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

ISSN: 1896-382X | www.wnus.edu.pl/epu
DOI: 10.18276/epu.2017.126/2-22 | strony: 219–229

Teresa Mendyk-Krajewska, Zygmunt Mazur, Hanna Mazur
Politechnika Wrocławska
Wydział Informatyki i Zarządzania
Katedra Inżynierii Oprogramowania
e-mail: Teresa.Mendyk-Krajewska@pwr.edu.pl

Nowe technologie informacyjne a rozwój przestępczości elektronicznej

Kody JEL: L86, M15
Słowa kluczowe: bezpieczeństwo e-usług, ataki sieciowe, internet rzeczy
Streszczenie. Powszechnie wykorzystywane niemal we wszystkich dziedzinach życia technologie informacyjne nie są wolne od zagrożeń. Wraz z ich rozwojem i poszerzaniem oferty usług sieciowych, pojawiają się nowe możliwości dokonywania nadużyć i prowadzenia działalności przestępczej drogą elektroniczną. Narzędziem ataku może być każde urządzenie podłączone do sieci. Firmy produkujące oprogramowanie, świadome realnych zagrożeń, wyposażają swoje produkty w coraz bardziej złożone mechanizmy zabezpieczeń, jednak skala zjawiska nie maleje i nic nie wskazuje na znaczącą poprawę bezpieczeństwa sieciowego w niedalekiej przyszłości. Złożony problem przestępczości elektronicznej nabiera w ostatnich latach istotnego znaczenia wobec intensyfikacji działań na rzecz cyfrowych podstaw rozwoju naszego kraju.

Wprowadzenie

Systemy informatyczne są wykorzystywane niemal we wszystkich dziedzinach życia z coraz większą intensywnością. Wdrażanie nowych technologii informacyjnych kształtuje dynamikę rozwoju e-gospodarki na całym świecie. Nowoczesne technologie usprawniają i zdecydowanie przyspieszają realizację usług, ułatwiają komunikację i prowadzenie biznesu. Coraz więcej osób sięga po zasoby internetowe, wykorzystując do tego urządzenia mobilne.

Środowisko infrastruktury informatycznej nie jest jednak wolne od zagrożeń, które niełatwo identyfikować i klasyfikować z powodu ich różnorodności oraz mnogości metod ataków. Skutkiem ataku hakerskiego może być nie tylko zniszczenie danych

czy bezprawny do nich wgląd, ale też przejęcie kontroli nad systemem, a nawet fizyczne uszkodzenie infrastruktury informatycznej. Przyczyn problemów jest wiele – począwszy od zaniedbań w konfiguracji i aktualizacji użytkowanego oprogramowania, poprzez niedoskonałość systemów zabezpieczeń i wykrywania zagrożeń oraz dostępność narzędzi do przeprowadzenia ataku, po świadome ignorowanie ryzyka.

Wraz z rozwojem technologii informacyjnych i popularyzacją usług realizowanych z ich wykorzystaniem, skala zagrożenia niepokojąco rośnie. Nowe technologie stwarzają rozległą przestrzeń do nadużyć i przestępczości elektronicznej. Celem artykułu jest zwrócenie uwagi na problem, którego nie można lekceważyć z uwagi na potencjalne następstwa skutecznych ataków i ich nieprzewidywalny zakres. Jak dotąd, wysiłki na rzecz ochrony systemów teleinformatycznych, wydają się mało skuteczne.

1. Informatyzacja kraju a zagrożenia

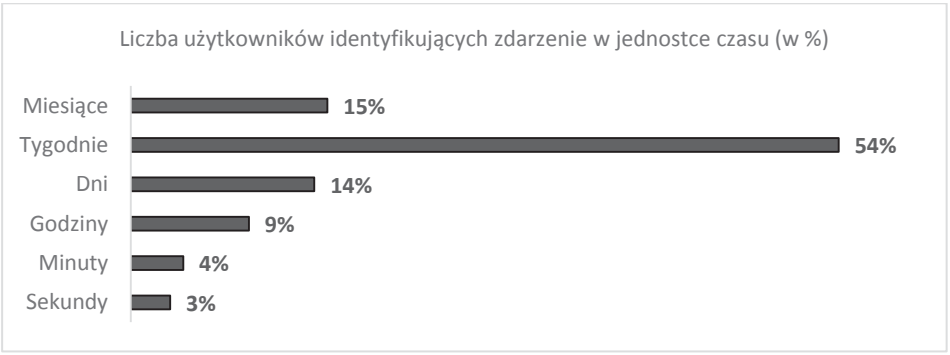
Dla wzmocnienia cyfrowych podstaw rozwoju kraju, Ministerstwo Administracji i Cyfryzacji oraz Ministerstwo Infrastruktury i Rozwoju przygotowały w 2014 roku projekt programu operacyjnego Polska Cyfrowa. Cyfryzacja kraju w ramach tego programu, realizowanego w latach 2014–2020, obejmuje trzy obszary: budowę i rozwój e-administracji, poprawę cyfrowych kompetencji społeczeństwa oraz upowszechnienie dostępu do szybkiego, szerokopasmowego internetu. Celem prowadzonego projektu jest budowa nowoczesnych usług publicznych dla obywateli i przedsiębiorstw.

