MODERN MANAGEMENT REVIEW **2018**
MMR, vol. XXIII, 25 (1/2018), pp. 131-139 **January-March**

Igor PROTASOWICKI[1]

WPŁYW ZAGROŻENIA ATAKAMI DOS/DDOS NA BEZPIECZEŃSTWO TELEINFORMATYCZNEJ INFRASTRUKTURY KRYTYCZNEJ

Rozwój cywilizacyjny sprawił, że działalność człowieka może być wspomagana przez rozwiązania teleinformatyczne niemal w każdym obszarze aktywności. Systemy teleinformatyczne wykorzystywane są także w ramach infrastruktury krytycznej państwa, czyli w obszarze niezbędnym do zapewnienia ciągłości funkcjonowania administracji państwa oraz społeczeństwa. Wielość przetwarzanych, przechowywanych i przekazywanych danych przekłada się na dynamiczny rozwój zagrożeń. Wśród zagrożeń tych wymienia się między innymi ataki typu DoS/DDoS, czyli zagrożenie blokowaniem usług. Do tej pory ataki tego typu wykorzystywane były do przeciążania serwerów WWW sztucznie generowanym ruchem sieciowym, obecnie jednak zważywszy na fakt, że coraz więcej systemów korzysta z łączności za pośrednictwem sieci globalnej zagrożenie to odnosi się także do systemów zarządzających procesami i pełniących inne istotne z perspektywy społeczeństwa funkcje. Jako że zmianie uległa także struktura i poziom skomplikowania samego ataku dotychczas stosowane środki zabezpieczenia mogą wkrótce okazać się nieskuteczne. Niniejszy artykuł stanowi próbę odpowiedzi na pytanie o to, jaki wpływ ataki typu DoS/DDoS mają i mogą potencjalnie mieć w przyszłości na funkcjonowanie krytycznej infrastruktury teleinformatycznej państwa. Posłużono się w tym celu metodami badawczymi właściwymi naukom społecznym: metodą analizy i krytyki literatury przedmiotu jak również analizy i krytyki dokumentów źródłowych, przez dokonanie syntezy dostępnych materiałów źródłowych z zakresu podjętej problematyki oraz danych z badań przeprowadzonych metodami ilościowymi, dotyczących częstotliwości występowania przedmiotowych zagrożeń. W tekście z wykorzystaniem metody obserwacyjnej oraz metody historycznej uwzględniono zarówno charakterystykę systemów, które mogą stać się celem ataku, współczesne metody zabezpieczania przed tymi atakami jak również określono najistotniejsze tendencje obserwowane w przedmiotowym obszarze. Wnioski mogą być wykorzystane do zwiększenia skuteczności zabezpieczenia infrastruktury krytycznej państwa jak również podmiotów prywatnych.

Słowa kluczowe: infrastruktura krytyczna, bezpieczeństwo, systemy teleinformatyczne.

[1] Igor Protasowicki, dr nauk społecznych, inżynier informatyki, specjalista z obszaru bezpieczeństwa energetycznego i teleinformatycznego, dyrektor Instytutu Nauk Informatycznych i Nauk Technicznych Wyższej Szkoły Informatyki, Zarządzania i Administracji w Warszawie; e-mail: igor@protasowicki.eu.
Igor Protasowicki, PhD, Eng, The Academy of Computer Science, Management and Administration, Łabiszyńska 25, 03-204 Warszawa; e-mail: igor@protasowicki.eu.

