Michał Lewandowski

Zagrożenia dla technologii informacyjno-komunikacyjnej w instytucji publicznej

Obronność - Zeszyty Naukowe Wydziału Zarządzania i Dowodzenia Akademii Obrony Narodowej nr 2(10), 76-90

2014

AUTOR
mgr inż. Michał Lewandowski
mslewandowski@wp.pl

ZAGROŻENIA DLA TECHNOLOGII INFORMACYJNO-KOMUNIKACYJNEJ W INSTYTUCJI PUBLICZNEJ

Wstęp

Dane w postaci elektronicznej są coraz bardziej istotne dla różnych organizacji, a w tym dla instytucji publicznych. Są one podstawą w podejmowaniu decyzji w organizacji. Coraz częściej wszelkie ważne dla instytucji informacje zaczynają być digitalizowane i są przechowywane w postaci elektronicznej oraz przetwarzane w elektronicznych systemach obiegu dokumentów wewnątrz organizacji. W związku z tym, że technologia informacyjno-komunikacyjna (IK) danej instytucji jest połączona z siecią Internet, to jest ona narażona na zagrożenia związane z tym medium. W literaturze przedmiotu poruszającej obszar bezpieczeństwa danych w postaci elektronicznej i technologii IK, autorzy posługują się różnymi określeniami, jak: technologia informatyczna, technologia teleinformatyczna, technologia informacyjna, mając na uwadze to samo. Ale równie często występujący termin, np. technologia teleinformatyczna, rozumiany jest inaczej przez różnych autorów. W związku z tym pojęcia zagrożeń jak i bezpieczeństwa teleinformatycznego mogą oznaczać dla różnych autorów inne rzeczy. Sytuacja ta jest związana z wieloznacznością pojęcia bezpieczeństwa i zagrożeń teleinformatycznych oraz zróżnicowanych sposobów ich definiowania[1]. Swoboda terminologiczna występująca w literaturze jest dość duża. Dodatkowo można spotkać określenia takie, jak bezpieczeństwo cybernetyczne, cyberprzestrzenne, komputerowe czy cyberbezpieczeństwo[2]. Zagrożenia mogą być różnie rozumiane w zależności od przyjętej definicji technologii. W niniejszym artykule autor posługiwać się będzie tym terminem według następującej definicji: *technologia informacyjno-komunikacyjna to technologia służąca do gromadzenia, przetwarzania i udostępniania danych w postaci elektronicznej z wykorzystaniem technik cyfrowych i wszelkich narzędzi komunikacji elektronicznej*.

[1] M. Madej, M. Terlikowski (red.), *Bezpieczeństwo teleinformatyczne państwa*, Polski Instytut Spraw Międzynarodowych, Warszawa 2009, s. 9.

[2] M. Lakomy, *Zagrożenia dla bezpieczeństwa teleinformatycznego państw – przyczynek do typologii*, e-Politikon nr 6/2013, s. 103.

Ze względu na ważność danych, które są podstawą do podejmowania decyzji przez człowieka i rosnący poziom zagrożeń, należy zadbać o bezpieczeństwo danych w postaci elektronicznej i samej technologii IK. Dbanie o bezpieczeństwo jest zapewnieniem odpowiednich środków kontroli i procedur w celu zapewnienia integralności, dostępności i poufności danych i infrastruktury teleinformatycznej. Poprzez poufność rozumiemy *właściwość polegającą na tym, że informacja nie jest udostępniana lub wyjawiana nieupoważnionym osobom, podmiotom lub procesom*. Poprzez integralność rozumiemy *właściwość polegającą na zapewnieniu dokładności i kompletności aktywów*. Poprzez dostępność rozumiemy *właściwość bycia dostępnym i użytecznym na żądanie upoważnionego podmiotu*[3].

Rozwój metod i sposobów ataków jest bardzo szybki i praktycznie z miesiąca na miesiąc powstają nowe zagrożenia, z którymi specjaliści od zabezpieczeń i pracownicy organizacji muszą się zmierzyć. Muszą oni ochronić przed atakami dane w postaci elektronicznej oraz infrastrukturę teleinformatyczną, aby nie została przejęta i użyta niezgodnie z jej przeznaczeniem.

Źródła zagrożeń dla technologii informacyjno-komunikacyjnej

W ostatnich latach zmienił się charakter osób stojących za atakami na technologię IK. Źródła zmieniły się od pojedynczych amatorów (którzy chcą zdobyć sławę poprzez spektakularne podmiany witryn w Internecie, dokonując tego zazwyczaj w ramach eksperymentów), hakerów (chcących sprawdzić swoją wiedzę i umiejętności w praktyce, dokonujących ataków w celu zdobycia sławy i uznania w swoim środowisku) i niezadowolonych pracowników (pragnących zaszkodzić swojemu obecnemu lub byłemu pracodawcy) do jednostek i grup motywowanych chęcią zdobycia korzyści materialnych lub grup działających z pobudek patriotycznych. Mogą to być przestępcy, którzy starają się zdobyć korzyści majątkowe bezpośrednio lub pośrednio poprzez sprzedaż wykradzionych danych, sponsorowane grupy działające w ramach wywiadu gospodarczego lub szpiegostwa przemysłowego, haktywiści próbujący przedstawiać swoje poglądy polityczne i organizacje, w tym terrorystyczne lub rządy państw. Bardzo często nie są to już indywidualne osoby, ale dobrze zorganizowane grupy z dużymi zasobami, które działają w sposób planowy, dobrze zarządzany i dążą do osiągnięcia wyznaczonych celów za wszelką cenę.

