Ekonomiczne Problemy Usług nr 1/2017 (126), t. 2

ISSN: 1896-382X | www.wnus.edu.pl/epu
DOI: 10.18276/epu.2017.126/2-21 | strony: 205–218

Marcin Krysiński, Przemysław Miller, Anna Pamuła
Uniwersytet Łódzki
Wydział Zarządzania
Katedra Informatyki
e-mail: marcin.krysinski@gmail.com, przemekm1@op.pl, apamula@wzmail.uni.lodz.pl

Zagrożenia typu *Distributed Denial of Service* jako przykład ryzyka związanego z prowadzeniem działalności gospodarczej w internecie

Kody JEL: A12, L86, O30, 039
Słowa kluczowe: DDoS, bezpieczeństwo danych, ryzyka działalności gospodarczej
Streszczenie. W artykule podjęto tematykę zagrożeń związanych z atakami DDoS[1] na działalność przedsiębiorstw. Ze względu na masowość korzystania z internetu jako medium komunikacji, ataki na systemy informatyczne, telekomunikacyjne i produkcyjne nie są już przedmiotem zainteresowania wyłącznie specjalistów ds. bezpieczeństwa informacji i IT, gdyż ich konsekwencje są odczuwalne dla zarządów firm oraz innych interesariuszy. W artykule poddano analizie problem ataków DDoS, jako przykład ryzyka związanego z prowadzeniem działalności gospodarczej. Przedstawiono studium przypadku oraz uproszczony model zastosowanego procesu postępowania w przypadku masowego ataku DDoS.

Wprowadzenie

Przetwarzanie, dostęp do danych oraz ich szybki i bezpieczny transfer należą do podstawowych potrzeb współczesnych organizacji, w tym organizacji gospodarczych. Naprzeciw tego rodzaju potrzebom wychodzą technologie internetowe oferowane przez branże IT, zaliczające się do najszybciej rozwijających gałęzi współczesnej gospodarki. Wykorzystanie internetu nie jest jednak wolne od ryzyka. Ryzyko to ma wiele źródeł, do których zalicza się między innymi zagrożenia związane są z naruszeniem danych

[1] Rozproszony atak typu odmowa usługi (*Distributed Denial of Service*).

osobowych, prawa autorskiego, nieuprawnionego transferu danych, praw cywilnych tak dostawców, jak i odbiorców usługi. Z uwagi na potencjalnie globalny zasięg usług dostarczanych za pośrednictwem internetu, ryzyko związane z jego użytkowaniem ma charakter globalny i podlega nie tylko ochronie prawa krajowego, europejskiego, ale także międzynarodowego.

Internet zrewolucjonizował sposób, w jaki prowadzona jest działalność gospodarcza. Dzisiaj globalne przedsiębiorstwa przetwarzają ogromne ilości danych w czasie rzeczywistym, a e-commerce szybko staje się główną siłą napędową handlu. Rozwój e-commerce stworzył nowe możliwości przedsiębiorcom, jednocześnie zwiększając zagrożenia atakami o charakterze przestępczym. Skalę zjawiska dobrze ilustrują dane udostępnione przez jednego z największych dostawców usług dostępu do internetu – Orange Polska. W 2014 roku zespół bezpieczeństwa tego operatora obsłużył 11 379 incydentów bezpieczeństwa, których źródłem bądź celem ataku była sieć usługowa Orange Polska. Informacje o incydentach pochodziły zarówno ze źródeł zewnętrznych, jak i alarmów z wewnętrznych systemów bezpieczeństwa. Wśród ataków i działań naruszających bezpieczeństwo zarejestrowano:

- Spam – wysyłanie niechcianej poczty elektronicznej z urządzeń pracujących w sieci Orange Polska lub do użytkowników tej sieci – to 39% incydentów,
- DDoS – rozproszone ataki blokujące usługę, których jednym ze źródeł bądź celem było urządzenie użytkownika sieci – 28% incydentów,
- Próby włamań – próby uzyskania nieautoryzowanego dostępu do systemu (np. zgadywanie haseł) – 20% incydentów,
- Malware – rozpowszechnianie złośliwego oprogramowania (np. umożliwienie hostowania złośliwej strony internetowej – 7% incydentów (*Raport CERT*…, 2015).

Ataki DoS/DDoS są jednymi z najbardziej popularnych ataków na sieć lub system komputerowy. Atak DoS (*denial of service*) oraz jego odmiana DDoS (*distributed denial of service*) polegają na blokowaniu dostępu do usługi przez zajęcie jej wszystkich wolnych zasobów (np. zalanie nadmiarową ilością danych lub zapytań), co prowadzi do przeciążenia i zawieszenia systemu (Grzelak, Liedel, 2012).

Część teoretyczną artykułu oparto o badania literaturowe. Dla zilustrowania problemu przedstawiono studium przypadku. Przeprowadzona analiza pozwoliła na przygotowanie uproszczony modelu procesu postępowania w przypadku masowego ataku DDoS.

1. Wpływ ryzyka związanego z prowadzeniem działalności w internecie na zarządzanie organizacją

Ryzyko gospodarcze to według Ehrlicha (1981) hipotetyczny brak uzyskania oczekiwanych profitów z prowadzonej działalności gospodarczej, jak również nieoczekiwana strata, względnie przekroczenie zakładanego budżetu. Wzrost ryzyka gospo-

darczego jest odwrotnie proporcjonalny do wiedzy niezbędnej do podjęcia, zmiany, kontynuacji lub zaniechania danej aktywności gospodarczej. Ryzyko to prawdopodobieństwo z jakim dane zjawisko lub działanie może wpłynąć (zarówno negatywnie – zagrożenie, jak i pozytywnie – szansa) na prowadzoną działalność. Przy tym może to dotyczyć całości prowadzonej działalności oraz jej poszczególnych części. Ważną cechą ryzyka jest możliwość oszacowania, z jakim prawdopodobieństwem, jak również na jaką skalę, może ono wystąpić. Bazując na tych informacjach możliwe staje się właściwe zarządzanie ryzykiem (Trocki, 2014)[2].