1. WPROWADZENIE

Postęp technologiczny sprawił, że cywilizacja ludzka XXI wieku tworzy globalne społeczeństwo oparte na wiedzy. Współcześnie niemal nic nie powstrzymuje przepływu informacji między ludźmi oraz tworzonymi przez ludzi podmiotami. Technologie teleinformatyczne, systemy komputerowe oraz rozwiązania mobilne znacząco wspierają działalność człowieka we wszystkich obszarach aktywności zarówno w życiu zawodowym jak i prywatnym. Ilość i różnorodność przetwarzanych, przechowywanych i przetwarzanych informacji doprowadziła do sformułowania pojęcia *big data*, które obecnie weszło do powszechnego użytku, natomiast dostępność rozwiązań sprawia, że większość urządzeń i usług można zaliczyć do rozwijającej się dynamicznie kategorii *always online*, ponieważ bezprzewodowe sieci lokalne w technologii WiFi, łączność komórkowa w systemach GPRS, UMTS, LTE czy łączność satelitarna są na tyle powszechne w skali globalnej, że dostęp do informacji uzyskać można z dowolnego miejsca na świecie w dowolnym momencie[2].

Powszechny dostęp do sieci globalnej umożliwia także zarządzanie w czasie rzeczywistym systemami zaliczanymi do infrastruktury krytycznej państwa oraz dostęp do oficjalnych serwisów informacyjnych prowadzonych przez organy administracji publicznej na stopniu samorządowym i centralnym. Elementy te są narażone na wszystkie zagrożenia występujące w Internecie, dlatego powinny być odpowiednio zabezpieczone, a osoby odpowiedzialne za ich obsługę przygotowane do niezwłocznego podjęcia działań w razie wystąpienia takiej sytuacji.

O powadze przedmiotowego zagrożenia świadczyć może rozległość przedmiotowa wspomnianej infrastruktury krytycznej państwa. Pojęcie to zostało wprowadzone w latach 90. XX wieku w USA i Kanadzie określając nim zbiór systemów teleinformatycznych, technicznych, mechanicznych oraz instalacji wykorzystywanych do zapewnienia nowoczesnym społeczeństwom i tworzonemu przez nie aparatowi administracyjnemu ciągłości funkcjonowania[3]. Rozszerzenie przytoczonej definicji zostało zawarte w Dyrektywie Rady UE 2008/114/WE z dnia 8 grudnia 2008 r. w sprawie rozpoznawania i wyznaczania europejskiej infrastruktury krytycznej oraz oceny potrzeb w zakresie poprawy jej ochrony[4], w której zapisano, że infrastruktura krytyczna oznacza składnik, system lub część infrastruktury zlokalizowane na terytorium państw członkowskich, które mają podstawowe znaczenie dla utrzymania niezbędnych funkcji społecznych, zdrowia, bezpieczeństwa, ochrony, dobrobytu materialnego lub społecznego ludności oraz których zakłócenie lub zniszczenie miałoby istotny wpływ na dane państwo członkowskie w wyniku utracenia tych funkcji[5]. W polskim systemie prawnym definicja infrastruktury krytycznej została zawarta w ustawie z dnia 26 kwietnia 2007 roku o zarządzaniu kryzysowym[6], w której

---

[2] Zob. A. Trifonova, M. Ronchetti, *Mobile Learning: Is Anytime + Anywhere = Always Online?*, Proceedings of the 6th IEEE International Conference on Advanced Learning Technologies, ICALT 2006, Kerkrade 5-7 July 2006.

[3] B. Cichoń, *System zarządzania kryzysowego w kontekście zapewnienia bezpieczeństwa publicznego* [w:] *I Międzynarodowa konferencja naukowa. Wyzwania bezpieczeństwa cywilnego XXI wieku – inżynieria działań w obszarach nauki, badań i praktyki*, red. B. Kosowski, A. Włodarski, Warszawa 2007, s. 28.

[4] Dz. Urz. UE nr L 375/75 z 23.12.2008 r. (dalej jako: Dyrektywa 114).

[5] Art. 2, pkt A Dyrektywy 114.

