Michał Młotek
Marcin Siedlarz

Rządowy Zespół Reagowania na Incydenty Komputerowe CERT.GOV.PL

Wstęp

Rolą Rządowego Zespołu Reagowania na Incydenty Komputerowe CERT.GOV.PL działającego w ramach Departamentu Bezpieczeństwa Teleinformatycznego jest zapewnianie i rozwijanie zdolności jednostek organizacyjnych administracji publicznej RP do ochrony przed cyberzagrożeniami, ze szczególnym uwzględnieniem ataków ukierunkowanych na infrastrukturę krytyczną. CERT.GOV.PL funkcjonuje zgodnie z przyjętymi w dniu 9 marca 2009 r. przez Komitet Stały Rady Ministrów Założeniami Rządowego Programu Ochrony Cyberprzestrzeni RP na lata 2009 - 2011 (RPOC).

Do zadań nałożonych na wyżej wymieniony Zespół i wykonywanych od momentu jego powstania w lutym 2008 r. należy:

a) kreowanie polityki w zakresie ochrony przed cyberzagrożeniami,
b) koordynowanie przepływu informacji pomiędzy podmiotami w tym zakresie,
c) wykrywanie cyberzagrożeń, rozpoznawanie ich i przeciwdziałanie im,
d) współpraca z krajowymi instytucjami, organizacjami oraz podmiotami resortowymi w zakresie ochrony cyberprzestrzeni,
e) reprezentacja RP w kontaktach międzynarodowych (w zakresie współpracy wojskowej, w porozumieniu z Centrum Koordynacyjnym Systemu Reagowania na Incydenty Komputerowe resortu obrony narodowej),
f) gromadzenie wiedzy dotyczącej stanu bezpieczeństwa i zagrożeń dla krytycznej infrastruktury teleinformatycznej,
g) reagowanie na incydenty bezpieczeństwa teleinformatycznego ze szczególnym uwzględnieniem krytycznej infrastruktury teleinformatycznej państwa,
h) prowadzenie analiz powłamaniowych,
i) tworzenie polityki ochrony systemów i sieci teleinformatycznych,
j) szkolenia i podnoszenie świadomości odnośnie do zagrożeń komputerowych,
k) przygotowywanie okresowych raportów w zakresie bezpieczeństwa teleinformatycznego państwa,
l) konsulting i doradztwo w zakresie cyberbezpieczeństwa.

System wczesnego ostrzegania o zagrożeniach w internecie – ARAKIS-GOV

Podstawowym sposobem ochrony rządowych systemów teleinformatycznych jest objęcie ich parasolem systemu wczesnego ostrzegania ARAKIS-GOV. Działanie tego systemu polega na agregowaniu informacji o zagrożeniach sieciowych na podstawie monitorowanego ruchu w sieci (za pomocą rozproszonych sond) oraz informacji ze źródeł zewnętrznych. Jego funkcjonalność to przede wszystkim informowanie o nowych zagrożeniach, opis tych zagrożeń w formie sygnatur, zapewniający środek ochronny, który może być wykorzystany w systemach wykrywania/prewencji włamań, analiza trendów związanych z zagrożeniami oraz korelacja informacji dotyczą-

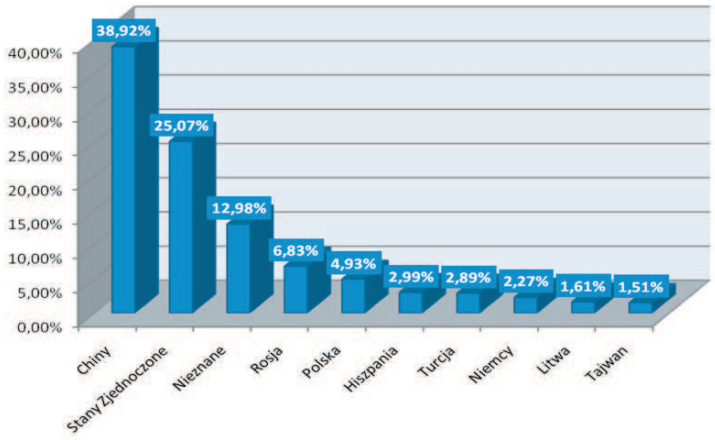
cych zdarzeń z różnych typów źródeł sieciowych oraz z różnych instytucji uczestniczących w systemie.

