Marcin Kowalczyk
Uniwersytet Przyrodniczo-Humanistyczny w Siedlcach
Koło Naukowe Informatyków „Genbit"

Zagrożenia systemów informatycznych e-administracji – szkodliwe oprogramowanie i ataki[1]

The risks of IT systems in e-administration – malicious software and attacks

Streszczenie: *W pracy zostały przedstawione zagrożenia systemów informatycznych: techniczne aspekty szkodliwego oprogramowania i ataki, zarówno w Internecie, jak i intranecie. Przegląd technik i zaleceń bezpieczeństwa systemów informatycznych dla firm i instytucji zajmujących się administracją oraz bazami i przetwarzaniem danych.*

Słowa kluczowe: zagrożenia, bezpieczeństwo, wirusy, ataki, e-administracja, systemy informatyczne

Abstract: *The paper shows risks of IT systems: technical aspects of malicious software and attacks. In the Internet and a intranet. The article presents an overview of techniques and security recommendations for companies and offices for administration, databases and data processing.*

Keywords: risks, security, virus, attacks, IT systems, office

Wstęp

Żyjemy obecnie w społeczeństwie informacyjnym, w czasach, kiedy ważną rolą pełni informacja – jej przetwarzanie, wykorzystywanie, przesyłanie i obsługa. Dużą rolę odgrywają tu technologie teleinformatyczne oraz cała branża ICT[2], dzięki której są informatyzowane wszelkie dziedziny życia[3]. Jedną z nich jest administracja. Skorzystanie z najnowszych technologii, informatyki i dobrej organizacji pozwala na stworzenie e-administracji[4]. Niezbędne usługi zapewniają systemy informatyczne. Według ustawy są to zespoły „współpracujących ze sobą urządzeń, programów, procedur przetwarzania informacji i narzędzi programowych

[1] Artykuł napisany pod opieką naukową dr. Piotra Świtalskiego.
[2] ICT – Information and Communication Technology.
[3] J. Papińska-Kacperek, *Społeczeństwo informacyjne*, PWN, Warszawa 2008, s. 17-19.
[4] Mikulski Kazimierz, *"e-administracja" - istota pojęcia,* [w:] *Technologia informacyjna w administracji i dla administracji*, Wydawnictwo Kujawsko-Pomorskiej Szkoły Wyższej, Bydgoszcz 2008, s. 72-74.

zastosowanych w celu przetwarzania danych”[5]. To, że wiele od nich zależy, budzi realne obawy i zagrożenia. Nie ma funkcjonujących systemów w pełni bezpiecznych. Zawsze należy brać pod uwagę, że wprowadzone zabezpieczenia kiedyś mogą zostać złamane, a dostęp do informacji uzyska osoba niepowołana[6]. Szczególnie trzeba chronić dane w e-administracji: systemach interakcyjnych i danych dostępnych dla użytkowników przez Internet (np. BIP, USOSweb). Należy chronić także same dane przed zniszczeniem, utratą lub modyfikacją. Najbardziej narażone są newralgiczne dane interesantów, firm, informacje gospodarcze lub finansowe. Zazwyczaj przyczyną incydentów są czynniki zewnętrzne (cyberprzestępczość), ale źródłami mogą być błędy w zabezpieczeniach (projektowe, implementacyjne, konfiguracyjne, operatora). Wszystkimi aspektami i przeciwdziałaniami zajmuje się bezpieczeństwo teleinformatyczne. W niniejszej pracy zostanie przedstawiony jedynie przegląd technik ataków oraz złośliwego oprogramowania.