W 2014 roku z szerokopasmowego dostępu do internetu korzystało 71% gospodarstw domowych, a 86% użytkowników łączyło się z siecią globalną za pomocą urządzeń mobilnych, jednak regularnie (tj. co najmniej raz w tygodniu) korzystało z internetu jedynie 63% Polaków (Polska Cyfrowa, 2016). Rozwój e-usług publicznych i kompetencji cyfrowych w szkołach realizowany jest też w ramach Regionalnych Programów Operacyjnych. Za sukces w procesie cyfryzacji administracji publicznej można uznać system rozliczeń podatkowych, Centralną Ewidencję i Informację o Działalności Gospodarczej, system elektronicznych ksiąg wieczystych oraz platformę ZUS. Wiele innych realizowanych projektów nadal pozostaje w fazie testowania i udoskonalania. Cyfrowy rozwój kraju nie może jednak przebiegać bez dostrzegania problemu zagrożeń dla nowych technologii.

Do nierozwiązanych zagadnień dotyczących użytkowania udostępnianych platform należą m.in.: identyfikacja obywateli oraz ochrona ich danych osobowych. Dostępne rozwiązania w tym zakresie dla wielu zastosowań nie są wystarczająco bezpieczne. Mechanizm potwierdzania tożsamości obywateli i autentyczności dokumentów w elektronicznych systemach administracji, jakim jest profil zaufany, może być stosowany jedynie w przypadku realizacji usług o niewielkim ryzyku.

Żadne systemy zabezpieczeń nie dają stuprocentowej gwarancji, zatem użytkownicy e-usług muszą się liczyć z potencjalnym zagrożeniem. Włamanie się do przeciętnego komputera zwykle nie trwa długo, co pokazują wyniki badań firmy Verizon, ze-

brane w raporcie „Data Breach Investigation Report" (Verizon, 2016). Aż 86% systemów można było przejąć w ciągu niespełna godziny, a do wszystkich atakowanych komputerów udało się hakerom włamać w ciągu jednego dnia! W 12% przypadków skuteczny atak trwał mniej niż minutę. Wyniki przedstawione na rysunku 1 ukazują, po jakim czasie ofiary włamania zauważają to. Okazuje się, że zagrożenie dostrzega tego samego dnia jedynie 16% użytkowników, zaś większość (54%) przynajmniej po tygodniu (do miesiąca) od przeprowadzenia ataku.



Rysunek 1. Dostrzeżenie zagrożenia

Źródło: opracowanie własne na podst. Verizon (2015).

Z raportu Verizon (2016) wynika, że 89% naruszeń bezpieczeństwa danych miało motywację finansową lub szpiegowską, a 65% było efektem słabych, niespełniających wymagań haseł lub ich kradzieży.

Bezpieczeństwo w sieci globalnej to iluzja. Podejmowane próby oceny skuteczności oprogramowania ochronnego wykazują, że standardowe narzędzia antywirusowe znanych firm, takich jak Symantec, McAfee, Microsoft czy Kaspersky Lab., wykrywają jedynie niewielki procent faktycznych zagrożeń.

Najmocniejsze zabezpieczenia wprowadzają systemy kryptograficzne. Dzięki dostępnym algorytmom można zapewnić danym poufność (np. z wykorzystaniem AES[1]), integralność i autentyczność (SHA-3[2], RSA[3]), a komunikującym się w sieci stronom umożliwić bezpieczne połączenie (z użyciem protokołów, takich jak SSL/TLS czy IPsec), jednak systemy kryptograficzne też wykazują podatność na ataki, a dostępność specjalistycznych narzędzi umożliwia podjęcie takich działań nawet osobom niedoświadczonym. Przykładem może być atak typu Man-in-the-middle na protokół SSL z użyciem narzędzia SSLStrip, polegający na podszyciu się atakującego pod router i przechwyceniu ruchu atakowanego użytkownika.

