PRACE NAUKOWE Akademii im. Jana Długosza w Częstochowie
Technika, Informatyka, Inżynieria Bezpieczeństwa 2018, t. VI, s. 575–590

http://dx.doi.org/10.16926/tiib.2018.06.41

Marlena Krakowiak, Teresa Bajor
Zakład Ergonomii i Inżynierii Bezpieczeństwa
Instytut Przeróbki Plastycznej i Inżynierii Bezpieczeństwa
Wydział Inżynierii Produkcji i Technologii Materiałów
Politechnika Częstochowska
al. Armii Krajowej 19, 42–200 Częstochowa,
e-mail: krakowiak.marlena@wip.pcz.pl; bajor.teresa@wip.pcz.pl

WSPÓŁCZESNE ZAGROŻENIA ZWIĄZANE Z UŻYTKOWANIEM SIECI

Streszczenie. Stosowanie nowoczesnych technologii umożliwiających zwiększenie komfortu bezpieczeństwa pracy w sieci jest zagadnieniem ciągle aktualnym. Podobnie jak większość rozwiązań, także sieć Internet ma swe blaski i cienie. Burzliwy rozwój technologii i techniki w XXI wieku stał się przyczyną ogólnodostępnej mnogości rozwiązań, częstokroć nie do końca sprawdzonych, których niezawodność pozostawia wiele do życzenia. Powszechna globalizacja, gromadzenie, przetwarzanie i przechowywanie ogromnych ilości danych osobowych, firmowych, państwowych, strategicznych – dają szereg możliwości, ale także stwarzają liczne i różnorakie zagrożenia. Dla każdego ważne jest by zachować poufność udostępnianych i przetwarzanych danych. Na tej płaszczyźnie pojawia się wiele konfliktów interesów. Ze względu na szeroko pojęte poczucie bezpieczeństwa, szczególnie w ostatnich kilku latach, użytkownik sieci nie pozostaje anonimowy. Firmy i instytucje zabezpieczają się przed utratą danych z jednej strony poprzez specjalistyczne oprogramowanie, z drugiej zaś poprzez wiedzę o swoich klientach (użytkownikach).
Dla usprawnienia działania sieci oraz zachowania anonimowości i uniknięcia komercjalizacji powstały takie rozwiązania, jak: sieć TOR, czy FreeNet. Działa również tzw. Darknet, Hidden services czy Deep Web. Są to rozwiązania dla tych wszystkich, którzy z różnych powodów chcą pozostać anonimowi. Niestety nie wynika to tylko z chęci bycia niezależnym od korporacji i szeroko pojętej inwigilacji w celach zapewnienia bezpieczeństwa. W artykule podjęta zostanie próba dokonania analizy bezpieczeństwa użytkowania i poruszania się w sieci w obliczu występujących zagrożeń i współczesnych wyzwań.
Słowa kluczowe: zagrożenia, bezpieczeństwo w sieci, TOR, Deep Web, netykieta, Internet Rzeczy, sieci społecznościowe.

CONTEMPORARY THREATS RELATED TO THE USE OF THE NETWORK

Abstract. The use of modern technologies to increase the comfort of work safety in the network is still an issue. Like most solutions, the Internet has the pros and cons. The turbulent development of technology and technique in the twenty-first century has become a cause of generally available multitude of solutions often with do not fully proven reliability which leaves much to be desired. The globalization, collection, processing and storage of huge amounts of personal, company, national and strategic data – give a number of possibilities, but also create a numerous and various threats. For each one it is important to preserve the confidentiality of data being shared and processed. There are many conflicts of interest on this level. Due to the broad sense of security, especially in the last few years, the network user does not remain anonymous. Companies and institutions protect themselves against data loss on the one hand through specialized software, and on the other by knowledge about their customers (users).
In order to improve the network operation, keep anonymity and avoid commercialization, solutions such as the TOR network or FreeNet were created. There is also a so-called Darknet, Hidden services or Deep Web. These are solutions for all those who want to remain anonymous for various reasons. Unfortunately, it does not result only from a desire to be independent from corporation and widely concept invigilation operated in order to security assurance. In the article, the attempt to analyze the safety of using and navigating the network in the face of existing threats and contemporary challenges will be made.
Keywords: threats, network security, TOR, Deep Web, netiquette, Internet of Things, Social Network Sites.