Jak twierdzą Romanowska i Trocki (2004): „zarządzanie ryzykiem określić można jako formułowanie planu działania nakierowanego na minimalizację lub eliminację negatywnych skutków ryzyka pojawiającego się w różnych obszarach funkcjonowania przedsiębiorstwa oraz poszukiwanie szans rozwoju poprzez podejmowanie przedsięwzięć w sferze podwyższonego ryzyka". Wawrzyniak (1981, s. 456) uważa, że ryzyko jest takim stanem, w którym przynajmniej jeden z czynników jest nieznany. Znane jest natomiast prawdopodobieństwo, z jakim ten czynnik bądź te czynniki mogą wystąpić. Przy czym owo prawdopodobieństwo może być zarówno rzeczywiste, jak i być jedynie subiektywnym odczuciem osoby podejmującej decyzję. Ryzyko można szacować przy użyciu chociażby metod statystycznych bądź też rachunku prawdopodobieństwa.

Ataki prowadzone za pośrednictwem internetu powodują, że krytyczna staje się odpowiednia identyfikacja ryzyka oraz plany zarządzania nim przez firmy. Dotyczy to ryzyka związanego z możliwością ataków typu DDoS, ale też innych zagrożeń. Plan zarządzania ryzykiem staje się dlatego elementem kluczowym dla bezpieczeństwa prowadzenia biznesu każdej organizacji. Naturalnie sam plan nie rozwiązuje jeszcze żadnych problemów związanych z potencjalnymi zagrożeniami. Należy w ramach kompleksowego zarządzania ryzykiem umiejętnie identyfikować zarówno zagrożenia, jak i szanse. Prowadzić jakościową oraz ilościową analizę ryzyka. Planować odpowiednie reakcje na ryzyko, pamiętając o adekwatnych działaniach. Są bowiem różne strategie reakcji na ryzyko.

2. Ataki typu DoS/DDoS

Ataki DDoS są jednymi z najprostszych do wykonania ataków na sieć lub system komputerowy (np. aplikacje i usługi dostępne z poziomu sieci internet), a zarazem jednymi z najgroźniejszych. Ich głównym celem jest utrudnienie lub uniemożliwienie dostępu do usług sieciowych (Biczysko, Korczak, Niedźwiedziński, Mosorow, 2011). Przebieg ataku to zwykle zalewanie atakowanego obiektu odpowiednio spreparowanymi danymi. Przy bardzo dużej ich liczbie dochodzi do błyskawicznej przerwy w działaniu usług oferowanych przez internet. W przypadku ataku na łącze sieciowe celem

[2] Por. też (Krysiński, Miller, Śmierciak, 2015, s. 17).

zazwyczaj jest zajęcie całej dostępnej przepustowości łącza, a co za tym idzie – odcięcie atakowanego celu od zasobów internetu (*Raport CERT*…, 2015). Atak DDoS na usługi sieciowe i systemy organizacji może spowodować niespodziewaną przerwę w działaniu przedsiębiorstwa, powodując wysokie koszty, rzędu tysięcy, a nawet milionów dolarów, niszcząc markę i skutkując odejściem klientów.

Atak DDoS to atak cybernetyczny przeprowadzany z wielu komputerów, które wysyłają serie pakietów, danych lub transakcji do docelowej ofiary (lub ofiar) za pośrednictwem sieci w celu uniemożliwienia korzystania docelowym użytkownikom z usług komputerowych (np. aplikacja internetowa). Ataki DDoS to zwykle wspólny wysiłek cyberprzestępców, usiłujących zatrzymać sprawne funkcjonowanie strony internetowej lub zablokować ją całkowicie. Ataki DDoS nie są nowym zjawiskiem, ale obecnie są zjawiskiem poważniejszym w skutkach z uwagi na nowoczesne zagrożenia i zastosowanie zaawansowanych taktyk. Pojawiają się ze wzmożoną częstotliwością i powodują coraz większe uszkodzenia szybko rosnącej liczby celów na całym świecie. Właściwie każdy ma łatwy dostęp do środków umożliwiających atak DDoS. Proste w użyciu, zautomatyzowane narzędzia można szybko pobrać z rozmaitych stron hakerskich dostępnych w internecie.