W zależności od motywacji możemy wyróżnić następujące źródła zagrożeń:

[3] PN-ISO/IEC 27001:2007.

1) amatorzy, tzw. script kiddies (zasoby organizacji są atakowane ponieważ są dostępne z Internetu i posiadają podatność na znane ataki),

2) hakerzy (zasoby organizacji są atakowane, ponieważ są dostępne z Internetu i posiadają podatności),

3) niezadowoleni pracownicy (zasoby organizacji są atakowane, gdyż są dostępne dla pracownika i są one podatne na ataki z wewnątrz sieci lokalnych),

4) przestępcy (zasoby organizacji są atakowane ponieważ są dostępne z Internetu i posiadają potencjalną wartość na rynku),

5) grupy sponsorowane (haktywiści, instytucje rządowe, korporacje, grupy terrorystyczne, zasoby instytucji są atakowane, gdyż posiadają wartość dla tych grup).

Trochę inny podział źródeł ataku z perspektywy politologicznej może być przedstawiany następująco:

1. hakerzy,
2. haktywiści,
3. „cyberwojownicy",
4. przestępcy,
5. pozostali, czyli posiadający różną motywację amatorzy (np. scripts kiddies)[4].

Dane w postaci elektronicznej, jak i technologia IK instytucji publicznej, mogą być celem ataku każdej z wyżej wymienionych grup. Bez względu na źródło pochodzenia ataków, jeśli taki atak zakończy się powodzeniem, może być bardzo kosztowny dla organizacji. Oczywiście dla instytucji publicznych nie zawsze przekłada się to na straty finansowe, które mogą być łatwo oszacowane jak w przypadku firm komercyjnych[5], ale utrata prestiżu, zaufania obywateli, czy też wpływ na stosunki międzynarodowe mogą być bardzo kosztowne dla danego państwa. Dodatkowo istnieje cały przemysł związany z pisaniem na zamówienie złośliwego oprogramowania, czy też dostarczania usług związanych z przełamywaniem zabezpieczeń. Już nie tylko usługi wysyłania spamu są dostępne do nabycia na czarnym rynku, ale również można zamówić usługi typu DDoS (ang. Distributed Denial-of-Service Attack[6]), dedykowane oprogramowanie do kradzieży cyfrowej tożsamości, dedykowane trojany i rootkity, oprogramowanie wymuszające okup (tzw. ransomware), zamówienie włamań na strony internetowe. Można kupić nawet dostęp do exploitów[7] zawierających wykorzystanie podat-

[4] M. Lakomy, *Zagrożenia…*, wyd. cyt., s. 110.

[5] Ponemon Institute LLC, *2013 Cost of Cyber Crime Study: United States*, październik 2013.

[6] Atak na usługę sieciową wykorzystujący wiele komputerów w celu uniemożliwienia działania tej usługi poprzez zajęcie wszystkich wolnych zasobów.

[7] Jest to program mający na celu wykorzystanie błędów w oprogramowaniu.

ności 0-day[8]. Przykładowo z analizy rynku rosyjskiego wynika, że już w 2012 roku 1 dzień ataku typu DDoS kosztował 30-70 dolarów, 1 tydzień 150 dolarów, usługa wysyłania spamu 10 dolarów za 1000000 maili, rootkit na system linuks 500 dolarów, a na system Windows 292 dolary. Ceny produktów i usług systematycznie maleją, a podobnych rynków jest coraz więcej[9].

Zagrożenia dla technologii informacyjno-komunikacyjnej

Obraz zagrożeń na rok 2014 zawiera większość zagrożeń z roku poprzedniego, ale pojawiły się też nowe, które muszą zostać uwzględnione przez firmy i instytucje w procesach analizy ryzyka i jeśli z niej wynika, że jest to konieczne, to wdrożyć nowe środki zapobiegawcze oraz uwzględnić te zagrożenia w swoich planach ochrony danych i systemów teleinformatycznych. Jednym z ostatnio wykrytych i opisywanych takich zagrożeń są ataki typu APT (ang. Advanced Persistent Threats). Ataki APT są złożonymi, długotrwałymi i wielostopniowymi działaniami kierowanymi przeciwko konkretnym osobom, organizacjom lub firmom. Według wielu źródeł jest to nowy typ ataku jednak zdaniem autora jest to raczej nazwa handlowa stosowana w celu wypromowania i sprzedaży nowych produktów z obszaru bezpieczeństwa teleinformatycznego. Ataki tego typu to złożone działania z wykorzystaniem dobrze znanych technik i wariantów ataków w celu uzyskania dostępu do danych organizacji, jest to rodzaj współczesnego szpiegostwa w świecie cyfrowym. Działania te charakteryzują się długotrwałym okresem, w którym kontrolowane są systemy komputerowe danej organizacji. Zazwyczaj takie działania składają się z następujących kroków: rozpoznanie (zebranie informacji o celu ataku), umieszczenie złośliwego oprogramowania (przeniknięcie do sieci wewnętrznej organizacji z wykorzystaniem szkodliwego oprogramowania lub przełamanie zabezpieczeń organizacji), komunikacja z serwerami Command&Control – C&C (ukryta komunikacja z zewnętrznymi systemami zarządzania i sterowania – centrum sterowania; w tym kroku może nastąpić pobranie dodatkowego złośliwego oprogramowania, które jest trudne do wykrycia), propagacja (rozprzestrzenianie szkodliwego oprogramowania i kompromitacja kolejnych systemów wewnątrz sieci organizacji w celu uzyskania dostępu do cennych danych) i na koniec zdobycie oraz wysyłanie danych (doprowadzenie do kradzieży danych). Za atakami APT stoją grupy dobrze zorganizowanych ludzi posiadających dostęp do wiedzy i mających duże źródła finansowania. Przykładami takich zagrożeń mogą być ataki RedOctober i Care-

[8] Są to luki nieznane publicznie ekspertom do spraw bezpieczeństwa ani producentom oprogramowania.