Wstęp

Żyjemy w czasach nieustannego postępu technicznego, rozwoju silnie zaawansowanych technologii, sztucznej inteligencji, miniaturyzacji i elektronizacji wszystkiego, co tylko człowiek jest na obecną chwilę w stanie wymyślić. Internet odgrywa tu ogromną rolę, gdyż poza źródłem wiedzy stanowi medium szerokiej i wszechstronnej wymiany informacji. Ze względu na rozpowszechnienie i szeroką rozbudowę infrastruktury sieciowej stała się ona narzędziem wykorzystywanym niemalże w każdej dziedzinie życia. Już nawet proste urządzenia gospodarstwa domowego, jak telewizory, pralki, lodówki mogą zostać podłączone do sieci. Zachwyt ludzkości nad możliwościami, jakie daje postęp technologiczny może jednak okazać się zgubny, przy całym szeregu dobrodziejstw, jakie ze sobą niesie. Internet, tak jak każde inne rozwiązanie, ma „dwie strony medalu". Pozostając w służbie człowiekowi, zależy w głównej mierze od jego intencji i pobudek, z jakich podejmuje on swą działalność.

Ochrona życia i mienia obywateli, w tym zapewnienie im poczucia bezpieczeństwa, powinna być priorytetem dla władz państwowych na całym świecie. W czasach niepokoju i wielu akcji militarnych oraz terrorystycznych jest to szczególnie trudne do zagwarantowania. Zorganizowane grupy przestępcze zaczęły używać świata cybernetycznego, jako broni (dezinformacja), źródła rekrutowania ochotników, bądź nieograniczonego medium rozpowszechniania propagandowych treści [1]. Międzynarodowe organizacje rządowe stanęły w obliczu konfrontacji z ukrytym Internetem, o którym większość z nas nigdy nie słyszała, zwanym *Deep Web* czy *Darknet* [2].

Takie popularne serwisy, jak *Google, Youtube* czy *Facebook* stanowią tylko wierzchołek góry lodowej (Rys. 1.), gdyż oprócz nich istnieje całe mnóstwo stron niewidocznych dla przeciętnego użytkownika sieci.

Rys. 1. Internet jako góra lodowa – stosunek części jawnej do ukrytej (opracowanie własne)

Wszystko, co ponad taflą wody można nazwać siecią zindeksowaną, która może być przeszukiwana przez popularne wyszukiwarki. Natomiast pod wodą, ta góra lodowa osiąga ogromne rozmiary. Ponad 80% całości stanowi sieć ukryta, nieindeksowana. W jej skład wchodzą m.in. bazy danych będące w posiadaniu firm i różnorakich instytucji, a nawet osób prywatnych, zasoby archiwalne, biblioteki, tablice ogłoszeń, fora internetowe. Nie obowiązuje w niej

cenzura, gdyż w większości przypadków sieć ukryta pozbawiona jest kontroli. Ukryty Internet, przede wszystkim *Darknet*, umożliwia całkowitą anonimowość, w przeciwieństwie do powszechnie używanej sieci. Użytkownik może bezkarnie wymieniać się dowolną informacją, swobodnie nawiązywać kontakty i dokonywać transakcji za pomocą wirtualnej waluty (tzw. *bitcoin*). W obrazowy sposób funkcjonowanie sieci przedstawiono na Rys. 2.

Rys. 2. Niekonwencjonalna mapa sieci [3]

Deep Web a bezpieczeństwo

Niestety wolność absolutna w *Deep Web* stanowi wyzwanie dla jednostek rządowych [1, 4], które w jej obliczu są w wielu przypadkach bezsilne. Z ich strony występuje zapotrzebowanie na technologie rozpoznające i analizujące treści ukryte. Ponadto ciągle podejmowane są próby ograniczenia anonimowości w sieci i jej ocenzurowania na drodze ustawodawczej.

Defense Advanced Research Projects Agency (DARPA) posiada nową wojskową technologię, tzw. MEMEX, która działa jak specyficzna wyszukiwarka „widząca" ślady aktywności w sieci ukrytej oraz na stronach niedostępnych drogą tradycyjną. Dzięki zastosowaniu MEMEX możliwe jest określenie, z iloma stronami internetowymi mamy do czynienia oraz jaka jest ich treść. System ten został wynaleziony w celu wyśledzenia handlu ludźmi w sieci. Obecnie jest on wykorzystywany w tropieniu użytkowników starających się pozostać w ukryciu. Daje możliwość wyśledzenia aktywności i lokalizacji [1].

Istnieje szereg konferencji naukowych i platform oferujących wymianę

poglądów i rozwiązań dotyczących tematyki bezpieczeństwa w sieci, w tym także sieci *Darknet*. To dzięki nim dowiadujemy się np., że powstała aplikacja „Daedalus" [5], japońskich twórców, służąca do monitoringu „ciemnej" strony sieci przede wszystkim w celach ochrony przed atakami, i dzięki temu stwarzająca możliwość szybkiego reagowania. Obecnie „cyberbezpieczeństwo" jest jednym z najbardziej intensywnie rozwijających się i prężnych nurtów związanych z działalnością człowieka.

