Teresa Mendyk-Krajewska, Zygmunt Mazur, Hanna Mazur

Intensyfikacja przestępczości w e-gospodarce

Ekonomiczne Problemy Usług nr 117, 707-716

2015

ZESZYTY NAUKOWE UNIWERSYTETU SZCZECIŃSKIEGO
NR 852 EKONOMICZNE PROBLEMY USŁUG NR 117 2015

TERESA MENDYK-KRAJEWSKA, ZYGMUNT MAZUR, HANNA MAZUR
Politechnika Wrocławska[1]

INTENSYFIKACJA PRZESTĘPCZOŚCI W E-GOSPODARCE

Streszczenie

Polska gospodarka elektroniczna wykorzystując technologie informatyczne, rozwija się bardzo intensywnie. Przekazywanie informacji w celach biznesowych, w administracji publicznej, podczas realizacji e-usług odbywa się z użyciem systemów teleinformatycznych, a procesy decyzyjne w przedsiębiorstwach są wspomagane przez rozbudowane narzędzia analityczne. Niestety, nowoczesne technologie niosą pewne ryzyko bezpiecznego ich użytkowania, i to mimo stosowania różnych metod i środków ochrony. Celem artykułu jest przedstawienie skali zagrożenia bezpieczeństwa sieciowego w dobie rozwoju e-gospodarki oraz ukazanie możliwości i skutków atakowania sieci firmowych i przemysłowych.
Słowa kluczowe: e-gospodarka, zagrożenia systemów informatycznych, cele ataków.

Wprowadzenie

Dynamikę informatyzacji kraju można obserwować od początku XXI wieku. Rozwój handlu elektronicznego w Polsce przypada na lata 90. XX w., a wprowadzenie usług realizowanych drogą elektroniczną do administracji publicznej obserwuje się od roku 2000, w którym to opracowano materiały znane dziś jako dokument Komitetu Badań Naukowych i Ministerstwa Łączności pt. *Cele i kierunki rozwoju społeczeństwa informacyjnego w Polsce*. W kolejnych latach uchwalano stosowne ustawy i wprowadzano dokumenty (wzorowane na opracowaniach europejskich) niezbędne dla planowanego rozwoju. W ramach prowadzonych prac

[1] Wydział Informatyki i Zarządzania, Katedra Informatyki.

w tym zakresie powstał m.in. dokument *Strategia Informatyzacji Rzeczypospolitej Polskiej – ePolska na lata 2004–2006*.

Wykorzystywane technologie informacyjno-komunikacyjne mają duży wpływ na działania i efektywność wielu sektorów gospodarki. Rozwój e-gospodarki, e-usług i e-administracji przynosi efekty ekonomiczne, prowadzi do oszczędności czasu, wzrostu jakości i zwiększenia przejrzystości realizowanych procedur, zwiększa możliwości kontaktów oraz dostępność informacji. Lista usług realizowanych drogą elektroniczną jest stale poszerzana. Dzięki dostępnym systemom można przez Internet znaleźć zatrudnienie, rozliczyć podatek, złożyć wniosek o wydanie dowodu osobistego, prawa jazdy czy paszportu, zarejestrować pojazd, uzyskać pozwolenie na budowę, dokonać zmiany zameldowania, kupić bilet, zarejestrować się na wizytę u lekarza czy przeglądać katalogi bibliotek publicznych. Z badań Polskiej Agencji Rozwoju Przedsiębiorczości dotyczących działalności małych i średnich firm w latach 2011–2012 wynika, że w Polsce 16% z nich posługuje się fakturami elektronicznymi (dla porównania – w UE 30%), 25% wysyła/odbiera zamówienia drogą elektroniczna (w UE 28%), 16% kupuje, a 9% sprzedaje towary za pośrednictwem Internetu (w UE odpowiednio 16% i 14%) (*Raport…* 2013).

Korzyści z cyfryzacji gospodarki i administracji są niekwestionowane, jednak pojawia się problem zapewnienia systemom należytego bezpieczeństwa. Rozwój e-usług związanych z handlem i finansami sprawił, że systemy informatyczne wykorzystywane są do przesyłania i przechowywania poufnych danych. Ich ochrona ma istotne znaczenie nie tylko dla biznesu, ale także dla władz (wiele szkodliwych działań ma podłoże polityczne). Skala zagrożenia bezpieczeństwa rośnie, co stanowi wyzwanie dla firm tworzących oprogramowanie oraz dla administratorów systemów.