[9] M. Goncharov, *Russian Underground 101*, Trend Micro INC., 2012.

to. Tak naprawdę ataki tego typu istnieją w sieci od wielu lat, np. atak określany nazwą Czerwony Październik (RedOctober) pojawił się w sieci w 2007 roku, natomiast został wykryty z dużym opóźnieniem. Atak ten był skierowany przeciwko instytucjom dyplomatycznym, agencjom rządowym i organizacjom naukowym[10]. Jednak przez niektórych specjalistów nie jest on uznawany za typowy atak APT, gdyż nie został użyty żaden z ataków 0-day, a jego zakres był dość szeroki[11]. Atak Careto jest nakierowany na zdobycie informacji z instytucji rządowych, przedstawicielstw dyplomatycznych oraz ambasad, firm z branży energetycznej i naftowo-gazowej, instytucji badawczych, prywatnych funduszy inwestycyjnych oraz od aktywistów[12].

Zaawansowanymi atakami, które zostały wykryte są również zagrożenia określone jako Stuxnet, Duqu, Flame. Pierwszy z nich był dedykowanym atakiem na wirówki wzbogacające uran, których używał Iran w swoim przemyśle nuklearnym, drugi był stworzony do wykradania danych z komputerów stosowanych w przemyśle, głównie w krajach takich, jak: Iran, Sudan i Indie. Trzeci – Flame – był złośliwym kodem stworzonym do zbierania i przekazywania danych z zarażonych systemów. Potrafił również aktywować podłączone lub wbudowane mikrofony i kamery w celu rejestracji dźwięku i obrazu oraz przesyłania go na określone serwery sterujące. Był on wymierzony przeciwko instytucjom badawczym i firmom powiązanym z sektorem naukowym. Po wykryciu jego istnienia, autorzy deaktywowali to zagrożenie poprzez samounicestwienie[13]. Wspomniane powyżej trzy zagrożenia wymagały od ich twórców szerokiej wiedzy i dużych nakładów środków, które należało zaangażować do zaprojektowania, wykonania, przetestowania i aktywacji ataków wykorzystujących stworzony złośliwy kod. Kolejnym przykładem zaawansowanego zagrożenia tego typu może być Gauss, który był trojanem bankowym kradnącym dane konieczne do uwierzytelnienia w serwisach bankowych oraz historię przeglądarek internetowych i konfigurację systemu. Był to atak wymierzony głównie w rejon Bliskiego Wschodu, a w szczególności w instytucje bankowe i finansowe Libanu[14].

[10] http://securelist.pl/threats/detect/7104,kampania_red_october_zaawansowana_operacja_cyberszpiegowska_obejmujaca_instytucje_dyplomatyczne_i_agencje_rzadowe.html, [dostęp: 15.02.2014].

[11] http://niebezpiecznik.pl/post/nie-taki-straszny-ten-czerwony-pazdziernik-jak-go-maluja-czyli-kto-wysyla-polakom-trojana-pod-przykrywka-opinii-rosjan-o-katyniu/, [dostęp: 15.02.2014].

[12] http://www.securelist.pl/blog/7260,zagrozenie_apt_careto_the_mask_czesto_zadawane_pytania.html, [dostęp: 15.02.2014].

[13] http://www.dlp-expert.pl/articles/id,709/jak_to_jest_z_tym_stuxnetem_flamem_duqu.html [dostęp: 15.02.2014] .

[14] http://www.chip.pl/news/bezpieczenstwo/wirusy/2012/08/gauss-nowe-zlozone-cyberzagrozenie-wycelowane-w-bliski-wschod, [dostęp: 15.02.2014].

Zagrożenia dla technologii IK mogą być również związane z konfliktami politycznymi w świecie rzeczywistym. Jako przykład można przytoczyć wydarzenia z 2007 roku i atak na technologię IK Estonii (zablokowanie serwisów należących do instytucji rządowych, mediów, banków największych przedsiębiorstw komunikacyjnych i transportowych[15]) podczas kryzysu pomiędzy tym krajem a Rosją, atak na system obrony przeciwlotniczej Syrii podczas ataku samolotów izraelskich na syryjski ośrodek wojskowy, w którym prowadzono prace nad rozwojem technologii nuklearnych[16], wydarzenia z sierpnia 2010 podczas konfliktu rosyjsko-gruzińskiego o Osetię Południową[17], czy też ataki na telefony komórkowe członków tymczasowego rządu ukraińskiego i służb bezpieczeństwa Ukrainy z marca 2014 roku[18].

Mimo że obszar zagrożeń dotyczących technologii IK jest bardzo dynamiczny, istnieją przesłanki pozwalające z dużym prawdopodobieństwem wskazać, które z zagrożeń w 2014 roku będą najbardziej aktywne. Przykładowo jako największe zagrożenia dla przedsiębiorstw są wskazywane[19]:

1. oprogramowanie szkodliwe typu ransomware (szkodliwe oprogramowanie wykorzystywane w przestępczości internetowej blokujące dostęp do danych użytkownika i wymuszające na nim przekazanie określonej sumy pieniędzy przestępcy w celu przywrócenia dostępu do danych użytkownika) dla przedsiębiorstw,
2. kompromitacja rozwiązań chmurowych,
3. zaawansowane kampanie phishingowe (wyłudzanie poufnych informacji osobistych przy wykorzystaniu podszycia się pod znaną osobę lub instytucję) na urządzenia mobilne,
4. zagrożenia typu APT na smartfony i tablety,
5. zagrożenia związane z użytkowaniem prywatnych tabletów i smartfonów w sieciach teleinformatycznych przedsiębiorstw.