W przypadku ARAKIS-GOV, jego architektura rozproszonego systemu sond rozlokowanych w instytucjach administracji publicznej na styku z siecią internet, z których informacje trafiają do centrum, gdzie w systemie SEC (*Simple Event Correlator*) następuje ich agregacja i analiza, odzwierciedla spojrzenie na bezpieczeństwo z punktu widzenia zagrożenia zewnętrznego wobec wszystkich chronionych sieci. W związku z tym, mając do dyspozycji informacje o możliwych incydentach pochodzących zarówno z jednostkowych systemów zapór (*firewalli*) jak i z systemów pocztowych, sieci „Darknet”[1] i z samych sond, które znajdują się w niewykorzystywanej przez chronione podmioty adresacji IP, można w sposób semi-zautomatyzowany wykrywać anomalie powiązane z sygnaturami. W rezultacie można tworzyć gotowe sygnatury, z których skorzystać może każdy administrator sieci chronionej przez ARAKIS-GOV. W ten sposób zagrożenie jest likwidowane, zanim praktycznie wystąpi.

Aktualnie ochroną systemu ARAKIS-GOV objętych jest 16 ministerstw, 11 jednostek samorządowych oraz 42 inne jednostki, takie jak Biuro Bezpieczeństwa Narodowego, Centralne Biuro Antykorupcyjne, Zakład Ubezpieczeń Społecznych czy Senat RP.

Na podstawie informacji zebranych przez wyżej wymieniony system w roku 2010 określono lokalizację geograficzną źródłowych adresów IP, z których wykonywano ataki na polskie sieci rządowe monitorowane przez ten system.

W czołówce napastników znajdują się adresy zlokalizowane w Chinach (≈39%) i Stanach Zjednoczonych (≈25%). Należy podkreślić, iż trend ten potwierdza się również w przypadku ogólnoświatowych systemów.



Rys. 1. Rozkład procentowy ataków na sieci monitorowane w różnych państwach przez system ARAKIS-GOV.

Na powyższym wykresie przedstawiającym procentowe wyliczenie ataków na monitorowane przez system ARAKIS-GOV sieci na trzecim miejscu znajduje się pozycja „nieznane”. Określenie to dotyczy adresów IP w chwili obecnej nieprzypisanych

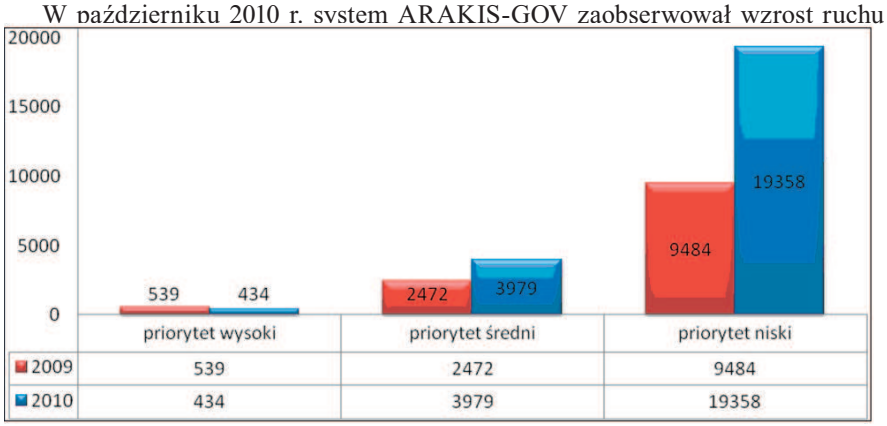
[1] Darknet – obszar sieci posiadający rutowalne, lecz nie przypisane aktualnie żadnemu podmiotowi bloki adresów IP. Każdy pakiet z takim adresem należy traktować jako potencjalnie wrogi.

żadnemu podmiotowi. Oznacza to, iż dokonano podszycia się (podmiany adresu źródłowego IP) pod nieistniejący adres IP.