1. Problem bezpieczeństwa systemów teleinformatycznych

Systemy teleinformatyczne nie mogą być traktowane jako całkowicie bezpieczne, gdyż ryzyko zagrożenia stale istnieje – nawet wówczas, gdy użytkowane oprogramowanie jest właściwie skonfigurowane i systematycznie aktualizowane, a systemy zabezpieczeń odpowiednio dobrane. Jest wiele tego przyczyn, wśród nich przede wszystkim błędy w oprogramowaniu (w szczególności w przeglądarkach internetowych oraz wykorzystywanych zewnętrznych wtyczkach[2]), dostępność narzędzi do przeprowadzenia ataku, szybki rozwój i różnorodność technik włamań oraz technologii szkodliwego oprogramowania, podatność na ataki dostępnych standardów ochrony. Szkodliwe kody przedostające się do systemu głównie przez luki w oprogramowaniu zwykle instalują się na twardym dysku, jednak bardziej

[2] Dodatkowe moduły do programów komputerowych rozszerzające możliwości wyjściowych produktów (tzw. pluginy).

zaawansowane, umożliwiające przejęcie kontroli nad systemem podczas aktywnego połączenia z Internetem, potrafią się ukryć w BIOS-ie[3], pozostając poza zasięgiem większości programów ochronnych.

Od wielu lat atakujący wykorzystują wady w programach napisanych w popularnych językach programowania, m.in. w podatnym na ataki języku Java, używanym do tworzenia aplikacji i programów sterujących. Podatność na ataki wykazują też języki tworzenia stron internetowych. Nowe zagrożenie wnosi np. kolejna wersja HTML5, pozwalająca na zwiększenie atrakcyjności stron WWW. Okazuje się, że programiści skupiając uwagę na rozwiązaniach multimedialnych, nierzadko zaniedbują stronę bezpieczeństwa.

Nieustanne rozwijanie technologii informatycznych sprawia, że równocześnie pojawiają się nowe zagrożenia. Ostatnie lata przyniosły duże zainteresowanie urządzeniami mobilnymi oraz możliwością przetwarzania danych w chmurze (*cloud computing*). Oba te rozwiązania, mimo niewątpliwych zalet, wprowadzają też nowe problemy. W 2010 roku odnotowano znaczący wzrost sprzedaży urządzeń mobilnych, z powodu poszerzenia zakresu ich funkcjonalności. Ich popularność (głównie smartfonów), możliwości wykorzystania do realizacji usług drogą elektroniczną oraz zadań i kontaktów biznesowych, spowodowała gwałtowny rozwój opracowanych na nie zagrożeń. W 2013 roku 14% ruchu internetowego pochodziło z urządzeń mobilnych, zaś według przewidywań analityków firmy Cisco w 2018 r. będą one stanowiły źródło większości generowanego ruchu sieciowego (Jaślan 2014). Głównym celem ataków jest platforma Android firmy Google, z powodu otwartości kodu, możliwości pobierania plików z różnych źródeł i łatwości modyfikacji aplikacji. Coraz więcej smartfonów wykorzystuje technologię NFC[4] do realizacji płatności, można więc oczekiwać ataków na używane przy tym aplikacje. Dostępne tagi NFC umożliwiają samodzielne ich programowanie z poziomu telefonu i wykorzystywanie np. do przekazywania danych. Firma Apple dostarcza własne rozwiązanie – system iBeacons oparty na technologii Bluetooth.

Z powodu wielu zalet *cloud computing* z usługi tej korzysta zarówno wielki biznes, jak i małe oraz średnie przedsiębiorstwa. Organizacje mają możliwość zdalnego wykorzystania środowiska informatycznego do przetwarzania danych, zgodnie ze swoimi potrzebami. Dostępność nowoczesnych zasobów IT o dostosowanej funkcjonalności pozwala im osiągać wysoki poziom wydajności przy ograniczeniu kosztów oraz unikać kłopotów związanych z administrowaniem systemu. Chmury obliczeniowe udostępniane za pomocą serwisów internetowych, takich jak np.

[3] *Basic Input/Output System* – system do obsługi we/wy komputera, pośredniczący pomiędzy sprzętem a systemem operacyjnym, ładowany przed jego uruchomieniem.