Wzrost liczby ataków DDoS wiąże się w dużej mierze z dwoma czynnikami – wzrost liczby światowych botnetów oraz nowe, niewykrywalne techniki ataku. Botnet to grupa zainfekowanych komputerów osobistych lub innych urządzeń. Bot to pojedynczy element (komputer) tzw. botnetu – grupy komputerów zainfekowanych złośliwym oprogramowaniem, pozwalającym na zdalną kontrolę nad wszystkimi komputerami należącymi do botnetu. Boty mogą być wykorzystywane np. do rozsyłania spamu lub prowadzenia ataków DDoS (Grzelak, Liedel, 2012). Te zainfekowane komputery nazywane są botami (lub też zombie). Atakujący może sterować botem na odległość (czasami nazywa się go bot-herderem, właścicielem bota), by przeprowadzać ataki DDoS, wykradać dane z sieci i serwerów ofiary czy też rozsyłać spam poprzez e-mail. Drugim głównym czynnikiem zwiększającym liczbę ataków DDoS jest przejście z metody „na siłę" do bardziej podstępnych ataków. W przypadku ataku „na siłę" atakujący przesyła do sieci docelowej organizacji wyjątkowo dużą ilość danych w celu przeciążenia przepustowości łącza w tej sieci. Tego typu tradycyjne ataki DDoS, nazywane atakami DDoS na poziomie sieci, są dziś nadal bardzo powszechne. Przeciążający atak DDoS na poziomie sieci może zakłócić lub przeładować infrastrukturę sieci do tego stopnia, że nie będzie ona w stanie prowadzić transmisji. Takie ataki mogą wpłynąć na połączenia, routery, zapory sieciowe i serwery dostawcy internetu tak, że jedna lub więcej usług zaczyna stanowić tzw. wąskie gardło, ograniczając lub eliminując możliwość dostawy usług przez serwer.

3. Cele ataków DDoS

Obecnie jedną z głównych motywacji dla przeprowadzania ataków DDoS jest wyłudzenie. Atakujący grozi ofierze przejęciem strony internetowej lub sieci, jeśli nie dostanie okupu (Network Security, 2015). Często groźbie towarzyszy ograniczony atak DDoS, prowadzony w celu podniesienia wiarygodności działań. Po zapłaceniu okupu, atakujący zwykle się wycofuje, jednak ofiara narażona jest na ryzyko kolejnych żądań okupu od samego atakującego lub innych przestępców. W branżach takich jak np. hazard online firmy są zastraszane możliwością zakłócenia ich pracy, często podczas ważnych momentów, takich jak przeddzień wielkich widowisk sportowych.

Inną ważną motywacją dla ataków DDoS jest aktywność polityczna i ideologiczna, zwany również haktywizmem, w którym atakujący nie zgadza się z zasadami i poglądami (lub istnieniem) organizacji i próbuje ukarać ofiarę lub jej zwolenników poprzez atak DDoS. Do uciążliwych ataków dokonywanych przez grupy hacktiwistów, próbujących zwyczajnie zwrócić uwagę na dany problem przez kampanie cyber-wojenne, doszło w Estonii w roku 2007 oraz w Gruzji w 2008 roku, a ostatnia działania takie można zaobserwować na Ukrainie. Inne przykłady ataków DDoS umotywowanych politycznie i ideologicznie, to między innymi ataki przeprowadzone przez grupę haktywistów LulSec przeciwko Senatowi Stanów Zjednoczonych, Centralnej Agencji Wywiadowczej (CIA) i Zarządowi ds. Zwalczania Poważnej Przestępczości Zorganizowanej (*Serious Organized Crime Agency*, brytyjski odpowiednik FBI) (Naked Security, 2011). W grudniu 2010 roku światowa grupa aktywistów znana pod nazwą Anonymous rozpoczęła Operację Payback – serię ataków cybernetycznych na całym świecie przeciwko MasterCard, Visa, PayPal, Amazon oraz innym dużym spółkom i organizacjom, które odcięły środki finansowe dla WikiLeaks w 2010 roku (Komputer Świat, 2010). W Polsce w dniach 14–17 sierpnia 2014 roku przeprowadzono ataki DDoS na strony internetowe www.prezydent.pl oraz www.gpw.pl, a także na niektóre witryny instytucji administracji państwowej. Do wspomnianych ataków przyznała się na swojej stronie grupa przedstawiająca się jako „Cyber-Berkut", podając jako ich powód rzekome zaangażowanie Polski w konflikt związany z sytuacją na Ukrainie (cert.gov.pl, 2014).

Sprawność i prostota, z jaką można przygotować i przeprowadzić atak DDoS na wielką skalę sprawia, że to narzędzie staje się coraz bardziej atrakcyjne dla wielu innych zainteresowanych. Ostatnio można zauważyć znacznie częstsze występowanie hybrydowych, wielowektorowych ataków, przy których atak DDoS zostaje użyty do odwrócenia uwagi od głównego działania. Coraz częściej, cybernetyczni przestępcy przeprowadzają ataki DDoS, aby zająć osoby odpowiedzialne za bezpieczeństwo firmy intensywnymi procedurami, wykorzystując ten czas na inne działania, jak instalacja złośliwego oprogramowania, kradzież danych lub inne formy intruzji. Atak można pomylić ze zwykłą uciążliwością – np. ingerencją grupki amatorów, którzy mają swoje osobiste pobudki (Mansfield-Devine, 2014).

Wyróżnia się dwa główne sposoby dostarczania usług Anty-DDoS – na żądanie i non-stop. Dostawcy usług bezpieczeństwa oferują także opcję hybrydową, tzn. taką,

w której klienci mogą wykorzystać swoje własne zasoby w przypadku niewielkich ataków, a w przypadku większych – mają możliwość przełączenia się na usługi dostawcy. Organizacje oceniając ryzyko i koszty z nim związane powinny rozważyć zalety i wady każdego rozwiązania (Holland, Ferrara, 2015):