[6] Tekst jedn. Dz.U. z 2017 r. poz. 209 ze zm. (dalej jako: UZK).

przyjęto, że są to: systemy oraz wchodzące w ich skład powiązane ze sobą funkcjonalnie obiekty, w tym obiekty budowlane, urządzenia, instalacje, usługi kluczowe dla bezpieczeństwa państwa i jego obywateli oraz służące zapewnieniu sprawnego funkcjonowania organów administracji publicznej, a także instytucji i przedsiębiorców[7], dodając przy tym katalog zamknięty składający się z 11 systemów (zaopatrzenia w energię, surowce energetyczne i paliwa, łączności, sieci teleinformatycznych, finansowe, zaopatrzenia w żywność, zaopatrzenia w wodę, ochrony zdrowia, transportowe, ratownicze, zapewniające ciągłość działania administracji publicznej, produkcji, składowania, przechowywania i stosowania substancji chemicznych i promieniotwórczych, w tym rurociągi substancji niebezpiecznych), co można traktować jako słabość tego aktu znacząco ograniczającą jego elastyczność.

Wyselekcjonowane w badaniach zgromadzonych materiałów źródłowych definicje wskazują, jak istotne znaczenie dla funkcjonowania społeczeństwa ma niezakłócone funkcjonowanie infrastruktury krytycznej. Podjęcie odpowiednich kroków w celu zabezpieczenia poszczególnych systemów na wypadek awarii lub ataku należy uznać za jedno z kluczowych zadań państwa[8].

W tym miejscu należy zauważyć, że w ramach krytycznej infrastruktury państwa coraz większą rolę odgrywa jej warstwa teleinformatyczna. Jak już stwierdzono na wstępie, w społeczeństwie informacyjnym, w którym coraz więcej sprzętów wspierających działalność człowieka ma cechę *always online* nie może dziwić fakt powszechnego wykorzystywania sieci globalnej także do przechowywania, przetwarzania i przekazywania informacji przez podmioty administracji publicznej. Wprawdzie najbardziej kluczowe systemy zaliczane do strategicznych zasobów państwa są ze względów bezpieczeństwa odseparowane od Internetu, niemniej jednak wiele spośród pozostałych systemów tej łączności potrzebuje do wykonywania swoich działań i są one narażone na wszelkie zagrożenia, które się z faktem takowego połączenia wiążą.

2. ZAGROŻENIA ZWIĄZANE Z DOSTĘPEM DO SIECI

Jednym z zagrożeń związanych z dostępem do sieci globalnej jest atak DoS/DDoS, czyli tzw. blokada usług (ang. *Denial of Service* oraz *Distributed Denial of Service*). Ataki tego typu wykorzystują słabość architektury TCP/IP oraz serwerów DNS umożliwiającą przeciążenie zasobów systemowych sztucznie wygenerowanym ruchem sieciowym[9]. Wyjaśniając najprościej, sieć komputerowa w praktyce składa się z określonej liczby urządzeń, spośród których każde może w danej jednostce czasu przyjąć określoną liczbę połączeń przychodzących od innych urządzeń – jeśli zatem zmusi się wiele urządzeń w tym samym momencie do nawiązania połączenia z konkretnym urządzeniem w danej sieci, w końcu fizyczny limit połączeń z nim zostanie osiągnięty i każda kolejna próba połączenia zakończy się niepowodzeniem.

---

[7] Art. 3, pkt 2 UZK.

[8] M. Żuber, *Infrastruktura krytyczna państwa jako obszar potencjalnego oddziaływania terrorystycznego*, „Rocznik Bezpieczeństwa Międzynarodowego", Vol. 8, nr 2, Wrocław 2014, s. 179.

[9] Ł. Apiecionek, *Fuzzy Observation of DDoS Attack* [w:] *Theory and Applications of Ordered Fuzzy Numbers. A Tribute to Professor Witold Kosiński*, P. Prokopowicz, J. Czerniak, D. Mikołajewski, Ł. Apiecionek, D. Slezak, Bydgoszcz 2017, s. 240.

