, serwisów aukcyjnych czy zakupowych; komunikatorów internetowych i innych. Oprócz tego, polityka bezpieczeństwa niektórych firm wymaga cyklicznej zmiany haseł, które nie mogą być zbyt proste ani krótkie. Dodatkowo powinny zawierać cyfry, znaki specjalne, wielkie i małe litery. Konsekwencją tego jest wprowadzanie przez przeciętnego użytkownika urządzeń mobilnych identycznego hasła dla wszystkich aplikacji bądź zapisywanie ich w łatwo dostępnym miejscu tj. plik na pulpicie czy przyklejona kartka na monitorze. Zagrożeniem jest także stosowanie automatycznego podpowiadania haseł, gdzie cyberprzestępca może bez trudu zalogować się do systemu użytkownika. Niestety cyberatak na użytkowniku urządzeń mobilnych może być przeprowadzony za pośrednictwem publicznych sieci z każdego miejsca na ziemi, co może stanowić utrudnienie do zlokalizowania przestępcy[19].

Mając świadomość tego, jak wiele istnieje ataków na systemy i obiekty informatyczne, należy wyselekcjonować potencjalne obszary ich występowania, dlatego w tab. 1 przedstawiono najważniejsze metody ataków, które mogą bezpośrednio dotyczyć użytkowników urządzeń mobilnych.

Tabela 1. Metody ataków w cyberprzestrzeni

Metoda ataku	Cel działania
Wirusy, robaki	Wirus jest kodem mającym za zadanie uszkodzenie danych lub programów, czego konsekwencją jest zmiana sposobu działania danego sprzętu. Robak (worm) jest programem rozprzestrzeniającym się w sieci teleinformatycznej, który może powodować szkodliwe działanie takie jak wirus czy koń trojański.
Koń trojański	Koń trojański jest programem mającym za zadanie wykonywać niepożądane działanie na urządzeniach mobilnych np. formatowanie dysku, usuwanie plików czy przesyłanie danych do twórcy programu. Działania te wykonywane są bez wiedzy użytkownika.
Uwierzytelnianie	Podszycie się za osobę uprawnioną do autoryzowanego dostępu w celu konieczności przekazania informacji potrzebnych do poprawnego uwierzytelniania.
Ominięcie	Ominięcie procesu procesu zabezpieczającego system.
Czytanie	Dostęp do informacji, nie posiadając przy tym wymaganych uprawnień.
Kradzież	Kradzież danych z urządzenia mobilnego oraz usunięcie kopii.

[19] K. Billewicz, *Problematyka bezpieczeństwa informatycznego w inteligentnych sieciach*, Aktualne problemy w elektroenergetyce. Jurata 8–10 czerwca 2011, Instytut Energoelektryki Politechnika Wrocławska, s. 116–117.

Metoda ataku	Cel działania
Kopiowanie	Tworzenie kopii dokumentów przez osoby nieuprawnione.
Modyfikacja	Zmiana charakterystyki lub danych.
Usunięcie	Zniszczenie danych.
Tylne drzwi	Twórcy programów mogą dostać się do komputerów, na których użytkowane są ich programy.
E-mail bombing	Przesyłanie poczty elektronicznej z załączonymi wielkimi plikami na serwer pocztowy w celu przepełnienia skrzynki adresata.

Źródło: opracowanie własne na podstawie E. Lichocki, *Model Systemu Zarządzania Kryzysowego w warunkach zagrożeń cyberterrorystycznych dla bezpieczeństwa informatycznego SZ RP*, Rozprawa doktorska, AON, Warszawa 2009, s. 62–62.

Zakończenie

Nowoczesne społeczeństwo jest synonimem społeczeństwa informacyjnego, które przetwarza i udostępnia informacje za pomocą urządzeń mobilnych czy komputerowych.

Ze względu na dostępność do środków komunikacji masowej, korzystanie z nowych technologii jest codziennością. W związku z tym bardzo ważne jest zadbanie o bezpieczeństwo użytkowników urządzeń mobilnych. Rozwiązania jakie można zastosować dotyczą teleinformatyki a przede wszystkim zastanowienia się przez Internautę czy powinno się udostępniać w sieci informacje mające znaczenie wywiadowcze. Niska świadomość użytkowników urządzeń mobilnych w zakresie cyberinwigilacji może doprowadzić przede wszystkim do: kradzieży tożsamości, ataków na urządzenia mobilne z wykorzystaniem szkodliwego oprogramowania, strat finansowych, nieupoważnionego wprowadzania lub kopiowania danych czy zakłócenia działania systemów. W cyberprzestrzeni powoli dochodzi do wzmocnienia środków bezpieczeństwa. Dlatego niezbędnym krokiem jest podnoszenie świadomości Internautów, w celu zmniejszenia ryzyka naruszenia prywatności w sieci online.