1. Rozwiązanie na żądanie – zapewnia usługi tylko wtedy, gdy są konieczne. Tego typu rozwiązania uruchamia się ręcznie lub automatycznie wtedy, gdy klient bądź dostawca wykryje atak DDoS. Dostawcy oferują ten sposób, gdy skala ataku jest mała, i powoduje tylko opóźnienie aplikacji. Klient (lub też dostawca działający w imieniu klienta) wykorzystuje zmiany BGP lub przekierowanie DNS, by przesłać ruch w jego sieci za pomocą infrastruktury dostawcy.
2. Rozwiązania non-stop – nie wymagają przekierowania ani zmian DNS. Zaletą rozwiązania non-stop jest brak potrzeby zmieniania przekierowania BGP i protokołów DNS. Rozwiązania te są najlepsze w przypadku częstych ataków. Wielu dostawców, którzy oferują rozwiązania non-stop twierdzi, że wpływają one na opóźnienie aplikacji. Ponadto dobrze działają z aplikacjami dostawy zawartości, ponieważ dostawca może powiązać usługi DDoS z usługą dostawy zawartości.
3. Rozwiązanie hybrydowe – oferuje wszystko, co najlepsze w obu rozwiązaniach, pozwala na użycie swoich własnych narzędzi DDoS w razie konieczności oraz zapór sieciowych jako pierwszej linii ochrony. Gdy te rozwiązania przestają wystarczać, klient może przekierować ruch do centrum dostawcy w celu uzyskania dodatkowych możliwości naprawczych.

Preferowane podejście zależy od wielu aspektów, w tym: infrastruktury firm, lokalizacji geograficznej centrum danych klienta, centrum zasobów i dostępnej przepustowości.

4. Ryzyko związane z atakiem DDoS

Nieprzygotowana, zaskoczona atakiem DDoS ofiara nie ma w większości przypadków możliwości obrony bądź też potencjalne środki obrony są tylko pozorne (np. restart aplikacji, serwerów, urządzeń), nie prowadząc do pełnego przywrócenia usługi. Odcięcia atakowanego serwisu od sieci nie można nazwać środkiem zaradczym, skoro właśnie to było celem atakującego. Obserwowane w grudniu 2014 roku (okres świąteczny) ataki na serwisy potentatów rozrywki sieciowej (PSN i XBOX Live) spowodowały straty finansowe liczone w milionach dolarów (Karami, Park, McCoy, 2015). Ataków DDoS będących w stanie zablokować usługi największych korporacji jest coraz więcej – choćby z racji dużej podaży botnetów, które można wykorzystać do ataku. Dzięki temu takie „usługi" są na czarnym rynku dostępne za niewielkie pieniądze.

Równie niebezpieczne są kilkuminutowe ataki proponowane za darmo w ramach „testu usługi" coraz bardziej powszechnego trendu związanego z oferowaniem usług typu CaaS (*Crime as a Service*). Pięciominutowy atak w zupełności wystarcza, aby uniemożliwić wykonanie transakcji w określonym czasie, zablokować dostęp do usługi w krytycznym

czasie czy wylogować gracza z gry online podczas e-sportowych rozgrywek. DDoS jest również używany jako atak pozorowany, mający w rzeczywistości umożliwić przepuszczenie złośliwego ruchu. Często w przypadku braku innych opcji dla zachowania ciągłości biznesu mogą zostać wyłączone bądź przeciążone urządzenia chroniące sieć (np. IPS). DDoS może też mieć na celu ukrycie pośród milionów pakietów znamion włamania i nieautoryzowanego uzyskania dostępu do serwerów przedsiębiorstwa (*Raport CERT*…, 2015).

E-commerce to siła napędowa wielu biznesów. Zgodnie z wspomnianym wcześniej badaniem, przeprowadzonym w 2015 roku przez firmę Gemius, wartość rynku E-commerce w Polsce szacowana była na 27 mld zł (Gemius, 2015). E-commerce funkcjonuje, ponieważ strony e-commerce są elastyczne, bezpieczne i dostępne na żądanie. Niestety z ogromnych możliwości internetu korzystają nie tylko przedstawiciele legalnego biznesu. Przestępcy sprawnie przenieśli się do internetu jak tylko rozmiar biznesów internetowych i transakcji online osiągnął punkt krytyczny. Firmy e-commerce są całkowicie dostepne (24/7) i udzielają odpowiedzi klientom na swoich stronach w czasie rzeczywistym. Za sprawą ataków DDoS biznes ten może stracić tysiące, a nawet setki dolarów, jeśli ich usługi zostaną spowolnione lub strona przestanie działać. Długotrwałe przerwy w dostawie usług mogą być katastrofalne w skutkach, zarówno jeśli chodzi o utratę dochodu, jak i szkodę dla firmy. Jeśli chodzi o klientów – dla nich taki biznes istnieje tylko wtedy, gdy działa jego strona internetowa. Jeśli przestaje działać, to klienci zwyczajnie znajdują stronę konkurencji i mogą już nie wrócić. Zakłócenia w funkcjonowaniu strony internetowej trwające dłuższy okres mogą wpłynąć na biznes i znacznie obniżyć pewność klientów.

Spółki działające online są również odpowiedzialne za powierzone im poufne dane klientów, w tym dane uwierzytelniające konta, dane z kart kredytowych oraz dane osobowe. Nawet jeśli atak DDoS nie doprowadzi do wypłynięcia danych, to klienci będą mieć wrażenie, że strona firmy nie jest bezpieczna, co może przyczynić się do strachu przed dokonywaniem transakcji biznesowych na tej stronie i unikania korzystania z niej.