Złośliwe oprogramowanie

Kategorie złośliwego oprogramowania

Oprogramowanie o działaniu niepożądanym, szkodliwym określa się terminem **malware** (z ang. *malicious software*). Jest to cała klasa programów powodujących szkody na komputerach użytkowników. Wykorzystują one słabości w systemach informatycznych. Jeśli znajdą się na urządzeniu osoby korzystającej z systemu teleinformatycznego, może to powodować kradzież danych (dane osobowe, numery kont bankowych, hasła itd.) lub ich przekłamanie. Jeszcze bardziej niebezpieczne jest takie oprogramowanie na komputerach wewnątrz systemu informatycznego e-administracji (stacja robocza personelu, serwer). Wtedy zagrożenie nie będzie dotyczyło tylko jednego użytkownika, ale całej bazy danych, a także możliwe jest, że wszystkich użytkowników chcących połączyć się z systemem. Możliwa będzie kradzież danych tysięcy osób (i później sprzedaż ich na czarnym rynku lub wykorzystanie w innych celach niezgodnych z prawem), ich modyfikacja, zablokowanie całego systemu itd. Każdy incydent wymaga późniejszej analizy i naprawy poniesionych szkód. Instytucja lub firma, która będzie miała przestój, straci czas, pieniądze i zaufanie użytkowników oraz nie będzie mogła wykonywać swoich zadań. Z tego względu, że cyberprzestępcy mogą osiągnąć największe korzyści włamując się na komputery wewnątrz systemu informatycznego, problem dotyczy właśnie najbardziej tych obiektów.

[5] Ustawa z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (tekst jednolity: Dz.U. 2002 nr 101 poz. 926), Art. 7, pkt. 2a.
[6] A. Barczak, T. Sydoruk, *Bezpieczeństwo systemów informatycznych*, Wydawnictwo Akademii Podlaskiej, Siedlce 2002.

Adware

Adware jest najmniej groźnym typem złośliwego oprogramowania. Często zostaje wbudowane w programy shareware lub instalowane automatycznie bez zgody użytkownika (np. ściągane przez trojany). Jego głównym celem jest wyświetlanie reklam. O ile takie działanie technicznie powoduje głównie tylko zajęcie pamięci, czasu procesora i sieci, to jest bardziej szkodliwe ze względów psychologicznych: rozprasza i irytuje użytkownika oraz budzi niepokój (trudno je odinstalować).

Spyware

Podklasą malware jest spyware – oprogramowanie szpiegujące. Zbiera dane o użytkowniku bez jego wiedzy i przesyła je do cyberprzestępców. Mogą to być informacje o odwiedzanych stronach WWW, adresach email, numerach kart kredytowych i PIN oraz zapisywanie uderzeń klawiszy (keylogger). Tak wiele danych dostępnych dla przestępcy może pozwolić na kradzież tożsamości i np. wypłacenie pieniędzy z konta bankowego, zaś jeśli ofiarą padnie ktoś z personelu, może spowodować to nieautoryzowany dostęp do systemu.

Ransomware

Oprogramowanie ransomware żąda okupu w zamian za zatrzymanie lub usunięcie wcześniej wyrządzonego, szkodliwego działania. Może np. zablokować dostęp do komputera, zastraszać itp., aby uzyskać pieniądze. Przykładem jest CryptoLocker – trojan szyfrujący dokumenty użytkownika silnym 2048 bitowym, unikalnym kluczem RSA[7] i żądający zapłaty w zamian za ich odszyfrowanie[8].

Techniki złośliwego oprogramowania

Wirusy

Wirusy to samopowielające się szkodliwe oprogramowanie. Do działania i rozprzestrzeniania potrzebują jednak nosiciela. Najczęściej są przenoszone na pendrivach lub płytach CD/DVD, dawniej na dyskietkach. Mogą także rozprzestrzeniać się przez sieć z wykorzystaniem załączników w poczcie e-mail.

Tego typu złośliwe oprogramowanie ma wiele odmian. Wirusy plikowe nadpisują programy na dysku lub tylko doklejają swój kod do plików (najczęściej wykonywalnych), dzięki czemu oryginalny program działa tak jak przed infekcją, ale jednocześnie wykonuje szkodliwe działania. **Wirusy dyskowe** modyfikują sektor startowy dodając swój kod, przez to ładują się z każdym uruchomieniem systemu operacyjnego. Można je także podzielić

[7] RSA – niesymetryczny algorytm szyfrujący; składa się z klucza publicznego do kodowania informacji oraz prywatnego do ich odczytywania. Zabezpieczenie opiera się na trudności faktoryzacji dużych liczb.