[4] *Near Field Communication* – radiowy standard komunikacji o krótkim zasięgu (do 20 cm) bezprzewodowej wymiany danych; odbiór i nadawanie w tym samym czasie.

AmazonElastic Computer Cloud (Amazon EC2)[5], są wygodnym rozwiązaniem dla realizacji zadań wymagających dużej mocy obliczeniowej.

Model przetwarzania danych oparty na użytkowaniu usług dostarczanych przez zewnętrzną organizację niesie jednak wiele zagrożeń. Powierzenie zasobów firmy innemu podmiotowi (dostawcy usług) opiera się w dużej mierze na zaufaniu, co jednak nie daje żadnej gwarancji bezpiecznego nimi zarządzania.

Usługi w chmurze umożliwiają też np. szybkie łamanie złożonych haseł dostępowych, a operatorzy mają ograniczone możliwości zapobiegania takim nadużyciom, bowiem przetwarzane dane nie są analizowane. Rozwój koncepcji usług w chmurze wymaga zatem odpowiednich przepisów prawnych oraz jednolitych standardów dla ochrony danych i bezpiecznego ich przetwarzania.

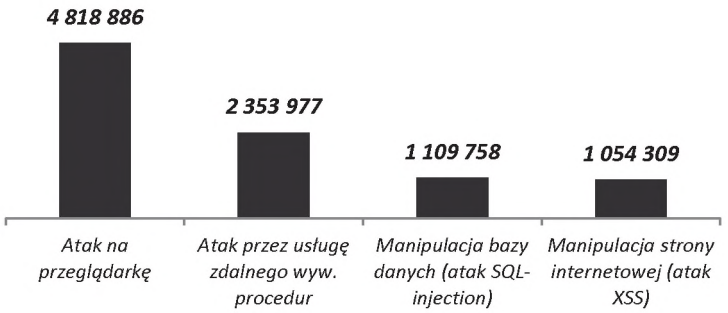
Na zagrożenia narażone są przede wszystkim duże korporacje, banki, firmy zajmujące się e-handlem elektronicznym i instytucje rządowe. Celem ataku na system teleinformatyczny może być uzyskanie informacji gospodarczych czy wojskowych, przechwycenie poufnych danych, destabilizacja pracy systemu lub przejęcie nad nim kontroli (np. dla wykorzystania systemu do innych bezprawnych działań, jak wysyłanie spamu czy dystrybucja nielegalnych treści). W wyniku ataku może dojść do wyłudzenia nazw i haseł dostępowych do kont bankowych, przechwycenia kodów do autoryzacji przekazów pieniężnych, zdobycia dostępu do tajemnic rządowych czy firmowych lub utraty wiarygodności organizacji.

2. Przykłady zagrożeń w sieciach komputerowych

Najczęściej motywem działań przestępców jest chęć osiągnięcia korzyści finansowych, ale nie należy lekceważyć możliwości podejmowania działań szpiegowskich (problem dotyczy firm i administracji rządowej) lub przeprowadzenia ataku terrorystycznego. Straty powodowane przestępczością internetową sięgają milionów dolarów – np. w Australii, gdzie celem ataków były linie lotnicze, sieci hoteli oraz firmy z sektora usług finansowych, straty oszacowano na 100 mln $ (pcworld.pl 2014). Według analiz firmy McAfee w trzecim kwartale 2013 r. ataki na komputery PC były głównie poprzez przeglądarki internetowe oraz przez usługę zdalnego wywoływania procedur Windows. Popularne typy ataków przedstawiono na rysunku 1.

Spośród wielu narzędzi wykorzystywanych do atakowania systemów bankowych i płatności online można wymienić np. konie trojańskie Citadel i Zeus p2p (dzięki którym można rejestrować aktywność komputerową użytkowników, zmienić wygląd wyświetlanych stron internetowych, przejąć kontrolę nad komputerem), lub URLZone atakujący konta z wykorzystaniem luk w zabezpieczeniach przeglądarek.

[5] Amerykańskie przedsiębiorstwo zajmujące się handlem elektronicznym, mające oddziały w wielu krajach, m.in. w Polsce; prowadzi największy na świecie sklep internetowy.



Rys. 1. Metody atakowania systemów komputerowych w III kw. 2013 r.