Pierwszym podmiotem, który może podjąć odpowiednie kroki po zaobserwowaniu sztucznie generowanego ruchu sieciowego jest dostawca usług internetowych. Jego infrastruktura powinna wychwytywać nienaturalne, odbiegające od normy zachowania sieciowe i je powstrzymywać pociągając autora takiego zachowania do odpowiedzialności przewidzianej umową o świadczenie usług. W tym kontekście jednak poważnym wyzwaniem staje się coraz powszechniejszy proceder podszywania się pod cudzy adres IP. Takie zachowanie znacząco utrudnia określenie danych i lokalizacji osoby odpowiedzialnej za atak, a tym samym monitorowanie ruchu sieciowego staje się coraz większym wyzwaniem. Kolejnym utrudnieniem jest duża łatwość komplikowania drogi, którą podczas ataku pokonują pakiety danych przez dodawanie do niej licznych punktów pośrednich, co uniemożliwia całościowe kontrolowanie przepływu danych od ich źródła[10].

Powagę zagrożenia potwierdza fakt, że na podstawie przeprowadzonych badań firma Arbor Networks zajmująca się zabezpieczaniem sieci przed atakami DoS/DDoS konkluduje, że od 2016 roku dochodzi do 124 tysięcy ataków tego typu tygodniowo, a liczba podmiotów, które doświadczyły przeszło 100 ataków w ciągu tygodnia uległa podwojeniu w stosunku do roku ubiegłego[11]. Do niedawna skuteczną formą ochrony infrastruktury przed atakiem typu DoS/DDoS było stosowanie urządzeń służących równoważeniu obciążenia ruchem sieciowym (ang. *load balancer*), których skuteczność jednak znacząco maleje wraz z rozwojem sieci i zwiększaniem się ilości danych przesyłanych w ramach pojedynczego ataku[12].

Przeprowadzenie omawianego ataku wymaga zaangażowania znacznych zasobów sprzętowych. Jako że mało kto dysponuje własnym rozbudowanym centrum obsługi danych osoby przeprowadzające ataki DDoS wykorzystują w tym celu systemy komputerowe nad którymi przejmują kontrolę za pomocą szkodliwego oprogramowania. Sieć tak przejętych urządzeń, wykorzystywanych do skoordynowanego wykonywania określonego zadania na rzecz autora szkodliwego oprogramowania nazywa się *botnetem*[13]. Po przejęciu kontroli nad szeregiem urządzeń komputerowych można wymusić na nich nawiązanie połączenia z systemem będącym celem ataku oraz wyczerpania jego zasobów systemowych.

Co istotne, współcześnie dynamicznie rozwija się przestrzeń tzw. Internetu rzeczy (ang. *Internet of Things* – IoT), czyli różnych przedmiotów – głównie urządzeń zaliczanych do grupy elektroniki użytkowej – mogących bezpośrednio lub pośrednio przechowywać, przetwarzać i przesyłać informacje za pośrednictwem sieci komputerowych. Termin ten został pierwszy raz użyty jako koncepcja w 1999 roku w prezentacji wygłoszonej w Procter & Gamble przez K. Ashtona[14] i przez minione lata stał się rzeczywisto-

[10] Zob. R. Niranchana, N. Gayathri Devi, H. Santhi, P. Gayathri, *Securing internet by eliminating DDOS attacks* [w:] *14th ICSET-2017. IOP Conf. Series: Materials Science and Engineering*, 263 (2017) 042099.

[11] *Global Threat Landscape NETSCOUT Arbor's 13th Annual Worldwide Infrastructure Security Report*, s. 10.

[12] Biao Han, Xiangrui Yang , Zhigang Sun, Jinfeng Huang, Jinshu Su, *OverWatch: A Cross-Plane DDoS Attack Defense Framework with Collaborative Intelligence in SDN*, "Security and Communication Networks" Vol. 2018, s. 1.

[13] Zob. A. Karim, R. Salleh, M. Khurram Khan, *SMARTbot: A Behavioral Analysis Framework Augmented with Machine Learning to Identify Mobile Botnet Applications*, "PLoS ONE", Vol. 11(3) March 2016.