[8] Raiu Costin, Kaspersky Lab, http://securelist.pl/analysis/7247,cryptolocker_chce_twoich_pieniedzy.html]; dostęp 2014.04.27.

na nierezydentne i rezydentne. **Wirusy polimorficzne** zmieniają swój kod (np. za każdym razem inaczej go szyfrując), aby było trudniej je wykryć (dlatego stosuje się metody heurystyczne). Jeszcze inną odmianą są **makrowirusy** – szkodliwe makra w doklejane w dokumentach tworzonych za pomocą pakietów biurowych np. Microsoft Office lub OpenOffice. kradzież tożsamości Ich grupa docelowa to biura i użytkownicy często tworzący pliki tekstowe (DOC, ODF) oraz arkusze kalkulacyjne (XLS, ODS).

Robaki internetowe

Wirusy mają tę słabość, że potrzebują plików, aby móc się rozprzestrzeniać – dzięki temu można łatwiej je wykryć. Robaki internetowe to programy komputerowe, które replikują się jako nowe pliki. Najczęściej używają sieci Internet, intranet lub LAN. Wysyłają się także w załącznikach e-mail, przez programy P2P oraz komunikatory, a także automatycznie przez zainfekowane strony internetowe (drive-by download) lub inne oprogramowanie (np. trojany typu dropper lub downloader).

Konie trojańskie

Trojany[9] imitują oprogramowanie (lub są dołączone do niego), które użytkownik umyślnie chce zainstalować. Często znajdują się w crackach[10], zmodyfikowanych programach z nieoficjalnych stron, oprogramowaniu podszywającym się pod antywirusy itd. Dzięki temu mogą łatwo się rozprzestrzeniać oraz trudniej jest je wykryć. Obecnie powstało wiele ich odmian. **Trojan dropper** służy do instalacji innego trojana lub szkodliwego oprogramowania bez wiedzy użytkownika. **Trojan downloader** podobnie jak poprzedni, instaluje inne szkodliwe oprogramowanie, ale ten nie przenosi w sobie kodu instalowanego programu, a może go ściągnąć z Internetu. **Trojan backdoor** zostawia „tylną furtkę", dzięki której cyberprzestępca może przejąć kontrolę nad zainfekowanym komputerem (tworząc komputer zombie, wykorzystywany np. w botnetach). **Trojan notifer** przekazuje informacje o zainstalowanym wcześniej trojanie oraz adresach IP, otwartych portach i inne wybrane dane. **Trojan spy** – oprogramowanie spyware, śledzi użytkownika na zainfekowanym komputerze. **Trojan clicker** otwiera wybraną stronę internetową w przeglądarce użytkownika (stosowane w atakach DDoS lub zwiększeniu zysków z reklam).

Keylogger

Złośliwe oprogramowanie typu keylogger to program, który monitoruje i zapisuje wszystkie naciskane klawisze bez wiedzy użytkownika, a następnie wysyła log cyberprzestępcom. Dzięki temu mogą oni uzyskać hasła do kont pocztowych, bankowych, gier online, wykraść tożsamość

[9] Nazwa „trojan" pochodzi od drewnianego konia, w mitologii greckiej, którego zbudowali Grecy podczas wojny trojańskiej w celu zdobycia Troi.

[10] Crack – program lub modyfikacja (patch) służąca ominięciu zabezpieczeń oprogramowania; wytwarzany zazwyczaj dzięki inżynierii wstecznej analizując i modyfikując zabezpieczony program.

lub uzyskać dostęp do systemu informatycznego. Są także odmiany, które wykonują zrzuty ekranu (screenscraper) np. podczas kliknięcia, ujawniając co dokładnie robi dana osoba (przez to nie działają zabezpieczenia typu klawiatura ekranowa). Dostępne są także legalne programy tego typu służące do monitorowania za zgodą i wiedzą monitorowanego np. jako ochrona rodzicielska, monitoring przez administratora, w celu zapewnianie bezpieczeństwa w firmie itp.[11]

Rootkit

Rootkit to oprogramowanie ukrywające w systemie inny szkodliwy kod. Po jego zainstalowaniu trudniej wykryć zarówno samego rootkita, jak i ukryte złośliwe oprogramowanie. W uruchomionym, zainfekowanym systemie operacyjnym pliki programów stają się niewidoczne, zarówno na dysku jak i w pamięci.