Oprogramowanie wyłudzające okup stanie się coraz bardziej agresywne, może się przenieść z atakowania klientów indywidualnych na atakowanie zasobów korporacyjnych. Nowe wersje tego oprogramowania charakteryzują się opcją szyfrowania danych (co było przewidywane w poprzednim roku[20]), przechowywaniem klucza szyfrującego na serwerach przestępców w Internecie oraz skróconym czasem na podjęcie decyzji przez użytkownika o przekazaniu pieniędzy (przykładowo po 24 lub 72 godzinach zostają usunięte klucze, które posłużyły do zaszyfrowania danych użytkownika).

[15] M. Lakomy, *Zagrożenia…*, wyd. cyt., s. 101.
[16] Tamże, s. 102.
[17] Tamże, s. 133.
[18] http://www.spidersweb.pl/2014/03/cyberatak-na-ukraine.html, [dostęp: 4.03.2014].
[19] http://www.webroot.com/blog/2013/12/18/top-5-enterprise-threat-predictions-2014/, [dostęp: 4.03.2014].
[20] M. Lewandowski, *Szkodliwe oprogramowanie typu ransomware – zagrożenie dla instytucji publicznych*, luty 2013.

Ze względu na to, że coraz bardziej powszechne stają się rozwiązania chmurowe i coraz więcej przedsiębiorstw przechowuje w nich dane, będą one atrakcyjnym celem dla przestępców i konkurencji. Kompromitacja i uzyskanie dostępu do chmury danego dostawcy tych usług może dać dostęp do danych wszystkich organizacji, które powierzyły mu swoje dane.

Zagrożenie typu phising nie jest nowym zagrożeniem, ale wykorzystanie popularności i powszechności smartfonów i tabletów oraz faktu, że zabezpieczenia tych urządzeń w porównaniu z laptopami są obecnie na niskim poziomie, może doprowadzić do powstania specjalnych akcji służących do przejmowania cyfrowej tożsamości lub wyłudzania poufnych informacji osobistych. Bazując na tych samych założeniach: popularności i słabego zabezpieczenia danych na urządzeniach mobilnych będą one wykorzystane w atakach typu APT. Zakładając, że urządzenia tego typu są bardzo popularne każda luka wykryta w oprogramowaniu systemowym lub użytkowym tych urządzeń daje duże możliwości przestępcom i ludziom stającym za atakami APT. Potwierdzać to mogą ostatnie informacje dotyczące podatności oprogramowania Android w wersji 4.2 z API starszym niż w wersji 17. Wynika z nich, że 70% użytkowników urządzeń z Androidem na świecie stało się podatnych na atak wykorzystujący tę podatność[21]. Podobnie jest z systemem firmy Apple, gdzie wykryta podatność umożliwia przechwycenie i odczytanie danych z ruchu zaszyfrowanego[22].

Powyżej wspomniane podatności związane z urządzeniami mobilnymi spowodują, że smartfony i tablety będą głównym wektorem ataku na zasoby teleinformatyczne firm, szczególnie jeśli prywatne urządzenia tego typu będą miały dostęp do sieci teleinformatycznych przedsiębiorstw.

Z kolei zagrożenia, które zdaniem analityków z firmy McAfee[23] będą najbardziej powszechne w 2014 roku to:

1. złośliwe oprogramowanie na urządzenia mobilne,
2. ataki uwzgledniające waluty wirtualne,
3. cyberprzestępczość i cyberwojna,
4. ataki społecznościowe,
5. ataki na komputery użytkowników i serwery,
6. zagrożenia związane z obszarem BigData[24] (przetwarzanie dużych zbiorów danych i ochrona informacji w nich ukrytych),
7. ataki na zasoby chmurowe.

Eksperci z tej firmy przewidują, że najwięcej złośliwego oprogramowania będzie powstawało na urządzenia mobilne, może się pojawić oprogra-

[21] http://niebezpiecznik.pl/post/powazna-dziura-w-androidzie-4-2-i-starszych-jego-wersjach-70-uzytkownikow-androida-podatnych-na-atak/, [dostęp: 22.02.2014].

[22] http://niebezpiecznik.pl/post/krytyczny-blad-w-iphonach-ipadach-i-mac-os-x-jak-najszybciej-wgrajcie-aktualizacje/, [dostęp: 22.02.2014].

[23] Przewidywane zagrożenia w roku 2014: raport McAfee Labs.