Należy zauważyć, że ze względu na specyfikę protokołu TCP/IP nie można bezpośrednio łączyć źródła pochodzenia pakietów z rzeczywistą lokalizacją zleceniodawcy ataku. Wynika to z faktu, iż w celu ukrycia swej tożsamości i fizycznej lokalizacji atakujący mogą wykorzystywać serwery pośredniczące (tzw. proxy) lub słabo zabezpieczone komputery, nad którymi wcześniej przejmują kontrolę.

W stosunku do roku 2009 system ARAKIS-GOV odnotował w roku następnym dwa razy większą całkowitą liczbę alarmów (28 109), przy czym mniejszą o priorytecie „wysokim". Zdecydowana jest przewaga alarmów o priorytecie „niskim". Tak duża liczba alarmów o priorytecie „niskim" spowodowana była obserwacją wzrostu ruchu typu BitTorrent[2] na przełomie miesiąca marca i kwietnia 2010 r. Na dalszym etapie obserwacji stwierdzono, że ruch ten zaburza obraz aktualnej sytuacji w monitorowanych sieciach, dlatego też wprowadzono filtry w systemie w celu wyeliminowania alarmów związanych z uznanym za nieszkodliwy ruchem BitTorrent.

W październiku 2010 r. system ARAKIS-GOV zaobserwował wzrost ruchu na



Rys. 2. Rozkład alarmów z uwzględnieniem priorytetów w latach 2009 - 2010.

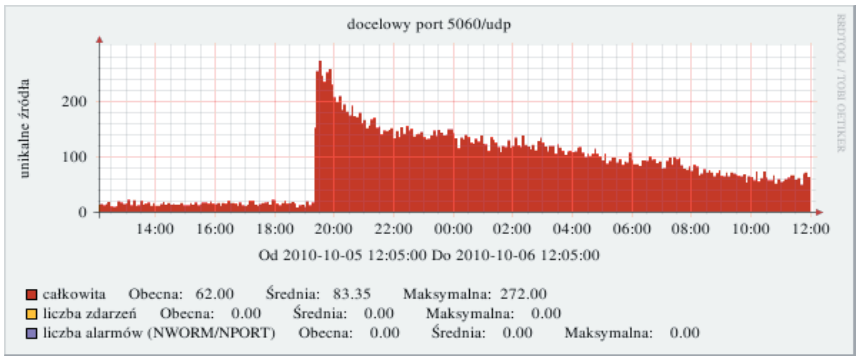
porcie 5060/UDP (*Session Initiation Protocol*) – jednym z protokołów używanych w technologii telefonii internetowej VoIP. Wzrost ten widoczny był zarówno w lokalizacjach chronionych przez system, jak i w przestrzeniach adresowych Darknetu. Poniżej przedstawiono wykres obrazujący powyższą sytuację.

Ruch został zaobserwowany z ponad 400 unikalnych źródłowych adresów IP i kierowany był na ponad 1560 unikalnych adresów docelowych objętych monitoringiem przez system ARAKIS-GOV. Sytuacja ta była wynikiem skanowania w poszukiwaniu serwerów VoIP. W tym celu wykorzystano żądania OPTION protokołu SIP, które pozwalają w odpowiedzi uzyskać informacje o opcjach pracy serwera. Powyższe dane zbierane były najprawdopodobniej w celu wykorzystania do ataku na serwery SIP

[2] BitTorrent – protokół wymiany i dystrybucji plików przez internet, którego celem jest odciążenie łączy serwera udostępniającego pliki. Jego największą zaletą w porównaniu do protokołu HTTP jest podział pasma pomiędzy osoby, które w tym samym czasie pobierają dany plik. Oznacza to, że użytkownik w czasie pobierania wysyła fragmenty pliku innym użytkownikom. Ruch sieciowy dotyczący usług współdzielenia plików z zasady nie powinien być obserwowany w systemach administracji publicznej. Sytuacja zaobserwowana przez system ARAKIS-GOV może mieć zarówno charakter przypadkowego skanowania sieci przynależących do administracji publicznej, jak i świadczyć o działających w przeszłości usługach współdzielenia plików w tych sieciach.

(VoIP). Ponadto informacje tego typu dostarczają także wiedzy na temat oprogramowania, na którego podstawie działa serwer SIP.