Ataki

Nawet jeśli poszczególne komputery nie są zainfekowane, to przez słabości w zabezpieczeniach system informatyczny nadal może być celem ataku.

Sniffing

Sniffer to narzędzie, dzięki któremu cyberprzestępcy mogą podsłuchiwać dane przesyłane w niezabezpieczonej (niezaszyfrowanej) sieci. Można wykraść podobne dane jak keyloggerami, z tym że ofiarą ataku jest nie poszczególny komputer, a cała sieć. Najczęściej podsłuchiwane są sieci WiFi. Technicznie możliwe jest jednak także zbieranie informacji z sieci kablowych. Dlatego przy przesyłaniu newralgicznych danych (np. haseł, poufnych dokumentów) ważne jest korzystanie z szyfrowania np. protokołem SSL (HTTPS – wersja na stronach internetowych np. banku, poczty e-mail itd). Chroni to przed poznaniem treści przez cyberprzestępcę, ale nie maskuje samego faktu przesyłania danych i ich ilości.

DoS

DoS – Denial of Service – odmowa usługi. Polega na wysłaniu dużej ilości zapytań do serwera (który będzie musiał na nie odpowiedzieć) w celu wykorzystania zasobów: pamięci RAM, pamięci dyskowej i czasu procesora. Istnieje odmiana ataku **SYN flood**. Przy nawiązywaniu połączenia TCP zamiast standardowego trójstopniowego przesłania trzech pakietów: SYN, SYN-ACK i ACK, cyberprzestępca wysyła podrobione pakiety SYN, serwer odpowiada pakietami SYN-ACK do nieistniejącego hosta i czeka na otrzymanie odpowiedzi ACK, aż do zapełnienia bufora. Jeśli atak jest przeprowadzany z jednego komputera (adresu IP) łatwiej przeciwdziałać.

[11] Grebennikov Nikolay, Kaspersky Lab, http://securelist.pl/analysis/5783,keyloggery_jak_dzialaja_i_jak_mozna_je_wykryc_czesc_1.html; dostęp 2014-04-27.

Sytuacja staje się trudniejsza do opanowania w przypadku wykorzystania wielu hostów z różnych miejsc (najczęściej komputerów zombie połączonych w sieć botnet) – taki atak nazywa się **DDoS** – Distributed Denial of Service – rozproszona odmowa usługi). Przy udanym ataku serwery mogą całkowicie przestać działać. Strony informacyjne WWW nie będą spełniały swojego zadania, dane przechowywane w chmurze (cloud) staną się niedostępne utrudniając pracę instytucjom, a firmy (szczególnie te działające głównie w Internecie np. sklepy internetowe) przestaną całkowicie działać. Tego typu ataki są często wykonywane przez nieuczciwą konkurencję lub haktywistów w ramach protestów.

Ataki na strony internetowe

Celem ataku mogą być bezpośrednio strony WWW i bazy danych przechowywane na serwerach. Wykorzystuje się w nich luki w oprogramowaniu, zarówno tym na serwerze, jak i w przeglądarce oraz systemie użytkownika wchodzącego na stronę. Celem cyberprzestępców nie jest tylko wyłączenie strony, ale też włamanie i uzyskanie poufnych informacji (np. haszy haseł[12], danych osobowych, całych baz danych), wstawienie własnego kodu lub informacji na stronę. Stosuje się tu techniki m.in. SQL Injection (przesłanie do bazy danych innego zapytania niż oczekiwał tego twórca; winą zazwyczaj jest niedokładne filtrowanie danych wejściowych) oraz XSS (cross-site scripting – osadzenie szkodliwego kodu np. JavaScript na stronie).