Sieci *FreeNet* [6] i *TOR* [7] powstały w celu zapewnienia ochrony prywatności internautów. Bodźcem do ich powstania były ograniczenia wolności poglądów panujące w systemach totalitarnych. Chroniono w ten sposób dane personalne opozycjonistów, jak również te dotyczące lokalizacji i prowadzonych akcji, nie dając przy tym okazji rządowym organizacjom na ich represjonowanie. Niestety, podobnie jak większość rewolucyjnych rozwiązań i to znalazło się w kręgu zainteresowań organizacji przestępczych.

Darknet (Hidden services lub *Deep Web)* uznawany jest za tę gorszą, niebezpieczną stronę pozostawania anonimowym użytkownikiem w sieci. Jego symbolem stała się *Hidden Wiki (Ukryta Wikipedia)*, zawierająca hasła związane z działaniem i treściami znajdującymi się w ukrytej „ciemnej" części Internetu [8].

FreeNet jest siecią działającą w sposób przypominający połączenia P2P. Do jej uruchomienia konieczny jest darmowy klient tradycyjnej przeglądarki. Każdy logujący się osobnik wyraża zgodę na udostępnienie części swojego dysku oraz łącza na pracę *FreeNet*-u. Tym sposobem wszystkie publikowane treści są dzielone i umieszczane na komputerach wielu użytkowników. Dzięki temu nigdy nie wiadomo, czy jednostka, z którą w danej chwili łączymy się jest faktycznym źródłem strony, czy też jedynie przekaźnikiem. Co pewien czas informacje przenoszone są na kolejne komputery, w celu uniemożliwienia ich lokalizacji, a transmisje danych kodowane [9].

Strony dostępne we *FreeNet* są wyjątkowo ubogie i proste. Kluczowym czynnikiem jest ograniczona przepustowość sieci, gdyż *FreeNet* nie korzysta z tradycyjnych domen internetowych. „Surfowanie" w sieci odbywa się za pomocą linków zamieszczanych na stronach oraz z wykorzystaniem oficjalnego katalogu stron [9].

System *TOR* w *Darknecie*

Na rynku roi się od subiektywnych komentarzy dotyczących *Darknetu*, zasad jego działania, a przede wszystkim treści, jakie można w nim znaleźć. Ponieważ jest to specyficzna sieć, należy do jej korzystania przystąpić, będąc w pełni świadomym możliwych tego konsekwencji.

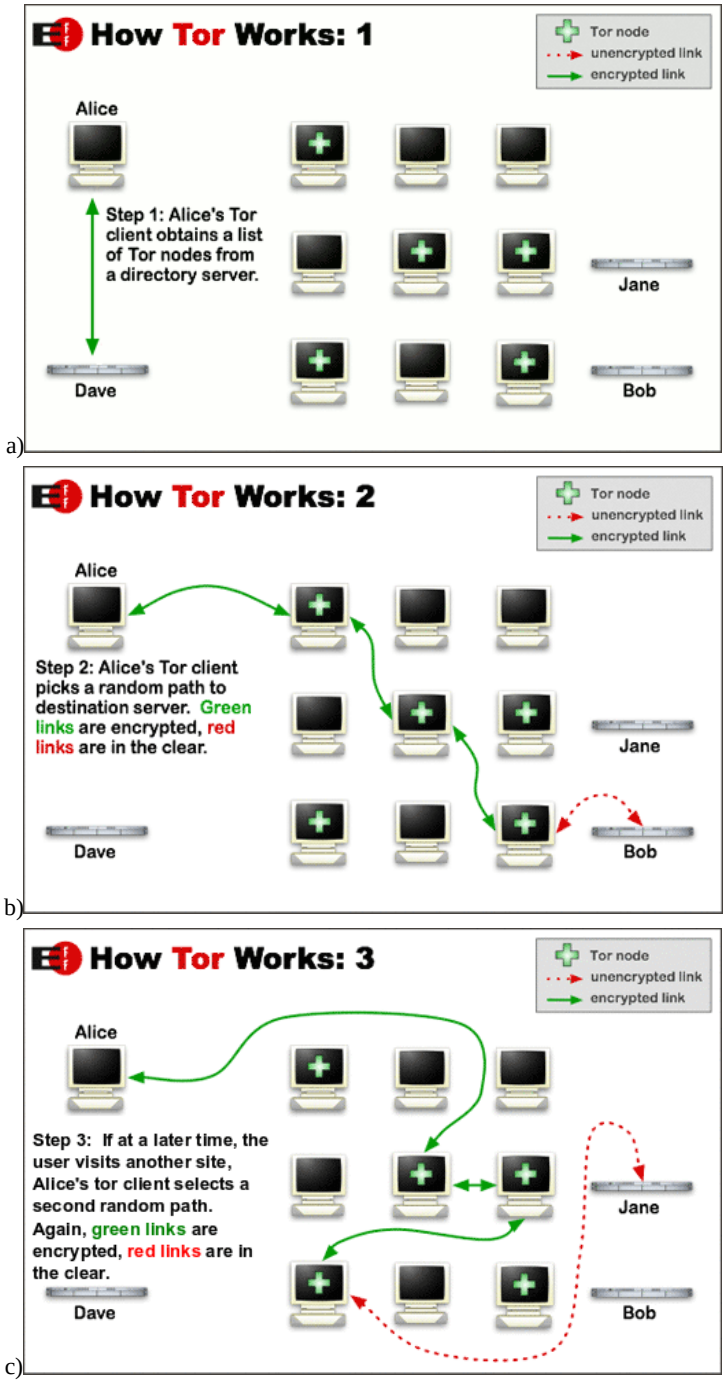
Jest wiele technik używania *Darknetu*, jednak najpopularniejszą jest sieć *TOR – Tor's Onion Router Network* (Rys. 3). Technologia „routera cebulowego"