Internet zrewolucjonizował sposób, w jaki funkcjonują instytucje finansowe, począwszy od internetowych usług bankowych, aż po szybkie transakcje globalne i przetwarzanie płatności. Transakcje finansowe na całym świecie odbywają się w błyskawicznym tempie, umożliwiając instytucjom, partnerom i klientom szybką reakcję na zmieniające się warunki finansowe i wymagania rynku. Klienci oczekują, że ich dane będą bezpieczne i że usługi są godne zaufania, szybkie i dostępne zawsze w razie potrzeby. W przypadku internetowych transakcji bankowych i finansowych – czas to pieniądz. W kilka minut można stracić miliony dolarów, jeśli usługa zostanie spowolniona lub zakłócona. W środowiskach, w których ważną rolę gra wydajność, na przykład w przetwarzaniu transakcji i dużej wymianie handlowej poważne zakłócenia w funkcjonowaniu usługi mogą przynieść katastrofalne skutki zarówno jeśli mowa o właściwej stracie finansowej, jak i szkodzie dla marki firmy. Wiele milionów osób angażuje się w internetowe gry hazardowe od pokera po bingo i gra w gry wideo, takie jak strzelanki i szeroko rozpowszechnione gry fantasy na platformach, w tym

PC, Microsoft Xbox i Sony PlayStation. Według raportu Global Betting and Gaming Consultants wartość światowego przemysłu internetowych gier hazardowych wzrosła o 12% w 2010 roku – do 29,3 mld USD (Stradbrooke, 2010). Według Online Gaming Association 20 mln użytkowników Microsoft Xbox spędza 12 mld godz. online; istnieje 40 mln kont Sony PlayStation Network.

Poza zagrożeniem ze strony DDoS firmy prowadzące działalność za pośrednictwem internetu, podobnie jak inne spółki angażujące się w e-commerce i transakcje finansowe, stoją na straży poufnych danych użytkowników i informacji finansowych i muszą z tego powodu działać w zgodzie z rozmaitymi przepisami i licznymi państwowymi wymogami dotyczącymi zachowania poufności danych. Ogólne załamanie w etyce biznesowej sprawia że firmy, które angażują się w szpiegostwo przemysłowe korzystają również z sabotażu, by zyskać nieuczciwą przewagę konkurencyjną. Zwykle tego typu ataki DDoS wobec konkurencji firma zleca osobom trzecim. Poszkodowana firma może znacząco ucierpieć pod względem kosztów bezpośrednich, które obejmują utracony dochód i koszt naprawienia szkód, jak również koszty pośrednie (zwykle o wiele większe niż bezpośrednie) związane z nadszarpnięciem reputacji i utratą przyszłych możliwości biznesowych.

5. Atak na system EDI – studium przypadku

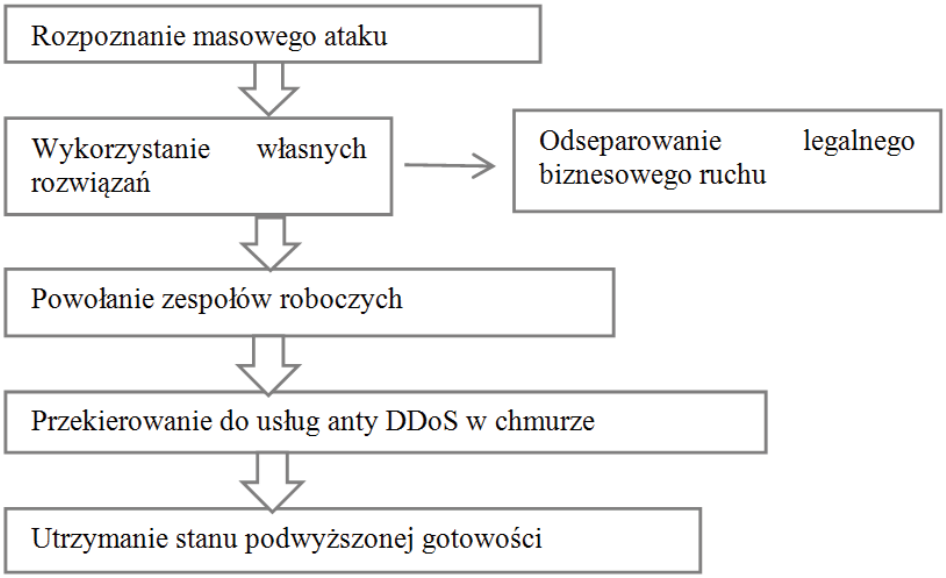
Elektroniczna wymiana danych (EDI – *Electronic Data Interchange*) jest formą wymiany informacji między komputerowymi systemami różnych organizacji. Oznacza ona bezpośrednią wymianę zestandaryzowanych dokumentów i komunikatów przekazywanych drogą elektroniczną między komputerami dwóch organizacji (Miller, 2015). Aby uniknąć konieczności budowania połączeń między poszczególnymi podmiotami gospodarczymi, korzysta się z kolei z usług pośrednika – operatora, który centralnie zarządza danymi (dokumentami). Jednostka przesyła dokumenty elektroniczne do operatora, a ten przekazuje je do ich odbiorcy. W tej sytuacji pośrednik funkcjonuje jako biuro rozliczeń dla transakcji realizowanych za pomocą elektronicznych usług o dużej szybkości przesyłania danych. Operatorami są wyspecjalizowane firmy informatyczne (Nadolna, 2012), które często są narażone na ataki.