Źródło: opracowanie własne na podstawie (komputerswiat.pl 2014).

W 2013 r. w ciągu 3 tygodni zidentyfikowano ponad 164 tys. komputerów zaatakowanych przez Citadel w 75 krajach (www.tvn24.pl 2014). Według danych z września 2014 r. z e-bankowości korzysta już prawie 13 mln Polaków (biznes.onet.pl). W celu podniesienia poziomu bezpieczeństwa świadczonych usług banki umieszczają informacje na temat wykrywanych zagrożeń i sposobów zabezpieczeń.

Przykładem zaawansowanego kodu jest Trojan.PWS.Papras.4, którego działanie umożliwia kradzież haseł i danych wprowadzanych przez użytkownika do formularzy internetowych, zdalną kontrolę nad sprzętem czy wbudowanie obcych treści w przeglądane strony WWW. Każdą funkcję realizuje inny moduł, np. Backconnect pozwala zarządzać komputerem nawet przy włączonej zaporze sieciowej. Do zainfekowania urządzenia może dojść podczas korzystania z aplikacji sieciowych lub portali wymagających uzupełnienia formularza danymi osobowymi.

Innym przykładem złożonego wirusa jest zidentyfikowany w 2012 roku Flame (rozmiar 50 MB!), który pobiera zrzuty ekranu z poczty użytkownika oraz dzięki funkcji włączania mikrofonu urządzenia przesyła nagrania podsłuchanych rozmów.

Według danych firmy Kaspersky Lab ataki na użytkowników internetowych kont bankowych, klientów sklepów i instytucji finansowych stanowią już 42% otrzymywanych fałszywych e-maili (rok wcześniej było to ok. 33%) (biznes.onet.pl). W kwietniu 2014 r. firmy Kaspersky Lab i B2B International przeprowadziły w 27 krajach badania dotyczące zabezpieczeń kontaktów pomiędzy firmami finansowymi i ich klientami – aż 30% takich firm nie zapewnia bezpieczeństwa (także przy połączeniu bezprzewodowym) transakcji online po stronie klienta, nie widzi w tym problemu i nie zamierza wprowadzić żadnych mechanizmów ochrony (Kurzak 2014).

Przykładem zagrożenia dla urządzeń mobilnych jest robak AndroRAT[6], który umożliwia lokalizację, zdalną obsługę (np. wykonywanie połączeń) i podsłuch, śledzenie wiadomości SMS i kamery. Specjaliści z Fortiguard Labs firmy Fortinet[7] umieścili w Internecie demonstrację symulacji jego działania i skutki ataku (www.fortinet.pl 2014).

Nowe rodzaje zagrożeń niesie wirtualna waluta cyfrowa BitCoin wprowadzona w 2009 r. (obecnie w obiegu jest ok. 11 mln bitmonet; http://finanse.wp.pl 2014). Wzrost wartości bitcoinów może prowadzić do nieuczciwego ich generowania, nasilają się ataki dla pozyskania haseł i kluczy do tzw. portfela bitcoinowego. Względna anonimowość tej waluty przyczyniła się do aktywacji nielegalnych transakcji, umożliwiając ukrywanie przepływu pieniędzy, co utrudnia powołanym służbom identyfikację internetowych przestępstw. Sam fakt, że wartość tej waluty obliczana jest komputerowo, czyni ten proces podatnym na ataki. W kwietniu 2013 r. użytkownicy komunikatora Skype poprzez określony odsyłacz instalowali na komputerze generator bitcoinów (http://technowinki.onet.pl). W 2014 r. jedną z największych platform wymiany bitcoinów MtGox odłączono od Internetu z powodu problemów technicznych (http://finanse.wp.pl 2014).

Nowe zagrożenie stwarza podłączanie do sieci konsumenckich urządzeń elektronicznych, np. telewizorów z funkcją Smart. Odbiorniki te umożliwiają uruchamianie specjalnych aplikacji, korzystanie z Internetu, z serwisów społecznościowych i komunikatora Skype oraz odbieranie powiadomień o listach przesłanych na konto pocztowe. Przy braku odpowiednich zabezpieczeń istnieje możliwość zdalnego zarządzania telewizorem (np. podmiany pobieranej strony WWW, a tym samym wyświetlania fałszywych informacji). Różne zagrożenia dotyczą też innych urządzeń domowych podłączonych do sieci globalnej.