została opracowana przez wojska amerykańskie w celu umożliwienia anonimowego przesyłania informacji. Domena „onion" jest częścią rejestru *ICANN* i nie jest możliwe połączenie się z nią bez użycia programu *TOR*. Zarówno host, jak i klient są ukryci, a ich identyfikacja jest bardzo utrudniona.

Rys. 3. Widok na stronę startową *TOR* [7]

Jest to system, który działa sprawniej i bardziej intuicyjnie niż *FreeNet*. Korzystając z przeglądarki *TOR*, możemy penetrować również klasyczne zasoby sieci, zapewniając sobie przy tym zwiększoną anonimowość. *Darknet* posiada zdecydowanie większą ilość zasobów niż *FreeNet*, a dostępne strony są nieco bardziej zaawansowane [9].

TOR obsługiwany jest przez grupę serwerów-wolontariuszy. Jego użytkownicy wykorzystują sieć po podłączeniu poprzez serię wirtualnych tuneli, zamiast bezpośrednich połączeń, dzięki czemu zarówno organizacje, jak i użytkownicy indywidualni mogą wymieniać się informacjami w sieciach publicznych, bez naruszenia prywatności. Dodatkowym zabezpieczeniem jest maskowanie adresu IP użytkownika. Zasadę działania przedstawiono na Rys. 4 a, b, c. Jest to skuteczne narzędzie obejścia cenzury, co pozwala w inny sposób dotrzeć do zablokowanych treści. Klienta *TOR* można pobrać bezpłatnie [7].



Rys. 4. Zasada działania sieci *TOR:* a) etap 1, b) etap 2, c) etap 3 [7]

Użytkownicy indywidualni mogą wykorzystywać sieć *TOR* m.in. do utrzymania stron internetowych niezależnych od różnych form inwigilacji bądź blokowania przez lokalnych dostawców. Sieć taka może być używana do komunikacji społecznie wrażliwej, wykorzystywana przez dziennikarzy do bezpiecznych kontaktów z informatorami i dysydentami. Ponadto umożliwia firmom pozarządowym komunikowanie się z pracownikami pozostającymi poza zagranicami kraju bez ujawniania ich lokalizacji, co może być elementem strategicznym dla danego przedsiębiorstwa. Pozwala na prowadzenie analizy konkurencyjności, samemu pozostając niewidocznym. Może także stanowić skuteczne zabezpieczenie przed podsłuchem np. pilotowanych przetargów i stanowić zastępstwo dla tradycyjnych VPN, które ujawniają dokładną treść i czas komunikacji.

Różnorodna społeczność korzystająca z tej sieci jest czynnikiem zapewniającym jej bezpieczeństwo. Według twórców sieci, im liczniejsza i bardziej różnorodna baza użytkowników, tym lepiej chroniona jest ich anonimowość. TOR zabezpiecza przed powszechną w Internecie inwigilacją w postaci znanej jako „analiza ruchu sieciowego" - często wykorzystywanej chociażby w celach marketingowych.

Bankowość elektroniczna

Można pokusić się o stwierdzenie, że znakiem obecnych czasów jest bankowość elektroniczna. To usługa bardzo rozpowszechniona ze względu na wygodę, ilość i szybkość dokonywanych transakcji. Różnego rodzaju zlecenia stałe sprawiają, że nie musimy zaprzątać sobie głowy informacjami o terminach płatności, gdyż zobowiązujemy do tego instytucję bankową. Ponosimy koszty obsługi konta, nie martwiąc się o dodatkowe opłaty manipulacyjne. Nie musimy mieć w ręku gotówki, by dokonać transakcji i nie stwarzamy okazji wzbogacenia się naszym kosztem „kieszonkowcom". To wszystko sprawia, iż „kwitną" operacje bezgotówkowe i rośnie popularność e-bankowości. Jednakże należy w związku z tym liczyć się z występowaniem nowego rodzaju zagrożeń, zarówno związanych z działalnością przestępczą, jak i nieodpowiedzialnością użytkowników, bądź nieznajomością podstawowych zasad bezpieczeństwa w sieci.