[24] E. Frankowski*, Big Data w teorii i trochę w praktyce*, [w:] ITbiznes.pl, czerwiec 2013.

mowanie wyłudzające okup przeznaczone dla smartfonów i tabletów. Przy wykorzystaniu zainfekowanych prywatnych urządzeń i podłączeniu ich do infrastruktury korporacyjnej nieświadomy użytkownik może ułatwić potencjalnym napastnikom wydobycie poufnych informacji. Kolejnym zagrożeniem będą ataki związane z wirtualnymi walutami. Umożliwiają one anonimowe płatności w sieci Internet i mogą być wykorzystywane przez oprogramowania wymuszające okup w stosunku do danych firmowych. Dodatkowo wzrośnie liczba ataków, których celem będzie przejecie wirtualnej waluty (jak BitCoin[25] lub Billon[26]). Coraz częstsze będą też ataki wykorzystujące sieci społecznościowe i przechwytujące cyfrowe tożsamości użytkowników. W obszarze komputerów osobistych i serwerów będą się one koncentrowały na atakowaniu przeglądarek sieciowych i na atakowaniu poniżej warstwy systemu operacyjnego na stos pamięci i system BIOS. Kolejne dwa obszary, które będą atakowane to są dane w chmurach i dane w dużych zbiorach danych (tzw. Bigdata).

Natomiast eksperci z firmy FireEye zakładają, że największe zagrożenia są związane z podatnościami przeglądarek internetowych i ze szkodliwym oprogramowaniem, które będzie wykorzystywane w ramach ataków APT[27]. Podobnie przewidują analitycy z firmy Sophos – największym zagrożeniem ma być szkodliwe oprogramowanie wykorzystywane w atakach typu APT, do kradzieży danych personalnych i do ataków na urządzenia mobilne[28].

Warto również przytoczyć przewidywania ekspertów z Polski dotyczące zagrożeń na 2014 rok. Ich zdaniem najistotniejszymi zagrożeniami będą:

1. ataki na rozwiązania chmurowe,
2. wycieki baz danych zawierające dane osobowe,
3. ataki drive-by download,
4. phishing z wykorzystaniem poczty elektronicznej i serwisów WWW,
5. zagrożenia dla platformy Android,
6. Ataki DDoS[29].

Inne podejście do zagrożeń, jeśli spojrzymy na nie z punktu widzenia politycznego, prezentuje Miron Lakomy. Według niego zagrożenia takie prezentują się następująco:

1. haking,
2. haktywizm,
3. „haktywizm patriotyczny”,

[25] http://bitcoin.pl/obitcoin, [dostęp: 22.02.2014].

[26] http://finanse.wp.pl/kat,1033767,title,Bedzie-nowa-polska-waluta-Nazywa-sie-Billon,wid,16388222,wiadomosc.html?ticaid=112553&_ticrsn=3, [dostęp: 01.03.2014].

[27] *FireEye Advanced Threat Report: 2013*.

[28] *Security Threat Report 2014 – Smarter, Shadier, Stealthier Malware*.

[29] Fundacja Bezpieczna Cyberprzestrzeń, *Raport: największe zagrożenia dla bezpieczeństwa w Internecie w roku 2014 – głos polskich ekspertów*, 2014.

4. wąsko rozumiana cyberprzestępczość,
5. cyberterroryzm,
6. cyberszpiegostwo,
7. militarne wykorzystanie cyberprzestrzeni[30].

Z kolei wychodząc z punktu widzenia użytkownika zagrożenia dla technologii IK i danych użytkowników mogą wyglądać w następujący sposób:

1. aplikacje zawierające trojana (złośliwy oprogramowanie „doklejone" jest do innej, pozornie nieszkodliwej aplikacji, którą użytkownik sam instaluje),
2. ataki drive-by download (włamanie do komputera lub urządzenia mobilnego następuje w momencie wejścia na stronę webową lub otwarcia pliku, np. PDF, MS Office),
3. botnet (sieć komputerów przejętych przez przestępców przy użyciu złośliwego programu, tzw. Bot lub Zombi, kontrolowana za pomocą centrum sterowania – serwera zarzadzania i sterowania, tzw. Command and Control),
4. ataki APT,
5. ataki typu wodopój – Watering Hole (ataki wykorzystujące przejęte przez przestępców zaufane serwisy webowe, z których korzysta określona organizacja lub docelowa grupa – zwykle wykorzystywane są exploity zawierające podatności 0-day),
6. phishing (przy wykorzystaniu email, sms, portali społecznościowych – przesyłane wiadomości mają na celu przekonanie adresatów do zainstalowana aplikacji, wejścia na wskazaną stronę webową, do otwarcia pliku dostępnego na stronie webowej lub przesłanego do adresata, przekazania określonych danych, itp.),
7. whaling (ataki typu łapanie „grubego zwierza" – celem są osoby ważne lub bogate, dzięki którym potencjalnie możliwe są duże zyski przestępców)[31].

Jak widać na kilku przytoczonych przykładach do określenia zagrożeń można podejść w różny sposób. Jednak z punktu widzenia służb technicznych instytucji publicznej odpowiedzialnych za bezpieczeństwo danych i technologii IK lub administratora konkretnego systemu, naprawdę nie ma to przeważnie znaczenia, czy atak zostanie zakwalifikowany jako atak hakerów, haktywistów, cyberwojowników, przestępców czy innych grup. Liczy się bezpośrednio dla nich efekt końcowy, który bez względu na grupę atakującą, jest ten sam – system został skompromitowany lub nastąpiła kradzież danych. Z ich punktu widzenia konieczne jest zapewnienie bezpieczeństwa – czyli poufności, integralności i dostępności danych w postaci

[30] M. Lakomy, *Zagrożenia…*, wyd. cyt., s. 110.
[31] M. Stawowski, *Konferencja: Kultura bezpieczeństwa informacji*, 03.03.2014.

elektronicznej i technologii IK. Dlatego, jeśli spojrzeć na zagrożenia z punktu widzenia instytucji publicznej, w nadchodzącym roku najgroźniejszymi zagrożeniami związanymi z technologiami IK mogą być:

1. szkodliwe oprogramowanie,
2. phishing,
3. ataki drive-by-download,
4. wykorzystanie znanych podatności systemów i oprogramowania użytkowego,
5. ataki typu APT,
6. złośliwe oprogramowanie na smartfony i tablety,
7. ataki DDoS,
8. ataki na publiczne dostępne serwisy webowe (manipulacja danymi lub zniszczenie danych),
9. kradzież danych,
10. inżynieria społeczna (Social Engineering)[32].