[14] http://www.rfidjournal.com/articles/view?4986 (dostęp: 4.02.2018 r.).

ścią. W wyniku rozwoju technologicznego na IoT współcześnie składa się wiele sprzętów RTV i AGD, a także elementów tzw. inteligentnych domów itp. Szacuje się, że do 2020 roku liczba urządzeń tego typu na świecie osiągnie łącznie 30 miliardów[15], ale już dziś wiele z nich pada ofiarą złośliwego oprogramowania i włączana jest do *botnetów*[16]. Tym sposobem ataki typu DoS/DDoS mogą być przeprowadzane coraz częściej, a jak wynika z przytaczanych badań ilościowych, ich skuteczność stale rośnie, co wymaga stosowania nowych rozwiązań zabezpieczających.

Administracja publiczna wykorzystuje systemy komputerowe połączone z siecią globalną w celu przechowywania, przetwarzania i przesyłania informacji. Są to zarówno systemy informacji publicznej, informacji wewnętrznej, jak i procedury służące do zarządzania działaniem infrastruktury. Część spośród systemów komputerowych należących do wymienionych kategorii należy do infrastruktury krytycznej państwa i od stabilności ich funkcjonowania zależy bezpieczeństwo obywateli oraz tworzonych przez nich podmiotów. Jeśli funkcjonują w sieci globalnej, to są narażone na ataki DoS/DDoS w takim samym stopniu jak wszystkie inne systemy teleinformatyczne. W historii niejednokrotnie zdarzały się przypadki ataków na strony WWW organów administracji publicznej, jednak w tym przypadku skutki ataku są krótkotrwałe, wiążą się przede wszystkim ze stratami wizerunkowymi i przeważnie nie mają poważniejszych konsekwencji. Dostawcy usług internetowych dokładają starań, by minimalizować ryzyko związane z atakami tego typu wymierzonymi w ich serwisy hostingowe i systemy serwerowe wyposażone są w skuteczne elementy równoważące ruch sieciowy.

Należy jednak zauważyć, że o ile w przypadku systemów teleinformatycznych służących przekazywaniu treści w witrynach WWW skutki ataku można w pewnym stopniu bagatelizować, to w przypadku ataków wymierzonych w systemy odpowiedzialne za zarządzanie infrastrukturą skutki mogą być bardziej poważne. W przypadku przeciążenia ruchem sieciowym infrastruktury wspierającej funkcjonowanie społeczeństwa i nawet czasowego utrudnienia dostępu przez systemy upoważnione skutki mogą bezpośrednio zagrażać mieniu, zdrowiu a nawet życiu obywateli.

Wiele obszarów bezpośrednio związanych z bezpieczeństwem obywateli jest znacząco zależna od szybkości i stabilności przekazywania informacji. Systemy sterowania ruchem kolejowym, lotniczym, drogowym, systemy przesyłu surowców energetycznych oraz energii elektrycznej, jak również systemy finansowe, informacji medycznej itp. umożliwiają dostęp do zasobów oraz podejmowanie decyzji w czasie rzeczywistym. W przypadku zakłócenia komunikacji między podsystemami infrastruktury krytycznej może dojść do opóźnień w istotnym procesie decyzyjnym lub awarii i katastrofy technologicznej. Przy czym należy pamiętać że atak DoS/DDoS nie musi być wymierzony bezpośrednio przeciwko systemowi komputerowemu należącemu do tejże infrastruktury, lecz w system wykorzystywany do wysyłania instrukcji zarządzających procesami na odległość, czyli na przykład przeciwko komputerowi osobistemu urzędnika lub pracownika, który w krytycznych sytuacjach jest odpowiedzialny za podjęcie działań. Uniemożliwienie mu nawiązania

[15] Hsu, Chin-Lung; Lin, Judy Chuan-Chuan, *An empirical examination of consumer adoption of Internet of Things services: Network externalities and concern for information privacy perspectives*, "Computers in Human Behavior" Vol. 62, s. 516–527.