Skutki nieuprawnionej ingerencji w system teleinformatyczny nie zawsze są od razu widoczne, a straty niełatwo jest oszacować. Ponadto firmy i banki, z obawy o utratę prestiżu, niechętnie informują o dokonanym na ich systemy ataku. Eksperci są zgodni, że skala zjawiska zagrożenia bezpieczeństwa sieciowego niepokojąco rośnie, wzrasta też profesjonalizm działań grup przestępczych.

3. Zagrożenie bezpieczeństwa systemów przemysłowych

Problem odpowiedniego poziomu bezpieczeństwa dotyczy także sieci przemysłowych wykorzystujących oprogramowanie SCADA (*Supervisory Control And*

---

[6] RAT – *Remote Administration Tool* – narzędzie zdalnego administrowania.

[7] W 2013 r. firma wykrywała dziennie ponad 1300 szkodliwych aplikacji (www.fortinet.pl 2014).

Data Acquisition)[8] nadzorujące przebiegi procesów technologicznych i produkcyjnych. Było ono projektowane dla wyizolowanych sieci sterujących (np. ruchem kolejowym, samolotowym, procesami przemysłowymi w fabrykach, elektrowniach czy w zakładach chemicznych), gdzie penetracja systemu zakładowego była w zasadzie niemożliwa. Istnienie wad oprogramowania w systemach sieci przemysłowych nabrało znaczenia wraz ze zmianą charakteru tych sieci, na co wpłynęło wykorzystywanie aplikacji komercyjnych i powszechnie stosowanych kanałów komunikacji oraz podłączanie komputerów zakładowych do sieci globalnej. Jedną z przyczyn wzrostu zagrożenia jest stosowanie połączeń bezprzewodowych i dostęp do zasobów firmy z urządzeń mobilnych. Ponadto w systemach SCADA często wykorzystywane są słabo zabezpieczone standardy komunikacji radiowej (technologia SDR[9]). Specjaliści ostrzegają przed możliwością wzrostu liczby ataków na połączenia radiowe wykorzystywane w infrastrukturze telekomunikacji.

W przypadku sieci przemysłowych skuteczny atak pociąga bardzo poważne skutki, prowadząc do przejęcia kontroli nad sterowanymi procesami. Konsekwencją może być wywołanie awarii, unieruchomienie lub zniszczenie obiektów gospodarczych i użyteczności publicznej (systemów energetycznych, sygnalizacji świetlnej, instalacji wodociągowych, systemów obsługujących transport itp.).

Pierwszym szkodliwym kodem, który na dużą skalę zaatakował systemy sterowania sieci przemysłowych, umożliwiając podsłuch i modyfikację parametrów pracy urządzeń, był program Stuxnet (Trojan-Dropper.Win32.Stuxnet, Rootkit.Win32.Stuxnet.a). Przy jego pomocy w 2010 r. dokonano ataku na irańskie sieci przemysłowe (w tym komputery elektrowni atomowej w Buszehr), zarażając 60% komputerów. Stuxnet, atakując systemy z oprogramowaniem WinCC, wyszukuje w sieci programowalny sterownik logiczny firmy Siemens, której urządzenia są stosowane w zakładach przemysłowych na całym świecie, m.in. w elektrowniach, rafineriach ropy naftowej, oczyszczalniach ścieków i zakładach nuklearnych. Zagrożeniem dla instalacji przemysłowych jest też robak Duqu, który wykorzystuje lukę w jądrze systemu Windows (dociera do systemu dzięki spreparowanemu plikowi Worda i zbiera dane potrzebne do ataku) (http://magazynt3.pl). Celem działań przestępczych były koncerny chemiczne, naftowe i zbrojeniowe, firmy paliwowe i energetyczne (http://di.com.pl/news 2011). Potwierdzono też możliwość wyłączenia, a nawet uszkodzenia turbin wiatrakowych oraz przejęcia kontroli nad publiczną siecią wodociągów.

Eksperci od bezpieczeństwa komputerowego ostrzegają też przed możliwością ukrycia szkodliwych obwodów w mikroczipach. Takie zagrożenie znacznie trudniej

---

[8] Rozproszony system elementów wykonawczych i monitorujących, połączonych z centrami dyspozycyjnymi przez rozległe sieci telekomunikacyjne.