Warto zauważyć, iż pod koniec lipca 2010 r. Zespół CERT.GOV.PL został poin-



Rys. 3. Rozkład ruchu na porcie 5060/UDP w przeciągu doby, w której wystapiły anomalie, na podstawie danych z lokalizacji chronionych systemem.

formowany o incydencie, który wystapił w jednym z Urzędów Miasta. Chodziło o kradzież impulsów telekomunikacyjnych. Na podstawie danych uzyskanych od administratora sieci lokalnej UM stwierdzono, iż chodzi o kradzież, której dokonano poprzez włamanie się na konto uprzywilejowane, które było zabezpieczone słabym hasłem. Konsekwencją powyższego było wykonanie połączeń na koszt UM o łącznym czasie 740 280 sekund (206 godzin = 8,5 dnia). Oszacowane przez Urząd Miasta straty z tytułu nieautoryzowanych połączeń telefonicznych wyniosły około 60 000 PLN.

Program badania bezpieczeństwa witryn internetowych administracji publicznej

Powiększając zakres usług świadczonych przez Rządowy Zespół Reagowania na Incydenty Komputerowe CERT.GOV.PL, od dnia 1 lipca 2008 r. rozpoczęto nowy program sukcesywnego badania stanu zabezpieczeń witryn internetowych należących do instytucji administracji publicznej. Działania te mają na celu określenie poziomu bezpieczeństwa aplikacji „www" instytucji publicznych, a także usunięcie wykrytych nieprawidłowości, zanim zostaną wykorzystane przez cyberprzestępców.

W 2010 r. przebadano 93 witryny należące do 63 instytucji państwowych. Stwierdzono ogółem 1277 błędów w tym: 451 błędów o bardzo wysokim poziomie zagrożenia, 40 błędów o wysokim poziomie zagrożenia, 440 błędy o niskim poziomie zagrożenia i 346 błędów oznaczonych jako „informacyjne".

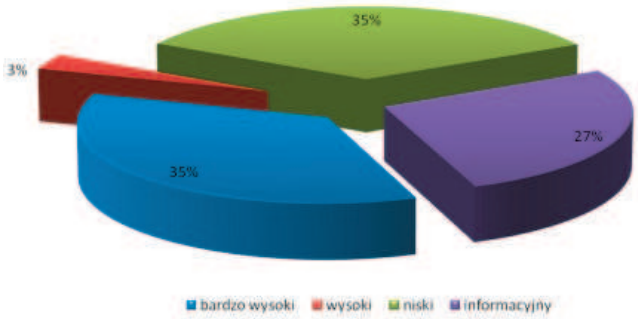
Do ważniejszych ministerstw, których witryny zostały przebadane przez Zespół CERT.GOV.PL należą:

1. Ministerstwo Spraw Wewnętrznych i Administracji,
2. Kancelaria Prezydenta RP,
3. Centrum Obsługi Kancelarii Prezesa RM,
4. Ministerstwo Spraw Zagranicznych,
5. Ministerstwo Infrastruktury,
6. Ministerstwo Finansów,
7. Ministerstwo Edukacji Narodowej,
8. Ministerstwo Pracy i Polityki Społecznej.

Ponadto testom poddane zostały strony „www" innych ważnych instytucji, takich jak:

1. Centralne Biuro Antykorupcyjne,
2. Ministerstwo Obrony Narodowej,
3. Komenda Główna Policji,
4. Kancelaria Polskiej Akademii Nauk,
5. Prokuratura Okręgowa w Bydgoszczy,
6. Państwowa Komisja Wyborcza,
7. Ministerstwo Finansów (Izby Celne i Urzędy Skarbowe).

W trakcie skanowania witryn stwierdzono, że 75% spośród nich zawierało przy-



Rys. 4. Statystyka wykrytych podatności na zawirusowanie w witrynach „www" należących do administracji publicznej (według poziomu zagrożenia).

najmniej jedną podatność, którą należało uznać za krytyczną dla bezpieczeństwa serwera i publikowanych na witrynie treści. Tylko w nielicznych przypadkach zabezpieczenia witryn były skuteczne i nie stwierdzono w nich żadnych podatności. Tak duże różnice w jakości zabezpieczeń systemów świadczą o bardzo zróżnicowanej wiedzy związanej z bezpieczeństwem wśród osób odpowiedzialnych za administrację i wykonanie systemów. Poniższa tabela przedstawia ranking przebadanych witryn pod względem ilości błędów krytycznych.