[16] Zob. M. De Donno, N. Dragoni, A. Giaretta, M. Mazzara, *AntibIoTic: Protecting IoT Devices Against DDoS Attacks* [w:] *International Conference in Software Engineering for Defence ApplicationsVolume: Advances in Intelligent Systems and Computing book series* (AISC, Vol. 717).

połączenia z systemem teleinformatycznym należącym do infrastruktury krytycznej może mieć równie poważne konsekwencje, co atak wymierzony przeciwko tej infrastrukturze.

Przeciwdziałanie atakom związanym z blokowaniem usług wymaga zaangażowania znacznych mocy obliczeniowych oraz negatywnie wpływa na szybkość komunikacji. Wiąże się bowiem z koniecznością stałego monitorowania ruchu sieciowego oraz przesyłanych treści pod względem możliwych nieprawidłowości. W kluczowych węzłach sieci globalnej rozmieszczono systemy autonomiczne, które pełnią taką rolę. Niemniej jednak ich praca polega przede wszystkim na pilnowaniu zgodności przesyłanych danych z polityką obowiązującą w danym kanale przesyłu danych[17]. Skuteczność ich działania zależy zatem bezpośrednio od przyjętego modelu zawartego w algorytmach. Im bardziej skomplikowane i dokładne modele matematyczne zostaną zastosowane, tym ich działanie będzie skuteczniejsze, lecz jednocześnie tym większe będą wymagania techniczne obsługującego je systemu teleinformatycznego i tym większy będzie negatywny wpływ na przepustowość kanału komunikacyjnego.

Warto także zaznaczyć, że w ostatnim czasie wzrasta znaczenie komunikacji elektronicznej w funkcjonowaniu urzędów administracji publicznej w kontekście interakcji z obywatelami. Rozwój platformy ePUAP i udostępnienie obywatelom narzędzi do załatwiania spraw urzędowych bez konieczności fizycznej wizyty w urzędzie za pomocą tzw. profilu zaufanego oraz podpisów elektronicznych sprawia, że dostępność witryn internetowych na których obywatele i tworzone przez nich podmioty mogą uzyskać dostęp do przedmiotowego narzędzia także będzie zyskiwać na znaczeniu. Już dziś obrót dokumentów z Zakładem Ubezpieczeń Społecznych odbywa się przede wszystkim w formie elektronicznej i wymaga instalacji odpowiedniego oprogramowania oraz posiadania kwalifikowanego podpisu cyfrowego. Doprowadzenie do analogicznego stanu obrót dokumentów z Urzędami Skarbowymi jak również innymi organami administracji publicznej, które można zaliczyć do przytoczonej wcześniej definicji infrastruktury krytycznej państwa jest tylko kwestią czasu. W stosunku do wspomnianych instytucji obywatele mają określone zobowiązania, których muszą dopełnić w ściśle określonych terminach pod groźbą kar. W przypadku przeprowadzenia ataku DoS/DDoS na element teleinformatycznej infrastruktury krytycznej odpowiedzialnej za obsługę wspomnianych urzędów istnieje ryzyko, że nie wszystkich formalności da się dopełnić w przewidzianym ustawowo terminie i w efekcie obywatele poniosą konsekwencje finansowe a skarb państwa poniesie koszty związane z czasowym wyłączeniem systemu.