[1] *Advanced Encryption Standard* – symetryczny algorytm szyfrowania blokowego.

[2] *Secure Hash Algorithm 3* – funkcja skrótu używana przy tworzeniu podpisu cyfrowego.

[3] Asymetryczny algorytm szyfr. używany m.in. w realizacji podpisu elektronicznego.

Coraz większa moc obliczeniowa współczesnych komputerów zdecydowanie zwiększa szanse powodzenia ataku siłowego (*brute-force*), polegającego na znalezieniu użytego klucza kryptograficznego[4] przez sprawdzenie wszystkich możliwych jego wartości. Wraz z rozwojem technologii informacyjnych i czasem ich użytkowania, systemy informatyczne wymagają ciągłego usprawniania zabezpieczeń – i ta konieczność systematycznego wzmacniania bezpieczeństwa infrastruktury informatycznej stanowi poważny problem.

2. Zagrożenia dla realizacji e-usług

Na ataki najbardziej narażone są systemy instytucji finansowych, serwisy aukcyjne, sklepy internetowe oraz agendy rządowe – wszystkie te jednostki, które przechowują i przetwarzają ważne dane (poufne, osobowe, wrażliwe). Komunikaty ostrzegawcze kierowane do użytkowników internetu słyszy się coraz częściej, a zakres i skala zagrożeń stale rośnie. Ukazują to liczne przykłady skutecznych ataków przeprowadzonych w ostatnim okresie.

W lutym 2015 roku informowano w prasie o rozbiciu przez Europejskie Centrum ds. Cyberprzestępczości przy Europolu siatki hakerów kontrolujących botnet Ramnit złożony z 3,2 mln zainfekowanych komputerów na całym świecie, które przestępcy mogli wykorzystywać do różnych bezprawnych działań. W przeprowadzonej operacji wzięły też udział znane firmy – AnubisNetworks, Microsoft i Symantec. W kolejnych miesiącach nadal odnotowywano aktywność botnetu. Jesienią 2015 roku przed atakami przestępców ostrzegała swoich abonentów firma Orange, świadcząca usługi telekomunikacyjne. Do jej klientów wysyłane były maile z powiadomieniami o niezapłaconych fakturach, zawierające odnośniki do szczegółowych informacji. Przejście pod wskazany adres skutkowało zainfekowaniem komputera szkodliwym oprogramowaniem (Czechowicz, 2015). Tego samego roku doszło do największego cyberataku, kiedy to włamano się do federalnej bazy danych amerykańskich urzędników (pracowników wojska, Agencji Bezpieczeństwa Narodowego i Departamentu Stanu), pobierając poufne dane ponad 21 mln osób (m.in. numery ubezpieczenia społecznego, dane dotyczące zdrowia, raporty z rozmów o pracę). Hakerzy podczas tego ataku przejęli też bazę z odciskami palców ponad 1 mln ludzi (Biznes, 2015).

W listopadzie 2016 roku zaatakowano internetową sieć Deutsche Telekom. Celem ataku były routery, w wyniku czego zawodziła ich identyfikacja przy próbie logowania. Problemy z korzystaniem z internetu, telefonów i telewizji kablowej miało wówczas 900 tys. osób, a skutki ataku były odczuwalne nawet w specjalnie chronionej sieci rządowej (Polsatnews, 2016).

[4] Informacja pomocnicza wykorzystywana w procesie szyfrowania.

Stale rośnie liczba ataków z wykorzystaniem internetu na konta bankowe. Jednym z najczęściej używanych do tego celu szkodliwych programów jest Trojan-Downloader.Win32.Upatre, umożliwiający kradzież danych dotyczących płatności. W 2016 roku informowano o ataku nowego wirusa na klientów polskich banków komercyjnych i spółdzielczych, który wcześniej atakował banki w USA i Kanadzie, skutkiem czego klienci ponieśli znaczne straty finansowe (infekcja następuje po otwarciu załącznika zawartego w mailu). Wirus ten ma zdolność dostosowywania się do systemu bankowego atakowanego użytkownika i umożliwia przejęcie pieniędzy z jego konta. Specjaliści ds. ochrony systemów bankowych odpierają dziesiątki (jeśli nie setki) ataków dziennie spodziewając się dalszego ich wzrostu (Przybysz, 2016). Te socjotechniczne ataki (tzw. *phishing*) należą do najczęstszych zagrożeń, a ich nasilenie przypada na przedświąteczny okres wzmożonej aktywności transakcji finansowych. Dla zdobycia cennych informacji cyberprzestępcy nierzadko infiltrują hotelowe sieci Wi-Fi w celu przejmowania danych gości hotelowych.