Możliwe sposoby ochrony technologii informacyjno-komunikacyjnej w instytucji publicznej

Ze względu na swój charakter i zazwyczaj szczupłe zasoby przeznaczone na zapewnienie bezpieczeństwa danych w postaci elektronicznej i technologii IK, w instytucji publicznej nie ma możliwości, aby jednakowo mocno chronić wszystkie zasoby teleinformatyczne. Takie podejście nie byłoby również racjonalne. Dlatego pierwszym krokiem powinna być analiza ryzyka. Należy określić, jakie zasoby są kluczowe dla danej organizacji i co należy chronić. Po określeniu tych zasobów, identyfikacji zagrożeń i oszacowaniu prawdopodobieństwa materializacji zagrożeń, powinny zostać dobrane odpowiednie mechanizmy ochronne w celu przeciwdziałania wskazanym zagrożeniom. Podjęte działania powinny przeciwdziałać utracie poufności i integralności danych oraz minimalizować czas niedostępności usług i minimalizować niekorzystny wpływ zmaterializowanego zagrożenia na działalność instytucji publicznej i jej prestiż.

Obecnie stosowanie tylko zabezpieczeń opartych na sygnaturach nie jest już wystarczające. Należy wprowadzać do infrastruktury teleinformatycznej instytucji publicznych rozwiązania wykonujące dokładną analizę zawartości komunikacji sieciowej przy uwzględnieniu kontekstu jej wystąpienia. Specjaliści od zabezpieczeń i instytucje publiczne muszą zwrócić większą uwagę na wykrywanie, monitoring i analizę tego, co dzieje się w ich sieciach teleinformatycznych. Udana korelacja zdarzeń i przepływów

[32] Lista zagrożeń dla technologii informacyjno-komunikacyjnej instytucji publicznych – opracowanie własne.

w sieciach może być bardzo dobrym systemem wczesnego ostrzegania. Działania proaktywne powinny być głównym punktem rozważań instytucji podczas wdrażania nowych warstw ochrony. W ostatecznym rozrachunku działania takie będą tańsze, a takie podejście jest bardziej skuteczne z punktu widzenia zapewnienia bezpieczeństwa danym w postaci elektronicznej i technologii IK – nie przeciwdziałamy tylko skutkom kompromitacji i ataków, a staramy się nie dopuścić do poczynienia dużych szkód przez potencjalnego napastnika. Z drugiej strony każdy wcześniej, czy później ulegnie atakowi – zależy to tylko od sił i środków atakującego. Jednak bazując na tym przekonaniu, nie można się jedynie skupiać na przygotowaniach instytucji tylko do usuwania skutków ataków. Zdaniem autora jest oczywiście bardzo ważne, aby mieć odpowiedni plan postępowania w sytuacjach kryzysowych i posiadać procedury odtworzenia działania funkcjonalności w środowisku teleinformatycznym instytucji, ale nie jest to podejście wystarczające w obecnych czasach. Zarządzanie planami ciągłości działania i planami na sytuacje kryzysowe jest istotnym czynnikiem, ale dobrze skonstruowany system wczesnego ostrzegania i świadomość pracowników w obszarze bezpieczeństwa systemów teleinformatycznych są podstawą działań zmierzających do niedopuszczenia do dużych szkód spowodowanych przez ataki na dane w postaci elektronicznej i technologię IK instytucji publicznej. Im wcześniej wykryjemy próby ataków, czy też oprogramowanie szkodliwe, tym szybciej jesteśmy w stanie wprowadzić środki zaradcze. Często jest tak, że na początku atakujący musi zrobić rozpoznanie, następnie dostarczyć oprogramowanie szkodliwe, dokonać jego rozprzestrzenienia w infrastrukturze instytucji, utrzymując komunikację ze swoimi serwerami zarządzania i sterowania. I dopiero kiedy namierzy odpowiedni cel i dokona kradzieży danych, dokonuje ich wysłania na zewnątrz. Jeżeli uda się wychwycić niepożądane działania przed ostatnim etapem, tzn. na etapach: infiltracji, sterowania i rozprzestrzeniania to można się uchronić przed wykradzeniem danych w postaci elektronicznej.

Skuteczny system monitorowania aktywności w sieci teleinformatycznej i zaawansowane techniki wykrywania oprogramowania szkodliwego mogą w znacznym stopniu wesprzeć instytucję w ochronie przed określonymi wyżej zagrożeniami – nie tylko przed złośliwym oprogramowaniem (zagrożenie nr 1 na liście zagrożeń dla technologii informacyjno komunikacyjnych instytucji publicznych), ale również przed atakami drive-by-download (zagrożenie nr 3), częścią działań w ramach ataków APT (zagrożenie nr 5).

Kolejną ważną rzeczą jest system automatycznej aktualizacji i wdrażania poprawek do systemów operacyjnych i oprogramowania użytkowego. Rozwiązania takie mogą wesprzeć instytucję publiczną w walce ze szkodliwym oprogramowaniem, atakami drive-by-download, atakami wykorzystującymi znane podatności systemów i oprogramowania użytkowego

(odpowiednio zagrożenia nr 1, 3, 4 na liście zagrożeń dla instytucji publicznych) oraz przed częścią działań w ramach ataków APT i ataków na publicznie dostępne serwisy webowe (zagrożenia nr 5 i 8).