[9] *Software Defined Radio* – system komunikacji radiowej, w którym działanie elementów elektronicznych jest sterowane przy pomocy programu komputerowego; rozwiązanie jest użyteczne i coraz częściej wykorzystywane w szybko rozwijających się systemach.

identyfikować, a konsekwencje mogą być bardzo poważne. Na tego typu atak podatne jest każde urządzenie z wbudowanym mikroprocesorem. Układy scalone, składające się ze zbioru bloków funkcjonalnych, realizujących różne zadania, znajdują się w systemach komunikacji, sieciach energetycznych, w systemach sterujących znajdujących się np. w samolotach czy samochodach. Wykorzystywane są też do kontroli dostępu do kont bankowych. Szkodliwy obwód można ukryć w sprzęcie komputerowym, a atak wywołać w dowolnym czasie, pod wpływem określonego bodźca. W wyniku ataku układ może przestać poprawnie działać, lub np. przekazywać poufne dane. Eksperci nie mają wątpliwości, że takie zagrożenie, którego skutki mogą być katastrofalne, jest całkiem realne. Problem ten dotyczy także wyposażonych w elementy elektroniczne urządzeń medycznych, takich jak rozruszniki serca czy automatyczne pompy insulinowe. Podsystemy takich urządzeń nie są bowiem w żaden sposób zabezpieczane, podczas gdy ich parametryzowanie i odczyt działania odbywają się bezprzewodowo, co stwarza możliwości zakłócenia prawidłowej pracy (http://technowinki.onet.pl 2014).

Istotną kwestią dostrzeganą ostatnio jest potrzeba ochrony oprogramowania wbudowanego (*firmware*), traktowanego dotąd jako bezpieczne. Projektowane jest ono tak, by przez długi czas działało niezmiennie, jednak wykorzystywane obwody pozwalają na wielokrotny zapis, zatem istnieje możliwość jego modyfikacji.

4. Problem bezpieczeństwa sieci energetycznych

Najbardziej strategiczny cel może stanowić inteligentna sieć elektroenergetyczna (Smart Grid), łącząca elektrownie, instalacje do przesyłania i magazynowania energii oraz jej odbiorców, w której elektroniczne liczniki prądu przesyłają do dostawcy informację o jego zużyciu. Zagrożenie w szczególności dotyczy urządzeń I i II generacji wykorzystywanych na dużą skalę w niektórych krajach europejskich, bowiem były one projektowane bez uwzględnienia potrzeby bezpieczeństwa. Problem odnosi się również do inteligentnych sieci energetycznych integrujących małe alternatywne źródła energii, takie jak panele słoneczne, turbiny wiatrowe czy niewielkie elektrownie wodne, które w celu wzrostu wydajności i skutecznej kontroli są łączone z Internetem. Taka zaawansowana infrastruktura informatyczna umożliwia zdalne korelowanie produkcji energii z jej zużyciem, maksymalizowanie efektywności przepływu oraz eliminowanie przerw w dostarczaniu usług energetycznych. Niestety, używanie liczników energii elektrycznej posiadających adresy IP czyni je podatnymi na ataki DoS (polegające na blokadzie realizacji usługi) oraz modyfikację przesyłanych do operatora danych, skutkiem czego może być odcięcie odbiorcy dostawy prądu.

W 2011 r. odnotowano atak na japońską firmę Mitsubishi Heavy Industries, producenta urządzeń dla wojska oraz sektorów energetycznego i stoczniowego

(http://technowinki.onet.pl 2014). W 2014 r. firma Symantec upubliczniła wiadomość, iż monitoruje aktywność grupy szpiegowskiej Dragonfly (znanej też jako Energetic Bear) koncentrującej działalność na sektorze energetycznym, której prawdopodobnym celem jest szpiegostwo przemysłowe (www.symantec.com 2014). Obszarem jej działania jest głównie Ameryka Płn. i Europa (także Polska). Ocenia się, że Dragonfly dysponuje szerokimi zasobami i może stosować różne metody infiltracji organizacji z sektora energetycznego na całym świecie.

W wyniku ataku na sieci energetyczne mogą ucierpieć takie obszary gospodarki, jak transport, telekomunikacja, produkcja żywności czy opieka medyczna. Według przewidywań ekspertów ryzyko awarii zasilania będzie rosło.