Cyberprzestępcy, wraz z rozwojem technologii i techniki komputerowej, mają coraz doskonalsze narzędzia i dostęp do wysoce wyspecjalizowanych fachowców. Wykorzystując opisany w poprzednim rozdziale *Darknet*, mogą funkcjonować sprawnie i prawie bez ograniczeń na terenie całego świata.

Według raportu CERT Polska, organizacji działającej w strukturach NASK (Naukowej i Akademickiej Sieci Komputerowej), będącej zespołem reagowania

na incydenty (Computer Emergency Response Team https://www.cert.pl/,) najczęściej odnotowanym incydentem związanym z naruszeniem bezpieczeństwa komputerowego w 2016 roku był „phishing" (ponad 50% przypadków) [10]. Wzrosła znacznie liczba stron oraz rozsyłanych plików ze szkodliwym oprogramowaniem tego typu. Odnotowano, iż szeroki wachlarz rozwiązań prowadzących do kradzieży środków pieniężnych atakuje także urządzenia mobilne, z których chętnie i często korzystamy. Wiadomości „phishingowe" zwykle mają formę fałszywych powiadomień z banków czy systemów e-płatności bądź innych organizacji, które cieszą się społecznym zaufaniem. Ich twórcy wykorzystują metody socjotechniczne, by uśpić czujność adresata, a znacznie częściej spowodować szybką reakcję w afekcie, czyli np. pod wpływem strachu lub spowodowaną wywołanym poczuciem poniesienia straty. Często, jak na ironię, stosowane jest także wyłudzenie danych pod pretekstem ochrony przed szkodliwym oprogramowaniem. Użytkownik np. rejestruje się na witrynie świadczącej rzekomo usługi „antyphishingowe", która zwykle po kilku dniach przestaje istnieć, podając informacje dotyczące logowania, co jest wystarczające dla przestępców by zrobić z tego odpowiedni dla siebie użytek. W tabeli 1 przedstawiono udział procentowy incydentów odnotowanych w 2016 roku przez CERT Polska [10] po zakwalifikowaniu ich do poszczególnych typów.

Tabela 1. Najpopularniejsze zdarzenia incydentalne odnotowane w Polsce w 2016 roku (opracowane na podstawie [10])

Typ incydentu	Udział procentowy
Oszustwa komputerowe	55,50
Kradzież tożsamości, podszycie się	52,96
Obraźliwe i nielegalne treści	12,31
Spam	11,58
Złośliwe oprogramowanie	10,96
Próby włamań	5,66
Włamania	2,80
Skanowanie	2,65
Atak na bezpieczeństwo informacji	2,34
Dostępność zasobów	2,34

Przedstawione dane świadczą o tym, iż bardzo poważnym zagrożeniem jest kradzież tożsamości, będąca skutkiem wielu świadomych działań organizacji przestępczych oraz zaniechań i zaniedbań użytkowników sieci. Informacja od zarania dziejów jest najpopularniejszym środkiem wymiany, dającym profity tym, którzy ją posiadają i potrafią zrobić z niej użytek. Zatem ochrona tzw. „wrażliwych danych" powinna stanowić zadanie priorytetowe dla każdego, i to niezależnie od tego, czy jest to użytkownik prywatny czy korporacja. Jest to bodziec dla firm zajmujących się wykorzystaniem rozwiązań biometrycznych [11] do konstrukcji różnorakich zabezpieczeń technicznych przed niepowołanym dostępem osób trzecich. Powstają tzw. inteligentne budynki zaopatrzone w systemy monitoringu [12], połączone z systemami alarmującymi i powiadamianiem odpowiednich służb ochrony. Stosowanie zabezpieczeń na wielu płaszczyznach i odpowiednia edukacja [13] w zakresie bezpieczeństwa wydaje się być jednym z najbardziej skutecznych sposobów ochrony.

Na przestrzeni 20 lat (1996–2016) liczba odnotowanych incydentów związanych z użytkowaniem sieci wzrosła z 50 do 1926 [10], czyli ponad 38-krotnie. Wartość ta z pewnością jest znacznie większa, gdyż nie każde takie zdarzenie jest zgłaszane. Świadczy to o skali występowania tego typu zagrożeń w obecnych czasach i tendencji wzrostowej w przyszłości. Rys. 5 przedstawia sektory działalności człowieka narażone na „cyberataki" oraz ich główne bodźce.

Rys. 5. Główne przyczyny zagrożeń cyberbezpieczeństwa w wybranych sektorach działalności człowieka (opracowanie własne)

Analizując dostępne informacje i dane statystyczne, można z całą pewnością stwierdzić, że podłożem zdecydowanej większości ataków w sieci jest chęć wzbogacenia się, czy to na drodze przejęcia bezpośredniego środków zgromadzonych na kontach bankowych użytkowników sieci, czy też przez wymuszenia pod groźbą utraty danych, mobilności, zablokowania środków bądź zablokowania systemu na skutek działania np. złośliwego oprogramowania (tzw. trojanów). Zagrożone są nie tylko duże przedsiębiorstwa, chociaż te przeważnie mają lepsze zaplecze zabezpieczające niż małe firmy, szczególnie jednoosobowe.