Kolejnym istotnym krokiem są szkolenia dla pracowników instytucji publicznych z obszaru bezpieczeństwa danych w postaci elektronicznej i bezpieczeństwa technologii IK. Oczywiście szkolenia te muszą być dopasowane do konkretnej instytucji i w jasny sposób odnosić się do codziennych działań pracowników, w których przetwarzają dane organizacji i korzystają z technologii IK. Podniesienie świadomości pracowników w tych obszarach bardzo istotnie wspiera organizację w walce z zagrożeniami dotyczącymi omawianego obszaru, a w szczególności wspierają instytucje w walce z zagrożeniami związanymi z phishingiem, inżynierią społeczną (odpowiednio zagrożenia nr 2 i 10), oraz przed częścią działań w ramach ataków APT i na urządzenia typu smartfon oraz tablet (odpowiednio zagrożenia nr 5 i 6). Jednak ochrona danych i urządzeń mobilnych typu smartfon i tablet, które mają dostęp do sieci instytucji publicznej i na których są przetwarzane dane instytucji jest bardzo dużym wyzwaniem. Najlepszym rozwiązaniem w tym przypadku jest prywatna chmura i przetwarzanie danych po stronie instytucji z uwzględnieniem komunikacji wykorzystującej szyfrowanie.

Do ochrony przed zagrożeniami DDoS (zagrożenie nr 7) należy zastosować rozwiązania przeznaczone do walki z takim typem ataku i posiadać przygotowane procedury współpracy z dostawcą usług internetowych. Kolejnym bardzo ważnym mechanizmem jest kopia bezpieczeństwa danych. Wspiera ona instytucje w walce z zagrożeniami związanymi z kradzieżą danych, atakami DDoS i atakami na publiczne dostępne serwisy webowe – umożliwiając działania związane z odtworzeniem danych (odpowiednio zagrożenia nr 9, 7 i 8). W kontekście walki z kradzieżą danych (zagrożenie nr 9) bardzo istotnym mechanizmem jest szyfrowanie danych. Mechanizmami uzupełniającymi powyższe sposoby ochrony w instytucji publicznej powinny być odpowiednio zabezpieczenia organizacyjne w postaci zapewnienia odpowiednich struktur, zakresów czynności i odpowiedzialności, polityk, procedur oraz instrukcji. Kolejnymi mechanizmami wspierającymi instytucję są audyty zarówno wewnętrzne, jak i zewnętrzne, w obszarze zapewnienia bezpieczeństwa danych w postaci elektronicznej i technologii informacyjno-komunikacyjnej danej instytucji.

Podsumowanie

We współczesnym świecie dane w postaci elektronicznej stanowią coraz większą wartość dla instytucji publicznych. Ze względu na połączenie systemów teleinformatycznych tych instytucji z globalną siecią Internet

dane te są narażone na zagrożenia, które związane są z tym medium. W każdym roku dochodzą nowe zagrożenia związane z danymi w postaci elektronicznej i z technologią informacyjno-komunikacyjną. Wspomniane w tekście zagrożenia są zagrożeniami przewidywanymi, ale może się okazać, że w obecnym roku wystąpi zagrożenie, którego obecnie nie jesteśmy w stanie przewidzieć. Jednak skutki większości zagrożeń jesteśmy w stanie określić, a prawdopodobieństwo ich wystąpienia jesteśmy w stanie obniżyć, stosując przedstawione mechanizmy ochronne. Instytucje publiczne powinny zachować równowagę pomiędzy zastosowaniem automatycznych technicznych środków ochrony, a zabezpieczeniami organizacyjnymi i w postaci odpowiedniej świadomości pracowników w obszarze bezpieczeństwa technologii informacyjno-komunikacyjnej. Ze względu na ilość przesyłanych danych i metody ukrywania szkodliwej działalności powinno się stosować nowoczesne mechanizmy ochronne, które są dedykowaną odpowiedzią na nowe zagrożenia. Jednocześnie nie można zapominać o człowieku i jego edukacji w obszarze bezpieczeństwa danych. Te dwa podejścia, zaplanowane i przeprowadzone w instytucji publicznej bardzo dobrze się uzupełniają i w wyniku synergii mogą spowodować wzrost bezpieczeństwa danych i technologii IK, większy niż wynikałoby to tylko z wdrożenia rozwiązań oddzielnie w każdym z tych obszarów. Oczywiście nie ma idealnych zabezpieczeń. Organizacja musi sobie zdawać sprawę z tego, że przy odpowiedniej determinacji jednostek, czy też zorganizowanych grup, atak na infrastrukturę teleinformatyczną i dane może się powieść i instytucja musi być przygotowana na takie zdarzenie. Powinna posiadać plany działania na wypadek kryzysu i plany ciągłości działania – o ile z analizy ryzyka wynika, że takie plany są wymagane. Istotną rzeczą jest to, że zazwyczaj od uzyskania dostępu do infrastruktury teleinformatycznej instytucji do wycieku danych mija trochę czasu i skuteczne mechanizmu monitoringu oraz świadomość pracowników w obszarze bezpieczeństwa danych i technologii IK może doprowadzić do powstrzymania ostatniej fazy, czyli wycieku danych z instytucji.