Pułapkę dla użytkowników internetu mogą stanowić usługi oferowane przez rzekomo darmowe serwisy (prowadzone np. dla potrzeb przedsiębiorstw), które z czasem wymagają uiszczenia wysokich opłat za udostępniane materiały, bez uprzedniego poinformowania o tym fakcie zainteresowanych. Przykładem zagrożenia może być też atak robaka (bardzo trudnego do usunięcia) na użytkowników portalu aukcyjnego eBay (2016 r.), w szczególności na stronach dotyczących motoryzacji. Na rynku pojawiają się także oferty usług hakerskich, np. w sieci działają serwisy zajmujące się blokowaniem na zlecenie aktywności stron WWW wskazanych firm. W 2016 roku właściciel jednego z nich został aresztowany pod zarzutem przestępstwa komputerowego (News, 2016).

Niezależnie od nieupoważnionego przejęcia danych na skutek włamania do systemu (tzw. wycieku) odbywa się nimi handel w świetle prawa. Dostawcy usług internetowych, operatorzy telefonii komórkowej oraz inne instytucje będące w posiadaniu danych o swoich klientach (np. banki czy serwisy samochodowe) przekazują te informacje firmom handlującym danymi osobowymi, co jest legalne[5] i praktykowane na całym świecie. Jako przykład można wskazać przypadek skopiowania w 2010 roku, a następnie odsprzedania (przez spółkę należącą do firmy reklamowej Nielsen) danych wrażliwych umieszczanych przez internautów na stronie WWW PatientsLikeMe (uruchomionej w 2004 r.) firmom z branży medycznej. Użytkownicy, najczęściej nieświadomie, sami wyrażają zgodę na przetwarzanie i przekazywanie swoich danych akceptując regulaminy portali, bez czytania ich treści[6]. Niekiedy, za wyrażenie takiej zgody, firmy proponują swoim klientom rabat przy zawieraniu umowy. Zgromadzone w sieci dane wykorzystują również, w różnych celach, organa państwowe. Jest wiele firm zaj-

[5] Wykorzystywanie zgromadzonych danych nie zawsze wymaga zgody zainteresowanego. By zastrzec sobie do nich prawo, należy złożyć stosowny wniosek w odpowiednim urzędzie.

[6] Zapoznanie się z regulaminem określającym politykę prywatności utrudnia forma jego sporządzenia (są to bardzo długie dokumenty pisane małą czcionką, z pojedynczą interlinią).

mujących się inwigilacją elektroniczną – wszystkie one gromadzą i analizują dane, a następnie odpowiednio je kategoryzują, tworząc różne profile użytkowników internetu. Najczęściej jest to sporządzane w celach marketingowych.

Zwykłym użytkownikom sieci trudno jest zachować prywatność. Wszystkie urządzenia są jednoznacznie identyfikowane poprzez adresy IP sieci komputerowej, z której realizowane jest połączenie z internetem, adresy MAC (*Media Access Control*) karty sieciowej oraz, w przypadku telefonów komórkowych, unikatowy numer identyfikacyjny używany przez sieć GSM, czyli IMEI (*International Mobile Equipment Identity*) lub numer identyfikujący kartę SIM, tzw. IMSI (*International Mobile Subscriber Identity*) – dzięki czemu łatwo jest śledzić ich aktywność.

Dla bezpieczeństwa, użytkownikom zaleca się regularne skanowanie komputerów oprogramowaniem antywirusowym, aktualizowanie użytkowanego oprogramowania, nieotwieranie załączników do e-maili od niezidentyfikowanych nadawców. Działania te, choć konieczne, nie rozwiązują jednak problemu.

3. Ataki na systemy przemysłowe, szpiegostwo i terroryzm

W dobie powszechnej cyfryzacji, ostrej konkurencji gospodarczej oraz coraz większego zagrożenia terrorystycznego – problem bezpieczeństwa sieci globalnej, wykorzystywanej we wszystkich dziedzinach życia, nabiera nowego znaczenia. Ataki stają się coraz bardziej wyrafinowane – do ich przeprowadzenia można użyć kradzionego certyfikatu, pojawiają się coraz bardziej zaawansowane szkodliwe kody o dużych możliwościach, jak np. Flame[7] czy Android.Titan.1.