Jedna z polskich firm oferująca tego typu usługi była celem ataków DDoS w listopadzie 2015 roku. Atak rozpoczął się 15-minutowy atakiem rozpoznawczym. Atakujący prawdopodobnie skorzystali z ataku proponowanego za darmo w ramach „testu usługi" typu CaaS (*Crime as a Service*). Początkowo atak został zignorowany, ale skala ataków dramatycznie wzrosła – uderzono w 15 serwisów jednocześnie, po czym zaatakowano wszystkie usługi świadczone w centrum danych, wykorzystując wiele rodzajów skomplikowanej taktyki. Aby uchronić się przed atakiem, na początek podjęto decyzję o przeniesieniu prefixu IP BGP do innego centrum. Podjęto również próby odizolowania legalnego biznesowego ruchu sieciowego od ruchu tworzonego przez boty. Drugi etap ataku był dla firmy druzgocący i przyniósł wiele konsekwencji, gdyż działania prowadzone przez napastników znacząco wpływały na inne przedsiębiorstwa

(klientów firmy), korzystające z usługi EDI. W wyniku ataku nastąpiła blokada dostępu do kluczowej dla klientów infrastruktury. W reakcji na działania napastników z obiegu sieci odłączono główne centrum danych. Zespół pracujący w firmie nad unieszkodliwieniem ataku postanowił nawiązać kontakt z przedsiębiorstwami, które ostatnio zmagały się z atakami DDoS. Analiza uzyskanych informacji wykazała, że atak był prowadzony przez bardzo groźnych, zupełnie nieznanych dotąd napastników, których celem wydawało się być zablokowanie usługi EDI za wszelką cenę. Ataki nie ustawały w ciągu kolejnych godzin. Dla ich osłabienia zastosowano podejście metodyczne z podziałem prac na powołane zespoły zadaniowe. Jeden z zespołów został szybko oddelegowany do pozyskania informacji na temat ataku, drugi zajął się szukaniem rozwiązania, a trzeci prowadził rozmowy z partnerami firmy dostarczającymi usługi Anty-DDoS. Firma dysponowała zapleczem potrzebnym do zwalczania takich ataków. Zespół do spraw sieci i bezpieczeństwa zatrudniał inżynierów zarządzania siecią oraz dysponował odpowiednim budżetem. Po kilku godzinach pracy wszystkich zespołów podjęto decyzję o przekierowaniu całego ruchu kierowanego do platformy EDI do firmy świadczącej usługi Anty-DDoS w chmurze, co zostało przeprowadzone za pomocą protokołu BGP. Ze względu na sposób działania tej metody, jej efekty nie były widoczne natychmiast, poprawę zauważono wczesnym rankiem następnego dnia. Ataki wprawdzie nie ustawały, lecz ich skutki zostały znacząco zmniejszone. Przez kolejny tydzień powołane zespoły pozostawały w gotowości do podjęcia kolejnych działań w przypadku powrotu ataku. Tydzień to bardzo długi okres na prowadzenie ataków DDoS, lecz nie można było wykluczyć, że napastnik podejmie nowe lub zmodyfikowane działania i będzie próbować atakować ponownie.

Analizując przebieg ataku, zauważono, że przypomina on środki używane przez hakerów pracujących dla rządu np. Korei Północnej bądź zorganizowane grupy w krajach dopuszczających taką działalność (np. Rosja). Niestety nie udało się zidentyfikować sprawców. Grupa napastników nigdy nie wysunęła żadnych żądań, nikt również nie podpisał się pod tym atakiem. Prawdopodobnie jedynym celem ataku było utrzymywanie zaatakowanej firmy w trybie offline. W wyniku tego ataku dostęp do systemu EDI poprzez stronę WWW był niemożliwy przez kilkanaście godzin, a przez 4 dni występowały przejściowe trudności w dostępie do niego.

Uproszczony model działań zastosowany przez firmę do odparcia ataku DDoS przedstawiono na rysunku 1.



Rysunek 1. Model działań dla odparcia ataku DDoS

Źródło: opracowanie własne.

Należy dodać, że ataki DDoS nakierowane na firmy nie ustały. Platforma EDI jest częsta atakowana, ale obecnie firma potrafi sobie z tym poradzić. Pomijając kilka krótkich przerw w działaniu serwisu, związanych z jego rekonfiguracją w ciągu ostatnich miesięcy udało się utrzymać dostępność usług, a także zachować efektywność systemu ochrony. Jako jeden z dostawców usług EDI firma ma dostęp do danych wielu firm, co niestety sprawia, że staje się częstym celem ataków. Nie można również wykluczyć, że najpoważniejszy atak był finansowany przez konkurencję.

Bazując na zaprezentowane w artykule studium przypadku, można zaproponować model postępowania związanego z atakami DDoS. Pierwszym bardzo istotnym krokiem jest uświadomienie i zaakceptowanie możliwości wystąpienia ataku DDoS. Kolejnym etapem powinno być podjęcie decyzji o sposobie reakcji na ryzyko wystąpienia ataku DDoS. Ze względu na skomplikowany charakter oraz możliwe skutki autorzy rekomendują przeniesienie ryzyka przez zawarcie umowy z dostawcą rozwiązań Anty-DDoS, ale to od charakteru prowadzenia działalności powinno zależeć jaki model ochrony firma wybierze.

Podsumowanie

Z roku na rok obserwowany jest wzrost siły ataków DDoS, spowodowany nie tylko coraz większą dostępnością i przystępnością cenową szerokopasmowych łączy internetowych oraz większą liczbą urządzeń w sieci, lecz także stosowaniem nowych

technik wzmacniania ataków oraz spadkiem cen na czarnym rynku za opłacenie ataku. Zbyt wiele organizacji jest nieodpowiednio przygotowanych jednak, by poradzić sobie ze skutkami ataków DDoS oraz innymi zagrożeniami bezpieczeństwa internetowego. Brak adekwatnych rozwiązań, zabezpieczeń dotyczy również sektora państwowego. Raport kwartalny (styczeń–kwiecień 2012 r.) opublikowany na stronie rządowej w 2012 roku (*Raport z działalności*…, 2012) wskazywał, że tylko około 7% stron internetowych w domenie .gov.pl ma akceptowalny poziom bezpieczeństwa, a 18% to strony cechujące się nieakceptowalnym niskim poziomem bezpieczeństwa. W raporcie zwrócono uwagę na to, że coraz częściej występują nietypowe incydenty, niewykrywane przez standardowe systemy bezpieczeństwa. Zdaniem autorów raportu, wiąże się to z globalną tendencją stosowania ataków w cyberprzestrzeni do nielegalnego zdobywania informacji z systemów należących do konkretnych instytucji (Grzelak, Liedel, 2012).