Proces ochrony jest to wyścig zbrojeń – jak zostaną opracowane i wdrożone mechanizmy ochronne, to pojawiają się nowe metody, czy też sposoby ataku. Dla instytucji publicznej ważne jest, aby utrzymywać wymagany poziom ochrony danych i technologii IK, posiadać skuteczny system wczesnego ostrzegania oraz być przygotowanym na wypadek przełamania zabezpieczeń. Posiadane procedury postępowania na wypadek wykrycia włamania, procedury przywrócenia funkcjonowania usług – odtworzenia funkcjonalności w wymaganym czasie, procedury minimalizujące szkody dla organizacji (zawierające między innymi odpowiednią politykę informacyjną zarówno zewnętrzną, jak i wewnętrzną) oraz odpowiednie procedury ciągłości działania (o ile z analizy ryzyka wynika, że są wymagane) stanowią bardzo istotne uzupełnienie zabezpieczeń technicznych.

Wykorzystując odpowiednie audyty wewnętrzne i zewnętrzne w obszarze bezpieczeństwa danych w postaci elektronicznej i technologii IK, instytucja jest w stanie stale doskonalić swój system ochrony. Podstawowymi polami działania w obszarze bezpieczeństwa teleinformatycznego, z punktu widzenia instytucji publicznej, powinny być działania w obszarze zapewnienia poufności, integralności i dostępności danych w postaci elektronicznej oraz niezawodności sieci (odporności na ataki i awarie) i ciągłości działania technologii informacyjno-komunikacyjnej wykorzystywanej w instytucji publicznej.

Bibliografia

1. FireEye Advanced Threat Report: 2013.
2. Frankowski E., *Big Data w teorii i trochę w praktyce*, [w:] ITbiznes.pl, czerwiec 2013.
3. Fundacja Bezpieczna Cyberprzestrzeń, *Raport: największe zagrożenia dla bezpieczeństwa w Internecie w roku 2014 - głos polskich ekspertów,* 2014.
4. Goncharov M., *Russian Underground 101*, Trend Micro INC., 2012.
5. Lakomy M., *Zagrożenia dla bezpieczeństwa teleinformatycznego państw – przyczynek do typologii,* [w:] e-Politikon nr 6/2013.
6. Lewandowski M., *Szkodliwe oprogramowanie typu ransomware – zagrożenie dla instytucji publicznych*, luty 2013.
7. Madej M., Terlikowski M. (red.), *Bezpieczeństwo teleinformatyczne państwa*, Polski Instytut Spraw Międzynarodowych, Warszawa 2009.
8. PN-ISO/IEC 27001:2007.
9. Ponemon Institute LLC, 2013 Cost of Cyber Crime Study: United States, październik 2013.
10. Raport McAfee Labs: *Przewidywane zagrożenia w roku 2014*.
11. Security Threat Report 2014 – Smarter, Shadier, Stealthier Malware.
12. Stawowski M., Konferencja: *Kultura bezpieczeństwa informacji*, 03.03.2014.

Źródła internetowe

1. http://bitcoin.pl/obitcoin.
2. http://finanse.wp.pl/kat,1033767,title,Bedzie-nowa-polska-waluta-Nazywa-sie-Billon,wid,16388222,wiadomosc.html?ticaid=112553&_ticrsn=3.
3. http://niebezpiecznik.pl/post/krytyczny-blad-w-iphonach-ipadach-i-mac-os-x-jak-najszybciej-wgrajcie-aktualizacje/.

4. http://niebezpiecznik.pl/post/nie-taki-straszny-ten-czerwony-pazdziernik-jak-go-maluja-czyli-kto-wysyla-polakom-trojana-pod-przykrywka-opinii-rosjan-o-katyniu/.
5. http://niebezpiecznik.pl/post/powazna-dziura-w-androidzie-4-2-i-starszych-jego-wersjach-70-uzytkownikow-androida-podatnych-na-atak/.
6. http://securelist.pl/threats/detect/7104,kampania_red_october_zaawansowana_operacja_cyberszpiegowska_obejmujaca_instytucje_dyplomatyczne_i_agencje_rzadowe.html.
7. http://www.chip.pl/news/bezpieczenstwo/wirusy/2012/08/gauss-nowe-zlozone-cyberzagrozenie-wycelowane-w-bliski-wschod.
8. http://www.dlp-expert.pl/articles/id,709/jak_to_jest_z_tym_stuxnetem_flamem_duqu.html.
9. http://www.securelist.pl/blog/7260,zagrozenie_apt_careto_the_mask_czesto_zadawane_pytania.html.
10. http://www.spidersweb.pl/2014/03/cyberatak-na-ukraine.html.
11. http://www.webroot.com/blog/2013/12/18/top-5-enterprise-threat-predictions-2014/.

ABSTRACT
THREATS TO INFORMATION AND COMMUNICATION TECHNOLOGIES IN A PUBLIC INSTITUTION

Electronic data are becoming more and more valuable for public institutions in the modern world. Due to these institutions' ITC systems' connections with the Internet global network, their data are exposed to threats connected with this medium. The greatest threats for public institutions in 2014 include malware, phishing, drive-by-download attacks, taking advantage of users' systems and programs sensitivity, APT attacks, smart phones and tablets malicious software, DDoS attacks, attacks on public web services (connected with data destruction or manipulation), data theft or social engineering. In order to tackle these threats, public institutions should consider the implementation of dedicated technical and organizational solutions and use support of internal and external audits concerning sensitivity policy, integrity and accessibility of electronic data and maintaining information and configuration security. Due to the character of current threats to electronic data and information and configuration technology, public institutions should develop procedures and prepare activities in case of breaching existing protection, apart from dedicated protection programs.