Portale społecznościowe

Portale społecznościowe to kopalnia wiedzy *(podobnie jak internetowe tablice ogłoszeń)*, z której korzystać mogą wszyscy niezależnie od lokalizacji, światopoglądów i intencji. Jest to bogate źródło różnorakich informacji o użytkownikach, często opatrzonych dokumentacją fotograficzną, a nawet filmową. Można pokusić się o stwierdzenie, że jest to baza danych ciągle aktualizowana i wzbogacana o nowe rekordy. Szczególnie, że obserwuje się zjawisko nadmiernego korzystania z sieci społecznościowych (SNS – Social Network Sites), co uznawane jest już jako uzależnienie [14].

Społeczeństwo powinno zdawać sobie sprawę z mechanizmów działania sieci, przede wszystkim dotyczących poufności danych i sposobów administrowania nimi. Komunikacja prywatna i publiczna znacznie się od siebie różnią. Podczas gdy w jednym przypadku zgadzamy się na obserwowanie (śledzenie) naszych wypowiedzi, w drugim chcemy zachować prywatność i poufność. Należy uświadomić sobie, iż poza adresatem i nadawcą wiadomości umieszczanej w Internecie (serwisie społecznościowym, forum, komunikatorze) wgląd do niej ma także administrator, który, jeśli istnieje taka potrzeba, może się z nią zapoznać.

Z tego względu bardzo istotna jest edukacja i budowanie świadomości w społeczeństwie na temat podstawowych zasad bezpieczeństwa związanego z aktywnością w Internecie.

Kolejnym zagrożeniem, i to właściwie dla każdego, może okazać się rozpowszechnianie tzw. „fake news", które mogą stać się źródłem zarówno gry politycznej, jak i biznesu dotyczącego np. dochodu z reklam wyświetlanych przy okazji odwiedzania strony z zamieszczoną „sensacyjną" wiadomością [15]. Zatem model biznesowy oparty na reklamie kwitnie dzięki sztucznie wygenerowanemu ruchowi. Tym samym stanowi zagrożenie wolności słowa, pociągając za sobą wprowadzanie regulacji prawnych i mechanizmów dotyczących ograniczenia możliwości zamieszczania fałszywych informacji w Internecie. Nałożenie obowiązku usuwania nieprawdziwych treści na firmy, takie jak Goo-

gle czy Facebook, przekazuje im kolejne narzędzia, dzięki którym będą stanowić decydujący łącznik między odbiorcami wszelkich informacji w sieci.

Coraz trudniej przeciętnemu użytkownikowi poruszać się w środowisku przepełnionym treściami, które nie opisują rzeczywistości, a mają tylko generować ruch (kupno/sprzedaż). Jest to kolejny argument, by używać logiki i dobrych praktyk w tym zakresie, czyli m.in.: netykiety, nie ulegać emocjom i nie działać mechanicznie.

Internet Rzeczy

Terminem *Internet Rzeczy (Internet of Things, IoT)* określane są urządzenia codziennego użytku podłączone do sieci i potrafiące w sposób automatyczny gromadzić szereg danych i przesyłać je bez konieczności interwencji człowieka. Mogą to być zarówno komputery, jak i wyposażenie gospodarstwa domowego, liczniki zużycia energii elektrycznej, gazu, wody, kamery przemysłowe, systemy alarmowe, samochody, urządzenia mobilne, a nawet nowoczesne implanty medyczne (rozruszniki serca, pompy insulinowe, aparaty słuchowe).

Taki trend w ostatnich latach powoduje powstawanie różnorakich „inteligentnych" produktów, które zdobywają przebojem światowe rynki. Jednakże sprawa bezpieczeństwa tych rozwiązań wydaje się być poboczną. Firmy liczą na zyski dzięki zastosowaniu nowoczesnej, wygodnej technologii, bagatelizując na tym etapie możliwe zagrożenia dotyczące choćby niepowołanego dostępu do przesyłanych automatycznie danych [16].

Eksperymentowanie z wykorzystaniem nowoczesnych zminiaturyzowanych technologii do wygodniejszego życia codziennego jest faktem. Generuje to szereg nowych możliwości ograniczenia bezpieczeństwa i prywatności ich użytkowników.