Firmy komercyjne, organizacje i instytucje rządowe coraz częściej stają się ofiarami trudnych do wykrycia, bo niepozostawiających śladów ataków typu APT (*Advanced Persistent Threats*). O włamaniu większość z nich dowiaduje się dopiero po upublicznieniu przejętych danych lub w efekcie nieprawidłowego działania systemu. Ataki te są złożonymi, długotrwałymi działaniami o szerokim zasięgu. Ich celem mogą być firmy z branży przemysłowej, instytucje badawcze oferujące nowoczesne technologie, firmy energetyczne, koncerny samochodowe oraz instytucje ważne dla bezpieczeństwa lub obronności kraju. Ostatnio hakerzy zaczynają też dostrzegać, jako potencjalny cel ataku, mniejsze firmy (zwykle słabiej zabezpieczone), współpracujące z dużymi korporacjami, które również mogą być w posiadaniu cennych informacji.

Przestępcy dla przeprowadzenia ataku tworzą fałszywe profile i wirtualne tożsamości (pozyskując w ten sposób zaufanie pracowników atakowanej organizacji), wykorzystują pocztę elektroniczną i portale społecznościowe (Chip, 2013). Atakujący, trudni do zidentyfikowania, często prowadzą pracę wywiadowczą na zlecenie rządów. Cyberszpiegostwo będzie się rozwijać, bowiem ataki typu APT stanowią skuteczne narzę-

[7] Modułowy program szpiegujący (o rozmiarze ok. 20 MB), mający wiele wspólnego z Stuxnetem i Duqu, ale bardziej od nich zaawansowany.

dzie infiltracji systemów obrony, przy jednoczesnym małym ryzyku ujawnienia źródła. Eksperci przewidują, że w najbliższej przyszłości zmienią one formę i będą jeszcze lepiej maskowane, a tym samym groźniejsze (Kurek, 2016).

Można włamywać się do systemów informatycznych nadzorujących przebieg procesów technologicznych lub produkcyjnych, skutecznie atakować systemy zarządzania lotem, serwery łączności satelitarnej i systemy używane w kolejnictwie. Zakłócenia w pracy systemów przemysłowych mogą sparaliżować działalność przedsiębiorstwa i powodować wielomilionowe straty finansowe. Możliwość atakowania systemów energetycznych oznacza zagrożenie dla całej infrastruktury przemysłowej (Mendyk-Krajewska, 2011). Jednym z przykładów skutecznego działania cyberprzestępców jest atak na korporacje petrochemiczne (Exxon, Shell, BP), dokonany w 2009 roku, kiedy to z wykorzystaniem wirusa Night Dragon[8] uzyskano dostęp do systemów kontrolujących najistotniejsze procesy (Conowego, 2015). Ogromne straty finansowe oraz uszkodzenie infrastruktury były efektem ataku na niemiecką hutę stali w 2014 roku. Dostęp do wewnętrznej sieci przemysłowej hakerzy uzyskali w wyniku zabiegów socjotechnicznych. W tym samym roku odkryto, że wiele plików instalacyjnych oprogramowania przeznaczonego dla systemów SCADA (*Supervisory Control And Data Acquisition*)[9] zostało zmodyfikowanych (zawierają szkodliwy kod Havex), co umożliwia szpiegostwo przemysłowe, a nawet zdalne przejęcie kontroli nad systemem (Gołębiowski, 2015).

W połowie 2015 roku ukazała się informacja o ataku hakerów na włoską firmę Hacking Team, zajmującą się tworzeniem i sprzedażą specjalistycznego oprogramowania szpiegowskiego wykorzystywanego w wielu krajach (m.in. przez Arabię Saudyjską, Azerbejdżan, Kazachstan, Uzbekistan i Sudan), także przez służby specjalne (w tym polskie Centralne Biuro Antykorupcyjne) (Halicki, 2015). Włamywacze upublicznili m.in. wiadomości e-mail zaatakowanej firmy, zawarte umowy, listę jej klientów oraz kod źródłowy dystrybuowanego oprogramowania Remote Control System (znanego pod nazwami DaVinci i Galileo) służącego do śledzenia działalności użytkowników urządzeń mobilnych wyposażonych w platformy systemowe Android, iOS, Windows Mobile i BlackBerry. To oprogramowanie umożliwia m.in. nasłuchiwanie dźwięków otoczenia urządzenia (dzięki włączeniu mikrofonu), podglądanie otoczenia z użyciem wbudowanej kamery, monitorowanie wiadomości SMS i e-mail, pobranie listy kontaktów i historii połączeń, wykonanie zrzutów ekranu oraz odczyt pozycji GPS urządzenia.