Tab. 1. Ocena stanu bezpieczeństwa witryn internetowych wyszczególnionych instytucji.

Stan bezpieczeństwa przebadanych witryn	Instytucja
Bardzo dobry poziom bezpieczeństwa	Centrum Obsługi Kancelarii Prezesa RM
	Prokuratura Okręgowa w Bydgoszczy
	Urząd Kontroli Skarbowej w Białymstoku
	Urząd Kontroli Skarbowej w Katowicach
	Urząd Kontroli Skarbowej w Olsztynie
	Urząd Kontroli Skarbowej w Poznaniu
Średni poziom bezpieczeństwa	Krajowa Rada Radiofonii i Telewizji
	Izba Skarbowa w Gdańsku
	Ministerstwo Sprawiedliwości
	Państwowy Instytut Geologiczny
	Urząd Komunikacji Elektronicznej
Niski poziom bezpieczeństwa	Izba Skarbowa w Krakowie
	Rządowe Centrum Legislacji
	Polska Agencja Rozwoju Przedsiębiorczości
	Centralny Ośrodek Geodezji i Kartografii
	Izba Skarbowa w Katowicach

Rozwijając wizję systemu ARAKIS-GOV na podstawie doświadczeń zdobytych podczas testów witryn internetowych, na początku IV kwartału 2009 r. uruchomiono testową wersję systemu Honey Spider Network – GOV (HSN-GOV), która wykorzystywana jest w celu monitorowania rządowych stron „www" pod względem serwowania złośliwego oprogramowania. Wyżej wymieniony system przeznaczony jest na potrzeby administracji rządowej. HSN-GOV okresowo dokonuje weryfikacji zawartości strony w poszukiwaniu złośliwego kodu JavaScript, który może infekować komputery użytkowników odwiedzających stronę „www". Obecnie monitoringiem objęto ponad 2000 stron internetowych należących do administracji rządowej (gov.pl).

Na podstawie wyników zawartych w HSN-GOV okresowo generowana jest lista stron „www", zawierająca te adresy, które zostały przez system uznane za szkodliwe. Powyższa lista (*blacklist*) wykorzystana zostanie docelowo w projekcie DNS-Blackholing, który będzie realizowany w przyszłości w jednostkach administracji rządowej.

W systemie HSN-GOV zostały zaimplementowane dodatkowe funkcjonalności mające na celu wspomaganie analiz wykonywanych przez system. Jedną z najbardziej istotnych jest metoda wykrywania mechanizmu fast-flux[3]. Ponadto HoneySpider Network korzysta ze źródeł zewnętrznych wspomagających analizy oprogramowania złośliwego, takich jak VirusTotal, Anubis czy Norman Sandbox.

Ataki ukierunkowane

Jednostki administracji publicznej, w odróżnieniu od indywidualnych użytkowników cyberprzestrzeni, są szczególnie narażone na jeden z typów wrogich działań, tj. na ataki ukierunkowane. Ten typ ataków polega najczęściej na próbie nakłonienia użytkownika do otwarcia złośliwego załącznika w poczcie e-mail.

W roku 2010 coraz częściej rejestrowano ataki ukierunkowane wykorzystujące metody socjotechniczne, takie jak spersonalizowana przesyłka wysłana z adresu, do którego odbiorca ma zaufanie (przy czym tu następuje podszycie się pod nadawcę), czy zawartość zawierająca interesujące treści z punktu widzenia odbiorcy. Trend ten znacznie się nasilił po tragedii smoleńskiej. W niecałe dwa dni po katastrofie z konta Bill Murray bbc.news@wp.pl rozsyłana była poczta e-mail zatytułowana *Looking beyond Poland's, unprecedented disaster*. Treść wiadomości dotyczyła bezpośrednio wydarzeń z 10 kwietnia 2010 r. Jednocześnie zostały do niej dołączone dwa pliki – „Page1.pdf" oraz „Draft.doc", których otwarcie mogło doprowadzić do zainfekowania sytemu.