Zabezpieczania przed DDoS mają te same mankamenty, co każdy inny obszar bezpieczeństwa internetowego. Większość organizacji jest w dalszym ciągu nieprzygotowana na ataki DDoS. Jest to po części efekt braku świadomości (przypisanie przerw w dostawie usługi innym czynnikom), po części braku chęci poniesienia odpowiednich, kapitałochłonnych wydatków. Niektóre firmy twierdzą, że nie są i nie będą potencjalnym celem ataków z uwagi na charakter prowadzonej działalności gospodarczej. Inni utożsamiają DDoS z hacktivismem lub polityką, które wydają im się ideami bardzo odległymi od działalności. Niestety istnieje trend powodujący, że można paść ofiarą ataku DDoS nawet, jeśli nie jest się jego celem. Związane to jest z ogromnym wzrostem konsolidacji centrów danych i użyciem usług w chmurze. Jeśli jakieś przedsiębiorstwo przeniesie część lub całość swojej obecności w sieci do chmury, wystawi się tym samym na potencjalny atak. Celem tego ataku nie musi być przedsiębiorstwo, lecz samo centrum danych lub też inni jego współużytkownicy.

Korzystanie ze wspólnych zasobów niesie w tym przypadku nowe wyzwania. Z jednej strony sprawia, że zasoby przedsiębiorstwa są lepiej dostępne w internecie. Z drugiej usługi zostają przeniesione do środowiska o dużym prawdopodobieństwie wystąpienia ryzyka ataku. Należy zatem żądać gwarancji, że dostawca usługi/rozwiązania w chmurze będzie stosował adekwatne do zagrożenia rozwiązania bezpieczeństwa.

Trudno ocenić, czy firma potrzebuje, co prawda, drogich, ale bardzo użytecznych usług chroniących przed atakami DDoS. Przeprowadzenie analizy ryzyka nie daje wymiernych rezultatów. Coraz więcej przedsiębiorstw zaczyna jednak stawiać na takie bezpieczeństwo. Z przeprowadzonej przez firmę Verisign ankiety wynika, że aż 71% przedsiębiorców niemających tej ochrony, przyznało, że zamierzają włączyć ją do swojego planu budżetowego (Network Security, 2011, s. 11). Świadomość zagrożenia w dużym stopniu zależy od rodzaju branży, w której działa dana firma. Oczywiście wiele organizacji jest obecnie zagrożonych atakami DDoS, ale prawdopodobieństwo ataku jest wielokrotnie wyższe w odniesieniu np. do stron banków, e-commerce czy usług hazardowych online, Przedsiębiorstwa, w których usługi online stanowią więcej

niż 10% całkowitego dochodu doskonale zdają sobie sprawę z istnienia ataków DDoS. Można zatem stwierdzić, że ataki DDoS to problem z utrzymaniem ciągłości biznesowej, a nie kwestia bezpieczeństwa. Większe przedsiębiorstwa mają już odpowiednią infrastrukturę zdolną do udźwignięcia ogromnego ruchu w sieci. Bardzo często zawiązują również umowy z dostawcami internetu na wypadek nagłego napływu ruchu. Nie z powodu obawy przed atakami DDoS, ale w celu zagwarantowania nieprzerwanej dostępności usług. Wiele firm prawdopodobnie wciąż traktuje ataki DDoS jako formę łamania zabezpieczeń, mimo że bardzo rzadko skutkują one kradzieżą danych czy też włamaniami do systemu. To, że jest to raczej problem odporności na owe ataki niż kwestia zabezpieczenia, bywa dla wielu firm zaskakujący.

Jak pokazują wyniki badania PWC, w wielu firmach temat cyberzagrożeń wciąż nie znajduje się odpowiednio wysoko na agendzie zarządów. Prezesi światowych przedsiębiorstw wskazali na zagrożenia związane z cyberbezpieczeństwem jako na drugie najważniejsze ryzyko mogące zagrozić prowadzonym interesom. Tymczasem w Polsce często główne działania w tym obszarze wciąż koncentrują się jedynie na osiąganiu zgodności z wymogami ustawowymi, związanymi przede wszystkim z ochroną danych osobowych. W obliczu rosnących zagrożeń warto, aby firmy niemające specjalistów w tym zakresie, rozważyły ich zatrudnienie lub skorzystanie ze wsparcia zewnętrznego, a firmy dysponujące takim zespołem pomyślały nad jego rozbudową w przyszłości (PWC, 2015).

Bibliografia

Biczysko, D., Korczak, K., Niedźwiedziński, M., Mosorow, W. (2011). Model analizy skutków ataku DDoS na serwis internetowy. *Studia i Materiały Polskie Stowarzyszenie Zarządzania Wiedzą*, *53*, 19–29.

Choi, J., Choi, C., Ko, B., Kim, P. (2014). A method of DDoS attack detection using HTTP packet pattern and rule engine in cloud computing environment *Soft Computing*, 18, 1697–1703.

Ehrlich, A. (1981). Ryzyko gospodarcze. W: L. Pasieczny (red.), *Encyklopedia organizacji i zarządzania*. Warszawa: PWE.