Phishing

Atak oparty na socjotechnice. Cyberprzestępcy wykonują kopię strony instytucji np. banku. Następnie nakłaniają użytkownika, aby na nią wszedł i niczego nieświadomy wpisał swoje dane dostępowe, tak jak zazwyczaj to robi podczas normalnego użytkowania strony (np. hasło, numer karty). Dane zostają wysłane do cyberprzestępców, którzy mogą wykorzystać je już na prawdziwej stronie np. uzyskując dostęp do konta.

W celu nakłonienia użytkownika do wpisania danych cyberprzestępcy wykorzystują łatwowierność, nawyki i szeroko pojętą inżynierię społeczną. Dodatkowo korzystają oni ze środków technicznych np. podszywanie się pod domenę oryginalnej strony (poprzez zmianę DNS-ów: w pliku hosts lub poprzez pharming – zatrucie serwerów DNS). Zaś wiadomości e-mail mogą być wysyłane z adresów widocznych dla użytkownika jako oryginalne dla danej instytucji (spoofing).

[12] Hasła na serwerach zazwyczaj nie są przechowywane w postaci jawnej ze względów bezpieczeństwa (w przypadku włamania możliwe byłoby łatwe uzyskanie dostępu do wszystkich haseł, administrator operujący serwerem miałby też do nich bezpośredni dostęp). Dlatego stosuje się funkcje skrótu np. MD5, SHA-2 – które dopiero się porównuje. Nadal jest jednak możliwe złamanie prostych haseł (ponadto używając technik GPGPU proces ten może zostać przyspieszony).

Podsumowanie

Nie istnieją systemy informatyczne w pełni bezpieczne, każde zabezpieczenie może zostać złamane. Jednakże specjaliści ds. bezpieczeństwa zobowiązani są do dołożenia wszelkich starań, aby dane, komputery i ich użytkownicy byli chronieni w możliwie jak największym stopniu.

Zabezpieczeniami należy objąć zarówno poszczególne komputery użytkowników w systemie informatycznym, jak i całe serwery. W celu wykrywania złośliwego oprogramowania instalowane są tam programy antywirusowe. Aby uniknąć części ataków, powinny znajdować się tam też firewalle[13]. Wykorzystywane są także monitory HIPS (Host-based intrusion prevention system). Wygodnym rozwiązaniem dla instytucji oraz firm są tworzone przez producentów oprogramowania całe pakiety typu security zawierające ww. aplikacje. W przypadku pojawienia się podejrzanych plików wykorzystuje się również skanery antywirusowe dostępne online. Już zainfekowane komputery mogą zostać przeskanowane programami antywirusowym uruchamianymi z płyty LiveCD (bootowalne), a nie spod zainstalowanego systemu.

Ważnym aspektem w profilaktyce zagrożeń systemów informatycznych jest odpowiednie wykonywanie kopii zapasowych danych. W przypadku niektórych zagrożeń (np. typu CryptoLocker) może to być jedyny sposób na odzyskanie utraconych danych.

Oprócz technicznych zabezpieczeń istotny jest zdrowy rozsądek użytkowników i ich wiedza. Szczególnie w e-administracji potrzebne są szkolenia dotyczące bezpieczeństwa. Dzięki temu, personel będzie świadomy zagrożeń oraz będzie miał wiedzę na temat przeciwdziałania im. Ważne jest także przestrzeganie przez pracowników zasad polityki bezpieczeństwa w instytucji.

Bibliografia

Bezpieczeństwo w sieci, [w:] *Społeczeństwo informacyjne*, Papińska-Kacperek J. (red.), Wydawnictwo Naukowe PWN, Warszawa 2008, s. 241-362.

Słownik, [w:] *Securelist.pl*, Kaspersky Lab, http://securelist.pl/glossary.html; dostęp 2014-04-27.

Suchorzewska A., *Aspekty techniczne zjawiska cyberprzestępczości,* [w:] *Ochrona prawna systemów informatycznych wobec zagrożenia cyberterroryzmem*, Wolters Kluwer Polska, Warszawa 2010, s. 77-104.

[13] Zapora sieciowa (firewall) – przepuszcza ruch sieciowy odpowiadający zdefiniowanym regułom i blokuje pozostałe pakiety oraz żądania.