Przestępcza działalność w sieci podejmowana jest nie tylko dla korzyści finansowych lecz również z pobudek ideologicznych. Liczne przykłady skutecznych operacji wskazują na biegłe posługiwanie się terrorystów nowoczesnymi technologiami. Organizacje terrorystyczne gromadzą dane z internetowych źródeł (np. serwisów społeczno-

[8] Dystrybuowany przez e-maile za pomocą metody *spear phishing*.

[9] Systemy SCADA są stosowane w wielu gałęziach przemysłu do monitorowania różnych procesów; ataki na te systemy mogą prowadzić m.in. do uszkodzeń instalacji przemysłowych.

ściowych), korzystają z programów do rozpoznawania twarzy, posługują się nawigacją GPS w telefonach.

4. Nowe zagrożenia dla nowych zastosowań rozwiązań informatycznych

Nowe technologie z robotyki, sztucznej inteligencji, genetyki, nanotechnologii i wielu innych dziedzin mają ogromny wpływ na kształtowanie rzeczywistości. Jednocześnie te same technologie są intensywnie wykorzystywane w działalności przestępczej i terrorystycznej. Od wielu lat technologie informacyjne dostarczają przestępcom nowych możliwości działania, a ataki cybernetyczne o katastrofalnych skutkach mogą być potraktowane na równi z militarnymi.

Od kilku lat udostępnia się na pokładzie samolotów pasażerskich internetowe połączenie Wi-Fi. Pierwszymi liniami lotniczymi, które się na to zdecydowały, były amerykańskie linie Virgin America. W dobie eskalacji zagrożeń sieciowych i wzrostu światowego terroryzmu, eksperci ponownie zwracają uwagę, że stanowi to potencjalną możliwość przejęcia kontroli nad maszynami. Wprawdzie stosowane zabezpieczenia są systematycznie weryfikowane, jednak żadnemu oprogramowaniu nie można zagwarantować pełnego bezpieczeństwa. Amerykańskie Biuro Rozliczeń Rządu (GAO – *Government Accountability Office*) ostrzega, że elektronika kokpitu połączona z kabiną pasażerską poprzez współdzieloną sieć z wykorzystaniem zapory sieciowej nie jest dostatecznie chroniona przed atakami hakerów (Bankier, 2015). Tymczasem linie American Airlines w 2016 roku zapowiedziały znaczne usprawnienie dostępności internetu poprzez Wi-Fi na pokładach swoich samolotów (szybsze modemy firmy ViaSat, większa prędkość transmisji) (Farooqui, 2016).

Jesienią 2015 roku Europejska Agencja Bezpieczeństwa Lotniczego (AESE) poinformowała o możliwości dokonania cyberataku na samolot poprzez system ACARS (*Aircraft Communications Addressing and Reporting System*) wykorzystywany do przesyłania komunikatów między samolotem a stacjami naziemnymi. Wykryta już w 2013 roku luka w tym systemie polega na możliwości wstawienia dowolnego pakietu (np. fałszywego komunikatu) do przesyłanego strumienia danych, z powodu braku kontroli liczby transmitowanych pakietów. Podkreśla się przestarzałość całego wykorzystywanego od lat 70. XX wieku systemu, projektowanego bez uwzględnienia zagrożeń elektronicznych (Technowinki, 2015).

W czerwcu 2015 roku na warszawskim lotnisku im. F. Chopina awarii uległ komputerowy system wystawiający dokumenty konieczne do odbycia lotu (tzw. plany lotu). W efekcie tego ataku DoS na naziemne systemy IT odwołano wiele lotów krajowych i zagranicznych, a inne europejskie rejsy miały znaczne opóźnienia (Warszawa, 2015). Jest to jeden z ostatnich przykładów skutecznego atakowania systemów teleinformatycznych wykorzystywanych w lotnictwie. Już w 2004 roku odnotowano ataki na systemy kontrolne linii lotniczych British Airways i Delta Airlines (z użyciem robaka Sas-

ser, który wykorzystywał błąd przepełnienia bufora), a skutkiem przeciążenia systemów było wielogodzinne wstrzymanie pracy lotnisk i anulowanie części lotów.