3. WNIOSKI I REKOMENDACJE

Mając na uwadze, że ataki DoS/DDoS przeprowadzane są z wykorzystaniem *botnetu* skuteczność zapobiegania zależy nie tylko od zabezpieczeń kontrolujących ruch sieciowy, lecz także od zabezpieczenia urządzeń, które mogą być włączone do sieci *zombie*. Zwiększanie świadomości użytkowników w obszarze konieczności zabezpieczania swoich urządzeń na wypadek ewentualnej infekcji szkodliwym oprogramowaniem oraz propagowanie zachowań na wypadek, gdyby do takiej infekcji doszło może znacząco utrudnić tworzenie *botnetów* w przyszłości, a tym samym ograniczy skuteczność ataków blokady usług. Każdy powinien mieć świadomość, że nie tylko komputery osobiste, ale każde urządzenie działające pod kontrolą programowalnego systemu operacyjnego i podłączone do global-

[17] R. Niranchana, N. Gayathri Devi, H. Santhi, P. Gayathri, *Securing internet*…, s. 124.

nej sieci może paść ofiarą ataku[18]. Można zatem stwierdzić, że rozwój techniczny i zwiększanie się liczby urządzeń służących wspomaganiu człowieka w poszczególnych obszarach aktywności z jednej strony działa na naszą korzyść, przede wszystkim umożliwiając nam oszczędzanie czasu i środków finansowych, z drugiej jednak strony wiąże się z określoną odpowiedzialnością spoczywającą na użytkowniku. Zaniedbanie stanu zabezpieczeń systemów teleinformatycznych może nawet mimo braku intencji oraz świadomości takowych zagrożeń prowadzić do wyrządzenia określonej szkody innym użytkownikom sieci globalnej.

Wspomniane zagrożenia odnoszące się do stabilności funkcjonowania teleinformatycznej infrastruktury krytycznej państwa nie powinny być bagatelizowane. Jak wynika z przytaczanych badań mimo rozwoju zabezpieczeń liczba ataków typu DoS/DDoS sukcesywnie wzrasta. Rozwijają się też metody i środki wykorzystywane do ich przeprowadzania. Skuteczność wykorzystywanych obecnie systemów zabezpieczających jest ograniczona mocą obliczeniową, natomiast działanie odbywa się kosztem przepustowości łącz. Można więc przyjąć, że wkrótce zostanie osiągnięty poziom krytyczny w bilansie ataków i wydatków ponoszonych na zabezpieczenia, prowadzący albo do odczuwalnego ograniczenia sprawności działania globalnej sieci albo do utraty kontroli nad przepływem danych. Dlatego słusznym wydaje się modyfikacja dotychczasowego podejścia skoncentrowanego na rozwijaniu metod i technologii powstrzymywania ataków – zwłaszcza skierowanych przeciwko krytycznej infrastrukturze teleinformatycznej i przeniesienie części odpowiedzialności na użytkowników urządzeń, które mogą być wykorzystane w atakach.

Duża dostępność systemów komputerowych zaliczanych do grupy IoT sprawia, że przeprowadzanie ataków DoS/DDoS jest relatywnie łatwe i tanie. Zwiększenie świadomości użytkowników w obszarze konieczności zabezpieczania swoich urządzeń przed szkodliwym oprogramowaniem może być pierwszym krokiem do utrudnienia rozbudowy sieci *botnet*, a tym samym sprawi, że przeprowadzanie ataków z ich wykorzystaniem stanie się droższe, trudniej dostępne. Tym samym atrakcyjność tej formy ataku zmaleje w oczach potencjalnych zainteresowanych.

Z drugiej jednak strony należy mieć na uwadze, że obszar bezpieczeństwa teleinformatycznego rozwija się szczególnie dynamicznie i wkrótce zagrożenie atakami typu DoS/DDoS zostanie wyparte przez zagrożenie nowego typu i samoczynnie zostanie zmarginalizowane lub wygaśnie niemal zupełnie. Zanim tak się stanie należy dokładać starań, by maksymalnie utrudniać budowę systemów niezbędnych do przeprowadzania ataków oraz zabezpieczać krytyczne systemy teleinformatyczne na wypadek ich przeprowadzenia.