Podsumowanie

Wykorzystanie systemów teleinformatycznych w gospodarce determinuje dynamikę jej rozwoju, i to pomimo wielu realnych zagrożeń. Aby ich użytkowanie było bezpieczne, systemy ochrony muszą nadążać za rozwojem technologii informacyjno-komunikacyjnych, stanowiąc ich ważny element. Problem bezpieczeństwa systemów teleinformatycznych musi być uwzględniany już w fazie ich projektowania i tworzenia narzędzi programowych. Dobrze, że świadomość w tym zakresie zarówno wśród ich twórców, jak i użytkowników w ostatnich latach wyraźnie wzrosła.

Globalny charakter sieci ma ogromny wpływ na bezpieczeństwo wszelkiej działalności podejmowanej z wykorzystaniem Internetu. W wielu krajach brak jest ekspertów ds. bezpieczeństwa, a władze nie mają możliwości egzekwowania prawa w zakresie przestępstw informatycznych.

Wobec coraz bardziej masowego wykorzystywania w gospodarce technologii informatycznych oraz wzrostu zagrożeń pojawia się pytanie, jak długo jeszcze dostępne zabezpieczenia będą gwarantowały pożądany poziom ochrony. Stosowane do uwierzytelniania komunikujących się stron oraz ochrony poufności i integralności danych standardy kryptograficzne także wykazują podatność na ataki, zatem widać wyraźną potrzebę opracowania nowych metod ochrony oraz mocnych, mogących sprostać nowym wyzwaniom mechanizmów zabezpieczeń.

Literatura

1. Jaślan M. (2014), *Cisco: W 2018 roku większość ruchu IP będą generować urządzenia mobilne*, polskaszerokopasmowa.pl/artykuly/cisco-w-2018-roku-wiekszosc-ruchu-ip-beda-generowac-urzadzenia-mobilne.html.

2. Kurzak T. (2014), *Niepokojące wyniki badania bezpieczeństwa transakcji online*. http://Softonet.pl/publikacje/aktualnosci/Niepokojace.wyniki.badania.bezpieczenstwa.transakcji.online,270.
3. www.symantec.com/connect/blogs/dragonfly-western-energy-companies-under-sabotage-threat (2014).
4. www.fortinet.pl/jak-dziala-mobilny-robak-symulacja-ataku-na-smartfon (2014).
5. www.tvn24.pl/internet-hi-tech-media,40/nask-uderza-w-citadel-atakowal-uzytkownikow-polskich-serwisow-finansowych,318802.html (2014).
6. http://di.com.pl/news/41225,0,Duqu_-_nowy_trojan_do_atakow_ukierunkowanych.html (2011).
7. http://technowinki.onet.pl/inne/wiadomosci/urzadzenia-medyczne-podatne-na-hakowanie-moga-zabi,1,5287431,artykul.html (2014).
8. http://finanse.wp.pl/kat,1033767,title,Jedna-z-najwiekszych-gield-zamknieta,wid,16431945,wiadomosc.html (2014).
9. biznes.onet.pl/wirusy-podstepnie-okradaja-konta,18490,5655967,1,prasa-detal.
10. komputerswiat.pl/artykuly/redakcyjne/2014/04/tak-grozny-bedzie-rok-2014.aspx.
11. *Raport o stanie sektora małych i średnich przedsiębiorstw w Polsce w latach 2011–2012* (2013), PARP, Warszawa.
12. pcworld.pl/news/397199/McAfee.szacuje.globalne.koszty.cyberprzestepczosci.na.445.miliardow.dolarow.html (2014).
13. http://technowinki.onet.pl/aktualnosci/wiosenne-ataki-na-uzytkownikow-skype-a-oszusci-defrauduja-walute-bitcoin/d96t1.

INTENSIFICATION OF THE CRIME IN E-COMMERCE

Summary

The scope of use of ICT in the Polish economy is growing rapidly. Provision of information for the purposes of trade and business, and contacts between public administration and the general public is increasingly performed using electronic means and decision-making processes in enterprises are supported by powerful analytical tools. There is a risk of data and privacy loss related to the use of modern technologies, despite the use of available methods and means of protection. The aim of this article is to highlight the scale of the network security threat in the era of the development of electronic commerce, and to show the possibility of effective attacks against PCs and company and industrial networks.

Keywords: e-commerce, the risks of information systems, targets of attacks.

Translated by Zygmunt Mazur