Podatne na ataki są wszystkie urządzenia wyposażone w systemy komputerowe (np. samochody czy nowoczesne karabiny), a także sprzęt podłączony do internetu (np. telewizory). Przejęcie nad nimi kontroli może prowadzić do bardzo poważnych skutków, zatem coraz bardziej popularyzowany internet rzeczy IoT (*Internet of Things*) wydaje się być niebezpieczny dla społeczeństwa (Miller, 2015). Niestety, problem dostrzegają jedynie specjaliści, podkreślając trudną wykrywalność przestępców w przypadku ataku. Wiele inteligentnych urządzeń domowych z kategorii IoT połączonych z siecią (takich jak ekspres do kawy czy kamera IP monitorująca dziecko) zawiera luki w systemie zabezpieczeń, a sterowany smartfonem domowy system alarmowy można oszukać (co zostało udowodnione) przy użyciu zwykłego magnesu. Biorąc pod uwagę, iż urządzenia oparte na czujnikach pola magnetycznego są wykorzystywane przez wiele rozwiązań alarmowych – problem dotyczy dużej grupy użytkowników. By bezpiecznie korzystać z najnowszych technologii, trzeba mieć odpowiednią wiedzę na temat potencjalnych zagrożeń, jednak nie jest to dostatecznie podkreślane.

Według ekspertów przestępcy sieciowi działają jak zorganizowana korporacja. Potrafią na przykład spowodować i wykorzystać wahania cen akcji na giełdzie papierów wartościowych dla uzyskania korzyści finansowych. Przykładem jest efekt skutecznego ataku na twitterowe konto amerykańskiej agencji prasowej Associated Press w 2013 roku. Umieszczona tam nieprawdziwa informacja o problemach zdrowotnych prezydenta USA wywołała reakcję nowojorskiej giełdy, co przestępcy wykorzystali do zakupu akcji po chwilowym spadku kursu, by następnie je sprzedać z dużym zyskiem (Cyberprzestępcy, 2015).

Specjaliści ds. bezpieczeństwa analizujący trendy w przestępczości elektronicznej przewidują wzrost ataków na systemy płatnicze i działań blokujących realizację usług, a także rozwój szkodliwego oprogramowania dla procesorów i kart graficznych. Wskazuje się też na nowe zagrożenia: tworzenie jednorazowych narzędzi ataku, ulotne infekcje (szkodliwe kody rezydują w pamięci operacyjnej do czasu ponownego uruchomienia komputera) oraz nasilenie się ataków na systemy rządowe, co wynika z rosnącego napięcia geopolitycznego.

Podsumowanie

Rozwój i upowszechnianie ICT, intensywnie dokonywane w ostatnich latach, wymusza realizację coraz większej liczby usług drogą elektroniczną.

W Ministerstwie Cyfryzacji powstaje kolejny projekt realizowany we współpracy z MSWiA – mDokumenty, w ramach którego najważniejsze dokumenty (tj. dowód osobisty, prawo jazdy, dowód rejestracyjny pojazdu i polisa ubezpieczeniowa OC) będą mogły być przechowywane w pamięci smartfonów lub telefonów komórkowych. Wprowadzenie cyfrowej formy wszystkich tych dokumentów przewiduje się na drugą

połowę 2017 roku. Obserwowana intensyfikacja zagrożeń w pełni uzasadnia obawy o ich bezpieczeństwo. Na razie nowa forma ma być opcjonalna – nie wiemy jednak jak długo.

Wdrażanie projektów IT w różnych obszarach życia publicznego nie może odbywać się bez dostrzegania problemu bezpieczeństwa. Wobec możliwości eskalacji przestępczości elektronicznej, ciągłe podwyższanie standardów ochrony oraz ograniczone zaufanie do użytkowanych technologii informacyjnych staje się koniecznością. W dzisiejszych czasach systemy teleinformatyczne są wprawdzie coraz lepiej chronione, na rynku dostępnych jest wiele rozwiązań łączących najnowsze techniki zabezpieczeń, rośnie też wiedza na temat problemu bezpieczeństwa – niestety, zagrożenie wcale nie maleje.

Bibliografia

Bankier (2015). Pobrano z: bankier.pl/wiadomosc/GAO-internet-na-pokladach-samolotow-moze-stanowic-zagrozenie-3323984.html (10.05.2016).

Biznes (2015). Pobrano z: www.biznes.onet.pl/wiadomosci/swiat/21-5-mln-sosb-ofiarami-hakerskiego-ataku-na-rzadowe-komputery/3sdr04 (10.09.2016).

Chip (2013). Pobrano z: www.chip.pl/news/bezpieczenstwo/luki-bezpieczenstwa/2013/03/ cyber-ataki-typu-apt-nowym-frontem-wojny (3.01.2017).