Literatura

1. Apiecionek Ł., *Fuzzy Observation of DDoS Attack* [w:] *Theory and Applications of Ordered Fuzzy Numbers. A Tribute to Professor Witold Kosiński*, P. Prokopowicz, J. Czerniak, D. Mikołajewski, Ł. Apiecionek, D. Slezak, Bydgoszcz 2017.
2. Biao Han, Xiangrui Yang , Zhigang Sun, Jinfeng Huang, Jinshu Su, *OverWatch: A Cross-Plane DDoS Attack Defense Framework with Collaborative Intelligence in SDN*, "Security and Communication Networks" Vol. 2018.

[18] M. De Donno, N. Dragoni, A. Giaretta, M. Mazzara, *AntibIoTic: Protecting IoT…*, s. 217.

3. Cichoń B., *System zarządzania kryzysowego w kontekście zapewnienia bezpieczeństwa publicznego* [w:] *I Międzynarodowa konferencja naukowa. Wyzwania bezpieczeństwa cywilnego XXI wieku – inżynieria działań w obszarach nauki, badań i praktyki*, red. B. Kosowski, A. Włodarski, Warszawa 2007.
4. De Donno M., Dragoni N., Giaretta A., Mazzara M., *AntibIoTic: Protecting IoT Devices Against DDoS Attacks* [w:] *International Conference in Software Engineering for Defence ApplicationsVolume: Advances in Intelligent Systems and Computing book series* (AISC, Vol. 717).
5. *Global Threat Landscape NETSCOUT Arbor's 13th Annual Worldwide Infrastructure Security Report*.
6. Hsu, Chin-Lung; Lin, Judy Chuan-Chuan, *An empirical examination of consumer adoption of Internet of Things services: Network externalities and concern for information privacy perspectives*, "Computers in Human Behavior" Vol. 62.
7. Karim A., Salleh R., Khurram Khan M., *SMARTbot: A Behavioral Analysis Framework Augmented with Machine Learning to Identify Mobile Botnet Applications*, "PLoS ONE", Vol. 11(3) March 2016.
8. Niranchana R., Gayathri Devi N., Santhi H., Gayathri P., *Securing internet by eliminating DDOS attacks* [w:] *14th ICSET-2017. IOP Conf. Series: Materials Science and Engineering*, 263 (2017) 042099.
9. Trifonova A., Ronchetti M., *Mobile Learning: Is Anytime + Anywhere = Always Online?*, Proceedings of the 6th IEEE International Conference on Advanced Learning Technologies, ICALT 2006, Kerkrade 5-7 July 2006.
10. Żuber M., *Infrastruktura krytyczna państwa jako obszar potencjalnego oddziaływania terrorystycznego*, „Rocznik Bezpieczeństwa Międzynarodowego", Vol. 8, nr 2, Wrocław 2014.

THE IMPACT OF DOS/DDOS ATTACKS ON THE SECURITY OF CRITICAL ICT INFRASTRUCTURE

The development of modern civilization has meant that human activity can be supported by ICT solutions in almost every area. ICT systems are also used within the critical infrastructure of the state, that is in the area necessary to ensure the continuity of society and the state administration. The multiplicity of processed, stored and transmitted data translates into a dynamic development of threats. These threats include, among others, DoS/DDoS attacks, that is the threat of blocking services by the denial of service. Until now, this type of attacks have been used to overload web servers with artificially generated network traffic, but currently, given the fact that more and more systems are using communication via the global network, this threat also applies to process management systems and other relevant for society functions. As the structure and level of complexity of the attack have also changed, the previously used security measures may soon prove ineffective. This article is an attempt to answer the question of what impact DoS/DDoS attacks have and may potentially have in the future on the functioning of the country's critical ICT infrastructure. It includes both the characteristics of systems that may become the target of the attack, modern methods of protecting against these attacks, as well as the most important trends observed in the area.

The conclusion can be used to increase the effectiveness of securing critical infrastructure of the state as well as private entities.

Keywords: critical infrastructure, security, ICT systems.

DOI: 10.7862/rz.2018.mmr.9

Tekst złożono w redakcji: luty 2018 r.
Przyjęto do druku: marzec 2018 r.