Sposoby ochrony i netykieta

Powszechna cyfryzacja w niemal każdej dziedzinie życia stwarza całą paletę zagrożeń dla pospolitego użytkownika sieci, z czego nie wszyscy zdają sobie sprawę, często bagatelizując zasady prostej netykiety (etykiety obowiązującej w sieci). Wiele firm i instytucji podaje propozycje rozwiązań technicznych i metod postępowania w obliczu ataków komputerowych, bazując na dostępnej wiedzy i własnych doświadczeniach. Każdy użytkownik powinien jednak zastanowić się nad doborem takich środków prewencyjnych, by były one zharmonizowane z jego działalnością i aktywnością w sieci. W tabeli 2 zaproponowano kilka rodzajów działań, jakie należy podejmować, chcąc zminimalizować ryzyko ataku na polu prowadzonej aktywności w sieci.

Tabela 2. Środki zaradcze i zapobiegawcze, jakie należy podejmować, by chronić się przed cyberprzestępczością (opracowanie własne)

Rodzaj działania	**Podejmowane czynności**
Odpowiednie zabezpieczenie komputera/sieci/urządzeń mobilnych	– loginy i hasła o większym stopniu złożoności; – oprogramowanie ze sprawdzonych, legalnych źródeł; – aktualizacja oprogramowania zgodnie z zaleceniami producenta (ewentualnie wymiana na oprogramowanie wspierane); – posiadanie programów antywirusowych i antyspamowych oraz ich bieżąca aktualizacja (bazy wirusów); – instalacja oprogramowania chroniącego i ewentualny nadzór specjalisty IT nad funkcjonowaniem i dostępem do sieci; – rezygnacja z niewykorzystywanych dostępnych funkcji sieciowych (np. drukowanie); – nie używanie geolokalizacji, jeśli to nie konieczne; – odpowiednia konfiguracja sieci (oddzielne sieci wewnętrzne, np. dla gości); – odizolowanie od dostępu do sieci jednostek z danymi poufnymi.
Podnoszenie świadomości użytkowników sieci	– zapoznanie z zasadami poruszania się w sieci i zamieszczaniem materiałów informacyjnych (zdjęć, komentarzy, filmów itp.); – korzystanie z zaufanych witryn i połączeń sieciowych; – nie stosowanie funkcji automatycznego zapamiętywania haseł; – świadomość zagrożeń w sieci i sposobów ochrony przed nimi; – zapoznanie z netykietą i jej stosowanie w życiu codziennym; – kształtowanie dobrych nawyków; – uważność i rozwaga dotycząca reakcji na komunikaty programowe (nie lekceważenie ich); – świadomość konsekwencji wycieku danych na skutek niekontrolowanego dostępu osób trzecich (skali i skutków cyberataków).

Rodzaj działania	Podejmowane czynności
Korzystanie z usług sprawdzonych specjalistów z branży IT	– świadomość poziomu własnej wiedzy na temat zasad bezpiecznego funkcjonowania w sieci; – współpraca z zaufanymi specjalistami ds. IT i utrzymania bezpieczeństwa w sieci.
Monitorowanie rynku IT i tendencji dotyczącej nowych rozwiązań technologicznych	– śledzenie dostępnych rozwiązań technicznych i postępu w tej dziedzinie; – śledzenie nowych technologii; – orientacja w nowoczesnym oprogramowaniu; – aktualizacja oprogramowania i systemów zabezpieczeń.
Śledzenie raportów i zestawień oraz doniesień udostępnianych do publicznej wiadomości dotyczących bezpieczeństwa użytkowania sieci	– śledzenie forów tematycznych; – zapoznanie z aktualnie zidentyfikowanymi zagrożeniami; – śledzenie ilości i charakteru zdarzeń incydentalnych; – analiza ryzyka na podstawie dostępnych informacji i własnych doświadczeń oraz spostrzeżeń; – wymiana informacji i zgłaszanie zaistniałych zdarzeń incydentalnych odpowiednim organom/instytucjom.

Netykieta [17] stworzona przez samych użytkowników sieci jest przeniesieniem zasad kultury osobistej do przestrzeni internetowej. Zasady właściwego zachowania dotyczą zarówno zachowań ogólnych, jak i komunikacji, tworzenia i prowadzenia stron internetowych, blogów, forów. Netykieta uczy odpowiedzialności za zamieszczane treści i ich formę, a niestosowanie się do jej zasad może skutkować np. usunięciem z grupy dyskusyjnej, nie spowoduje jednak żadnych sankcji karnych. To dobre i sprawdzone praktyki stosowane przez osoby należące do światowej społeczności zrzeszającej użytkowników Internetu. Aktualizowane i przestrzegane zwiększają znacznie bezpieczeństwo w sieci.