Kilka dni później, tj. 16 kwietnia 2010 r., odnotowano kolejny przypadek wykorzystania tragedii narodowej do rozsyłania poczty internetowej zawierającej złośliwe oprogramowanie. Wiadomość *Dear colleagues! Kazakhstan head of state sends official condolences to Seym of Poland. Official text is attached. Condolences are also posted on official site* http://www.kazakhstan.org.sg/content/intro.php?act=news&c_id=726 rozsyłana z konta kazakstan.embass@mail.ru o tytule *Kazakhstan head of state sends official condolences* również zawierała złośliwy załącznik o nazwie *Official_condolences.pdf*, którego otwarcie mogło prowadzić do utraty istotnych informacji lub nawet do przejęcia komputera użytkownika.

[3] Fast-flux – jedna z technologii stosowana przy popełnianiu przestępstw internetowych, np. phishingu. Jest to mechanizm przełączający serwera DNS (jedna domena odnosi się do kilku adresów IP), w celu ukrycia stron, na które przesyłane są wyłudzone dane.

W maju 2010 r. dokonano ataku na Ministerstwo Spraw Zagranicznych. Polegał on na masowym przesyłaniu wiadomości mailowych do pracowników MSZ. Wiadomości tego typu były wysłane na 192 adresy pracowników zarówno centrali, jak i placówek zagranicznych. Była to próba podszycia się pod pracownika pomocy technicznej i zawierała prośbę o podanie nazwy użytkownika, adresu e-mail, hasła oraz numeru telefonu. Wiadomość wysyłano z maszyny przypisanej do Danii. Na podstawie informacji otrzymanych z duńskiego zespołu CERT wspomniany host został przejęty przez cyberprzestępców.

W grudniu 2010 r. natomiast odnotowano masowe rozsyłanie wiadomości mejlowych mających swoje źródło w Federacji Rosyjskiej, a adresowanych do kilku instytucji administracji publicznej w Polsce, m.in. do MSZ i ABW. Wiadomości te zawierały zainfekowane załączniki w postaci plików pdf bądź pakietu MS Office. Ich tytuły dotyczyły sytuacji m.in. wojsk NATO: *Rogozin Condemns secret NATO Pact* lub portalu Wiki Leaks i szczegółów aresztowania jego założyciela – Juliana Assange'a.

Oprócz metod socjotechnicznych, bardzo ważnym aspektem wspomnianych ataków są techniki „czysto" informatyczne. W przypadku zaobserwowanych ataków używano złośliwego oprogramowania, które wykorzystywało podatności typu „0-day" na popularne aplikacje. Oznaczało to, iż w dniu wykonania ataku nie była dostępna stosowna aktualizacja oprogramowania, która mogłaby zapobiec przełamaniu zabezpieczeń. Dodatkowo plik był wykrywany jedynie przez nieliczne silniki antywirusowe.

Wykorzystanie metod socjotechnicznych oraz phisingowych do ataku na użytkowników systemów handlu uprawnieniami do emisji CO_2

W styczniu 2010 r. właściciele kont krajowych systemów handlu uprawnieniami do emisji gazów cieplarnianych otrzymali e-maile, w których zostali poinformowani, iż w związku z powtarzającymi się atakami na systemy handlu Komisja Europejska zadecydowała o podniesieniu poziomu zabezpieczeń. Treść e-maila informowała, iż Komisja ta wskazała firmę do realizacji tego zadania, przekazując jej konieczne informacje o użytkownikach. W związku z tym należało wpisać adres wskazanej strony internetowej i potwierdzić na niej poprawność informacji. Następnie użytkownikom miał być przekazany klucz USB, dzięki któremu można by było bezpiecznie logować się do systemu.