Gemius Polska (2015). *E-commerce w Polsce 2015*. Warszawa.

Grzelak, M., Liedel, K. (2012). Bezpieczeństwo w cyberprzestrzeni. Zagrożenia i wyzwania dla Polski – zarys problemu. *Bezpieczeństwo Narodowe*, *22*, 125–139.

Holland, R., Ferrara, E (2015). *DDoS Services Providers, Q3 2015*. Cambridge: Forrester Research..

Karami, M., Park, Y., McCoy, D. (2015). *Stress Testing the Booters: Understanding and Undermining the Business of DDoS Services*. Nowy Jork: Cornel University Press..

Kasprzak, T. (2003). *Biznes i technologie informacyjne – perspektywa integracji strategicznej*. Warszawa: Wydawnictwo Naukowe PWN.

Komputer Świat (2010). *Operacja Payback, rok 2010, nowa era haktywizmu*. Pobrano z: http://www.komputerswiat.pl/artykuly/redakcyjne/2013/11/top-5-najwiekszych-atakow-ddos,5.aspx (8.04.2015).

Krauz, A. (2013). Internet narzędziem groźnej broni cyfrowej dla infrastruktury krytycznej w globalnym świecie wiedzy. *Edukacja – Technika – Informatyka*, *4*, 388–399.

Krysiński, M., Miller, P., Śmierciak, M. (2015). Zarządzanie ryzykiem projektu na przykładzie projektu „Instalacja infrastruktury odbioru sygnału WiFi". W: W. Grzegorczyk (red.), *Wybrane problemy zarządzania i finansów Studia przypadków* (s. 17–27). Łódź: Wydawnictwo Uniwersytetu Łódzkiego.

Mansfield-Devine, S. (2014). *The evolution of DDoS*. Computer Fraud & Security.

Miller, P. (2015). Nowoczesne narzędzia wspomagające proces finansowania przedsiębiorstw na przykładzie usługi Comarch EDI Finansowanie. W: T.H. Bednarczyk (red.), *Ubezpieczenia i bankowość z perspektywy młodego ekonomisty. Wybrane problemy* (s. 421–429). Lublin: Wydawnictwo Uniwersytetu M. Curie-Skłodowskiej.

Nadolna, B. (2012). Wpływ elektronicznej wymiany danych (EDI) na funkcjonowanie kontroli zarządczej w jednostkach sektora finansów publicznych. *Zeszyty Naukowe Uniwersytetu Szczecińskieg*, *718*. *Finanse. Rynki Finansowe. Ubezpieczenia*, *53*, 81–96.

Naked Security (2011). *CIA website brought down by DDoS attack, LulzSec hackers claim responsibility*. Pobrano z: https://nakedsecurity.sophos.com/2011/06/15/cia-website-down-hackers-lulzsec/ (9.04.2015).

Network Security (2015). *DDoS: attacks grow*. Oxford: Mayfiled Press.

Network Security (2011). *DDoS: threats and mitigation*. Oxford: Mayfiled Press.

PWC (2016). *W obronie cyfrowych granic czyli 5 rad, aby realnie wzmocnić ochronę firmy przed CYBER ryzykiem*.

Radware (2016), Global Application & Network Security Report 2014–2015. Nowy Jork.

Raport CERT Orange Polska za rok 2014 (2015). Warszawa: Orange Polska.

Raport z działalności zespołu CERT.GOV.PL za I kwartał 2012 (2012). Pobrano z: cert.gov.pl.

Raport o stanie bezpieczeństwa cyberprzestrzeni RP w roku 2014 (2014). Pobrano z: cert.gov.pl.

Romanowska, M., Trocki, M. (2014). *Podejście procesowe w zarządzaniu*. Warszawa: Szkoła Głowna Handlowa.

Stradbrooke, S. (2010). *GBGC Reports Online Gambling Market Grew 12% in 2010*. Pobrano z: http://calvinayre.com/2011/02/16/business/gbgc-report-online-gambling-growth/ (7.08.2015).

Światowiec, J. (2005). Koegzystencja marketingu partnerskiego i tradycyjnego. W: M. Skurzyński (red.), *Innowacje w marketingu – młodzi o marketingu* (s. 66–77). Materiały konferencyjne. Sopot: Uniwersytet Gdański.

Trocki, M. (2014). *Nowoczesne zarządzanie projektami*. Warszawa: PWE.

Wawrzyniak, B. (1981). Ryzyko. W: L. Pasieczny (red.), *Encyklopedia organizacji i zarządzania* (s. 456). Warszawa: PWE.

www.uke.gov.pl (1.12.2015).

DDOS RELATED RISKS, EXAMPLE OF THE RISKS ASSOCIATED WITH DOING BUSINESS ON THE INTERNET

Keywords: DDoS, data security, business risk

Summary. The article attempts to determine the impact of the risks associated with DDoS on business. It puts attention to the contemporary dangers of using the Internet as a medium of communication. Attacks against IT are no longer interested for Information security and IT professionals only. Their consequences are felt for management companies and other stakeholders. The article shows the problem of DDoS attacks as an example of the risks associated with doing business. The example shows also how to deal w such threat.

Translated by Marcin Krysiński

Cytowanie

Krysiński, M., Miller, P., Pamuła, A. (2017). Zagrożenia typu Distributed Denial of Service jako przykład ryzyka związanego z prowadzeniem działalności gospodarczej w Internecie. *Ekonomiczne Problemy Usług*, *1* (126/2), 215–218. DOI: 10.18276/epu.2017.126/2-21.