„Prywatność to podstawowy warunek
bycia wolnym człowiekiem”.
Gleen Greenwald
[Snowden. Nigdzie się nie ukryjesz, 2014]

Bibliografia

1. Aleksandrowicz T.R., *Analiza informacji w administracji i biznesie*, WSHiP, Warszawa 1999.
2. ASPRA-JR, Warszawa 2010.
3. Billewicz K., *Problematyka bezpieczeństwa informatycznego w inteligentnych sieciach*, Aktualne problemy w elektroenergetyce. Jurata 8–10 czerwca 2011, Instytut Energoelektryki Politechnika Wrocławska.
4. Gogołek W., *Komunikacja sieciowa. Uwarunkowania, kategorie, paradoksy*.
5. Hanausek T., *Kryminalistyka. Zarys wykładu*, Kraków 2005.
6. Lichocki E., *Model Systemu Zarządzania Kryzysowego w warunkach zagrożeń cyberterrorystycznych dla bezpieczeństwa informatycznego SZ RP*, rozprawa doktorska, AON, Warszawa 2009.
7. Marczyk M., *Bezpieczeństwo teleinformatyczne wobec ataków cyberterrorystycznych*, Difin, Warszawa 2014.
8. Miłosz M., *Systemy mobilne. Informatyka gospodarcza*, tom 4, C.H. Beck, Warszawa 2010.
9. Minkina M., *Gry wywiadów. Sztuka wywiadu w państwie współczesnym*, Rytm, Warszawa 2014.
10. Mroziewicz K., *Czas pluskiew*, Wydawnictwo „Sensacje XX wieku", Warszawa 2007.
11. Rdzanek G., Tokarz G., *Służby specjalne. Przeszłość i teraźniejszość*, GS Media, Wrocław 2009.
12. Sandvig C., *An Initial Assessment of Cooperative Action in Wi-Fi Networking*, Telecommunications Policy, vol. 28(7/8).
13. Szkotak M., *Technologie mobilne*, iTst@rt Wydawnictwo Informatyczne, Piekary Śląskie 2011.
14. Szubrycht T., *Cyberterroryzm jako nowa forma zagrożenia terrorystycznego*, Zeszyty Naukowe Akademii Marynarki Wojennej, nr 1, 2005.
15. Turaliński K., *Wywiad gospodarczy i polityczny. Podręcznik dla specjalistów ds. bezpieczeństwa, detektywów i doradców gospodarczych*, Artefakt, Warszawa 2015.
16. Wasilew A.Z., *Technologie „podłączenia" w społeczeństwie mobilnym*, Zeszyty Naukowe Uniwersytetu Szczecińskiego, Studia Informatica, Nr 28.
17. Wroński P., *Czas nielegałów. Krótki kurs kontrwywiadu dla amatorów*, Fronda, Warszawa 2016.
18. Zieliński B., *Bezprzewodowe sieci komputerowe*, Helion, Gliwice 2000.

Strony internetowe

1. Sienkiewicz B., *Historia pewnego złudzenia*, Przegląd Bezpieczeństwa Wewnętrznego, 20-lecie uop/abw, wydanie specjalne, https://www.abw.gov.pl/pl/pbw/publikacje/przeglad-bezpieczenstw-1/569,PrzegladBezpieczenstwaWewnetrznegoWYDANIESPECJALNE.html [dostęp: 20.02.2017].

2. *Słownik języka polskiego PWN*, witryna internetowa o nazwie www.sjp.pwn.pl [dostęp: 17.03.2017].

Keywords: *Open-source intelligence, surveillance, cybersurveillance, cybersecurity*

SUMMARY

Information technologies have dominated the 21st Century. The rapid development of technology and communication with mobile devices spawns major security problems for their users. "Open-source intelligence", which is based on gathering information from open source information (OSINT), is more and more important. Due to its widespread access, the security of online users data is at risk. The author attracts the attention to sources of obtaining information by mobile users, which affect their direct online safety.