Takie e-maile zostały przesłane do użytkowników z wielu krajów, w tym z Polski. Na uwagę zasługuje kilka szczegółów: tekst wiadomości napisany był w odpowiednim języku, w zależności od narodowości odbiorcy, na wskazaną stronę można było się dostać zarówno klikając link umieszczony w treści, jak i wpisując ręcznie adres samej domeny. Przestępcy stworzyli całą stronę internetową fałszywej firmy i umieścili na niej odpowiednie wersje językowe wraz z całym portfolio (fałszywym). Proces „potwierdzania" informacji składał się z kilku podstron, na których znajdowały się różne pytania. Na jednej z nich było pytanie o login do systemu, na innej o hasło. Jako że nie były one umieszczone obok siebie, lecz obok innych zapytań, np. o nazwę firmy, ulicę, numer budynku, kod pocztowy, miasto, numer kierunkowy itp., mogły nie wzbudzić podejrzeń. Dodatkowo, każda przesyłka e-mail była kierowana osobiście do każdej z atakowanych osób. Zawierała jej imię, nazwisko, numer telefonu służbowego oraz nazwę reprezentowanej firmy. W dużym stopniu podwyższało to zaufanie odbiorcy do prawdziwości treści. Wielu użytkowników w różnych krajach (w tym i w Polsce) podało dane, o które atakującym chodziło. Dane te natychmiast zostały wykorzystane do wykradzenia użytkownikom posiadanych przez nich uprawnień do emisji. Szkody powstałe np. w Niemczech szacowa-

ne są na trzy miliony euro. Dzięki szybkiej reakcji polskiego Krajowego Administratora Systemu Handlu Uprawnieniami, Polska nie poniosła strat.

Należy zauważyć, iż przestępcy wykorzystali metody zarówno socjotechniczne (e-mail w odpowiednim języku zawierający dane odbiorcy oraz odpowiednią formę fałszywej strony internetowej), jak i phishingowe (skupienie się na wyłudzeniu haseł i natychmiastowe ich wykorzystanie, podszycie się pod legalną stronę, duża skala ataku). Sądząc po stratach tylko jednego kraju należy sądzić, iż osiągnęli sukces. Spowodowane to było tym, że dane użytkowników rejestrów są publicznie dostępne (wymóg prawny Komisji Europejskiej), że posiadacze kont nie byli świadomi zagrożeń, a także niskim stopniem zabezpieczenia samych rejestrów (dostęp i użytkowanie chronione wyłącznie za pomocą hasła).

Streszczenie

W artykule przedstawiono proces tworzenia Rządowego Zespołu Reagowania na Incydenty Komputerowe CERT.GOV.PL, jego zadania i misję. Poza tym szczegółowo omówiono jedno z najważniejszych narzędzi stosowanych w pracy Zespołu, tj. system wczesnego ostrzegania o zagrożeniach w sieci internet – ARAKIS-GOV. Funkcjonalność tego systemu to przede wszystkim informowanie o nowych zagrożeniach w sieci, opis tych zagrożeń (w formie sygnatur) zapewniający środek ochronny, który może być wykorzystywany w systemach wykrywania i prewencji włamań, analiza trendów związanych z zagrożeniami oraz korelacja wiadomości dotyczących zdarzeń pochodzących z różnych typów źródeł sieciowych i z różnych instytucji uczestniczących w systemie.

Zaprezentowano również program odnoszący się do bezpieczeństwa witryn należących do instytucji administracji publicznej wraz z wynikami testów. Ostatnia część niniejszej publikacji została poświęcona omówieniu najistotniejszych incydentów wykrytych przez CERT.GOV.PL w 2010 r., tj. atakom ukierunkowanym oraz próbie wyłudzenia z systemu handlu uprawnieniami jednostek emisji dwutlenku węgla.

Abstract

he following article presents the creation of Polish Governmental Computer Security Incident Response Team – CERT.GOV.PL, its key activities and main tasks and duties. The aim of this article was also to describe one of the most important tools utilized by CERT, which is: ARAKIS-GOV – the early warning system on Internet threats, as well as the effects of its operation. The primary function of the system is informing of new threats within the networks and providing the description (in a form of signatures) of the identified threats. The definitions can be implemented into intrusion identification and prevention systems. Additionally, the system allows to analyze the trends in the nature of changing threats and coordination of data flow relating to security threats originating in different networks administrated by different institutional members of the system.

The article also presents the websites security software working at the websites of state administration and the test results.

Finally, the article describes the major incidents identified by CERT.GOV.PL in 2010, that is attacks aimed at obtaining clearances for access to the system of trade in CO_2 emission units.