Conowego (2015). Pobrano z: www.conowego.pl/aktualnosci/anatomia-atakow-scada-czyli-o-wlamaniach-do-systemow-przemyslowych-13822 (5.01.2017).

Cyberprzestępcy (2015). Pobrano z: komputerswiat.pl/sekcje-specjalne/klikaj-bezpiecznie/ zagrozenia/cyberprzestepcy-sa-grozni-jak-nigdy-dowiedz-sie-jak-dzialaja.aspx (2.02.2016).

Czechowicz, B. (2015). *Cyberprzestępcy polują na klientów Orange*. Pobrano z: pclab.pl/ news66135.html (20.09.2016).

Farooqui, A. (2016). *American Airlines Bringing Faster Wi-Fi To Planes*. Pobrano z: ubergizmo.com/2016/11american-airlines-bringing-faster-wi-fi-to-planes (10.11.2016).

Gołębiowski, Ł. (2015). *8 najgroźniejszych ataków hakerskich na obiekty przemysłowe*. Pobrano z: komputerswiat.pl/sekcje-specjalne/klikaj-bezpiecznie/ataki-hakerow/8-najgroz niejszych-atakow-hakerskich-na-obiekty-przemyslowe.aspx (5.12.2016).

Halicki, P. (2015). *Atak hakerów na firmę dostarczającą oprogramowanie dla CBA. Jest reakcja Biura*. Pobrano z: wiadomosci.onet.pl/warszawa/atak-hakerow-na-firme-dostarczajaca-oprogramowanie-dla-cba-jest-reakcja-biura/v5hz2k (17.10. 2016).

Kurek, A. (2016). *Ataki typu APT staną się znacznie groźniejsze*. Pobrano z: cyberdefence24.pl /343109,ataki-typu-apt-stana-sie-znacznie-grozniejsze (3.01.2017).

Mendyk-Krajewska, T. (2011). Podatność na ataki sieci przemysłowych. W: *Projektowanie, analiza i implementacja systemów czasu rzeczywistego* (s. 247–258). Warszawa: WKŁ.

Miller, M. (2015). *The Internet of Things: How Smart TVs, Smart Cars, Smart homes, and Smart Cities are Changing the Word*. Pearson Education.

News (2016). Pobrano z: News.softpedia.com/news/teen-behind-titanium-ddos-stresser-pleads-guilty-in-london-509811.shtml (10.12.2016).

Polsatnews (2016). Pobrano z: www.polsatnews.pl/wiadomosc/2016-11-28/hakerzy-staja-za-awaria-sieci-internetowej-deutsche-telekom (30.11.2016).

Polskacyfrowa (2016). Pobrano z: www.polskacyfrowa.gov.pl (15.12.2016).

Przybysz, A. (2016). *Nowy wirus atakuje polskie banki. Polska obiektem zainteresowania cyber-przestępców*. Pobrano z: wyborcza.biz/biznes/1,147883,19975377,nowy -wirus-atakuje-polskie-banki-polska-obiektem-zainteresowania.html?disable Redirects=true (15.11.2016).

Technowinki (2015). Pobrano z: technowinki.onet.pl/oprogramowanie/samoloty-pasazerskie-mogą-byc-zaatakowane-przez-system-acars/ms88hq (22.10.2016).

Verizon (2016). Pobrano z: www.verizonenterprise.com/resources/reports/rp_216-DBIR-Financial-Data-Security_en_xg.pdf (5.01.2017).

Warszawa (2015). Pobrano z: Warszawa.onet.pl/awaria-komputerow-lot-odwolana-czesc-lotow/y05lkb.amp (15.11.2016).

NEW INFORMATION TECHNOLOGIES AND THE DEVELOPMENT OF E-CRIME

Keywords: security of e-services, network attacks, Internet of Things

Summary. The information technologies commonly used in almost all areas of life are not risk-free. Alongside their development and the expansion of the range of network services, there are new possibilities of abuse and e-criminal activity. The means of attack can be any device connected to the network. Software companies, aware of the real threats, equip their products in increasingly complex security mechanisms, but the scale of the phenomenon is not decreasing, and nothing indicates that a significant improvement of network security can be achieved in the near future. The complex problem of cyber-crime has gained in importance in recent years, considering the intensification of digital development of our country.

Translated by Zygmunt Mazur

Cytowanie

Mendyk-Krajewska, T., Mazur, Z., Mazur, H. (2017). Nowe technologie informacyjne a rozwój przestępczości elektronicznej. Ekonomiczne Problemy Usług, *1* (126/2), 219–229. DOI: 10.18276/epu.2017.126/2-22