Podsumowanie

Pomimo wielu zagrożeń czyhających we współczesnym świecie, szczególnie związanych z działalnością terrorystyczną, Internet ma tendencje do niepohamowanego i niekontrolowanego rozwoju. Odpowiednio ukierunkowana edukacja w zakresie bezpiecznego użytkowania sieci (prowadzona już od naj-

młodszych lat), budowanie świadomości odnośnie do zagrożeń i ich konsekwencji dla przeciętnego człowieka, zarówno w pracy, jak i na gruncie prywatnym, odpowiedzialność za podejmowane decyzje, zamieszczane informacje, ich formę oraz sposób przechowywania, stosowanie właściwie dobranych narzędzi i rozwaga oraz netykieta stanowią najlepszą gwarancję bezpieczeństwa w Internecie. Bogate zasoby sieci i dostępne rozwiązania wykorzystywane w słuszny i odpowiedzialny sposób wzbogacają człowieka, pozwalając na korzystanie z dobrodziejstw nowoczesnych rozwiązań technologicznych i technicznych, zachowując niezależność i wolność wyboru.

Internet jest „zjawiskiem" zasługującym na szczególną troskę w zakresie utrzymania wolności słowa i wygłaszanych tą drogą poglądów oraz likwidowania barier międzyludzkich i terytorialnych. Wprowadzenie RODO (*Rozporządzenia Parlamentu Europejskiego i Rady UE w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych* i *w sprawie swobodnego przepływu takich danych*), cenzury związanej z „poprawnością wypowiedzi" oraz przyjętej *Ustawy o prawach autorskich i jednolitym rynku cyfrowym* stanowi jedno z bardziej znaczących zagrożeń, gdyż znacznie ograniczy swobodę wymiany poglądów i informacji, zmieniając tym samym oblicze Internetu.

Literatura

[1] http://euroislam.pl/dzihadysci-po-ciemnej-stronie-sieci/ (data dostępu: 12.04. 2018).
[2] http://libertarianin.org/forum/co-to-jest-darknet/ (data dostępu: 10.05.2018).
[3] http://euroislam.pl/app/uploads/2015/06/18.jpg (data dostępu: 12.04.2018).
[4] Haughey H., Epiphaniou G., Al-Khateeb H.M., *Anonymity networks and the fragile cyber ecosystem*, [in:] Network Security, Vol. 2016, Issue 3, March 2016, p. 10–18.
[5] Inoue D., Suzuki M., Eto M., Yoshioka K., Nakao K., *DAEDALUS: Novel Application of Large-Scale Darknet Monitoring for Practical Protection of Live Networks*, [in:] Recent Advances in Intrusion Detection, Volume 5758 of the series Lecture Notes in Computer Science, 2009, p. 381–382.
[6] http://libertarianin.org/freenet-uwolnij-swoje-ego-cz-1/ (data dostępu: 10.05. 2018).
[7] https://www.torproject.org/ (data dostępu: 7.05.2018).
[8] Grabowski J., *Darknet – internet do którego lepiej nie wchodzić*, [w:] Komputer Świat, maj 2012.
[9] Opulski P., *Po drugiej stronie lustra - ciemne zakątki Internetu*, [w:] Komputer Świat, marzec 2015.

[10] Raport roczny z działalności CERT Polska, Krajobraz bezpieczeństwa polskiego Internetu 2016, https://www.cert.pl/PDF/Raport_CP_2016.pdf (data dostępu: 4.05.2018).
[11] Krakowiak M., Bajor T., Rydz D., *Systemy biometryczne jako metoda zapobiegania zagrożeniom bezpieczeństwa publicznego*, [w:] Inżynieria bezpieczeństwa a zagrożenia cywilizacyjne. Wyzwania dla bezpieczeństwa (red.) Gil Alina, Nowacka U., Chmiel M., Centralna Szkoła Państwowej Straży Pożarnej w Częstochowie, Częstochowa 2013, s. 273–280.
[12] Prauzner T., *Systemy monitoringu w inteligentnym budynku*, [w:] Prace Naukowe AJD, Edukacja Techniczna i Informatyczna red. A. Gil, tom VII, 2012, s. 113–124.
[13] Prauzner T., *Bezpieczeństwo i edukacja w zmieniającej się rzeczywistości*, [w:] Edukacja XXI wieku, Przestrzenie edukacyjnego współdziałania w budowaniu społeczeństwa obywatelskiego, red. Górecka K., Kukiewicz A., 41 t.2, Wydawnictwo Wyższej Szkoły Bezpieczeństwa, Poznań 2017, s. 31–40.
[14] Kotyśko M., Izdebski P., Michalak M., Andryszak P., Pluto-Prądzyńska A., *Nadmierne korzystanie z sieci społecznościowych*, [in:] Alcoholism and Drug Addiction, Vol.27, Issue 2, 2014, p. 177–194.
[15] http://krytykapolityczna.pl/swiat/fake-newsy-czyli-biznes-jak-kazdy-inny/ (data dostępu: 7.05.2018).
[16] https://tech.wp.pl/do-czego-moze-doprowadzic-wszczepianie-sobie-chipow-pod-skore-6034897528504961a (data dostępu: 15.05.2018).
[17] http://webowadbp.wixsite.com/netykieta (data dostępu:15.05.2018).