Raport kwartalny CERT.GOV.PL
kwiecień – czerwiec 2012

Rządowy Zespół Reagowania na Incydenty Komputerowe CERT.GOV.PL został powołany w dniu 1 lutego 2008 roku. Podstawowym zadaniem zespołu jest zapewnianie i rozwijanie zdolności jednostek organizacyjnych administracji publicznej Rzeczypospolitej Polskiej do ochrony przed cyberzagrożeniami, ze szczególnym uwzględnieniem ataków ukierunkowanych na infrastrukturę obejmującą systemy i sieci teleinformatyczne, których zniszczenie lub zakłócenie może stanowić zagrożenie dla życia, zdrowia ludzi, dziedzictwa narodowego oraz środowiska w znacznych rozmiarach, albo spowodować poważne straty materialne, a także zakłócić funkcjonowanie państwa.

Do zakresu świadczonych przez CERT.GOV.PL usług należy:

- koordynacja reagowania na incydenty,
- publikacja alertów i ostrzeżeń,
- obsługa i analiza incydentów (w tym gromadzenie dowodów realizowane przez zespół biegłych sądowych),
- publikacja powiadomień (biuletynów zabezpieczeń),
- koordynacja reagowania na luki w zabezpieczeniach,
- obsługa zdarzeń w sieciach objętych ochroną przez system ARAKIS-GOV,
- przeprowadzanie testów bezpieczeństwa.

Dane kontaktowe:

- E-mail: cert@cert.gov.pl
- Telefon: +48 22 58 56 152 +48 22 58 56 176
- Fax: +48 22 58 56 099

Dodatkowe informacje na temat zespołu dostępne są na witrynie www.cert.gov.pl.

W drugim kwartale 2012 roku miały miejsce incydenty związane przede wszystkim z ujawnianiem typowych podatności w zakresie bezpieczeństwa teleinformatycznego administracji państwowej. Nie odnotowano incydentów naruszających w znacznej mierze dostępności zasobów centralnych i naczelnych organów administracji państwowej. Zespół CERT.GOV.PL udzielał na bieżąco wsparcia podmiotom administracji państwowej pokrzywdzonym w toku zaistniałych incydentów wraz z zaleceniami.

Dużym wydarzeniem, również w cyberprzestrzeni, były Mistrzostwa Europy w Piłce Nożnej UEFA EURO 2012, współorganizowane przez Polskę. Rządowy Zespół Reagowania na Incydenty Komputerowe aktywnie uczestniczył w obszarze cyberbezpieczeństwa zarówno w organizacji jak również i zapewnieniu prawidłowego przebiegu Mistrzostw.

Więcej informacji dotyczących działań CERT.GOV.PL w zakresie bezpieczeństwa Mistrzostw Europy w Piłce Nożnej EURO 2012 znajduje się w załączniku technicznym niniejszego Raportu.

W minionym kwartale Zespół CERT.GOV.PL w dalszym ciągu odnotowywał dużą ilość incydentów bezpieczeństwa teleinformatycznego polegających na podmianie treści witryn internetowych oraz upublicznieniu informacji pochodzących z baz danych serwerów należących do administracji państwowej. Na początku drugiego kwartału wyraźną rolę odgrywały również działania przeprowadzane przez ruchy hacktywistyczne np.: „FuckGovFriday".

Dokładne informacje dotyczące ataków odnotowanych przez Rządowy Zespół Reagowania na Incydenty Komputerowe CERT.GOV.PL przedstawione zostały w rozdziale „Istotne ataki odnotowane przez Rządowy Zespół Reagowania na Incydenty Komputerowe CERT.GOV.PL" w załączniku technicznym do Raportu.

Nadzorowany, przez zespół CERT.GOV.PL, system ARAKIS-GOV w drugim kwartale 2012 wygenerował następujące typy alarmów:

- informacyjne[1] - 55%,
- o priorytecie średnim[2] - 23%,
- o priorytecie wysokim – 8%,
- diagnostyczne i testowe - 14%.

W wyniku analizy zarejestrowanych połączeń stwierdzono, iż w większości źródłem ataku były kraje takie jak Chiny i Polska. Jednocześnie ARAKIS-GOV wykazał wzrost aktywności ruchu sieciowego związanego z przepływem pakietów µTorrent.

Pełne dane w tym zakresie oraz pozostałe informacje o statystykach ARAKIS-GOV znajdują się w rozdziale „Statystyki systemu ARAKIS-GOV" w załączniku technicznym do Raportu.

W przypadku incydentów komputerowych analizowanych przez Zespół CERT.GOV.PL, drugi kwartał charakteryzował się stosunkowo dużą ilością przesyłanych zgłoszeń, i co za tym idzie dużą liczbą faktycznych incydentów. Należy tu jednak podkreślić, że omawiane wartości były nieznacznie niższe, niż zarejestrowane w rekordowo wysokim pierwszym kwartale 2012 roku.

W tym kwartale CERT.GOV.PL zarejestrował 364 zgłoszenia, z których 109 zostało zakwalifikowane jako faktyczne incydenty.

Ponadto początek II kwartału to duża liczba incydentów rozwiązanych. Wynika

[1] Alarmy informacyjne – nie informują o bezpośrednich zagrożeniach, a jedynie np. o czynnościach administracyjnych, które wymagają weryfikacji

[2] Alarmy o stanie średnim i wysokim informują o faktycznym zagrożeniu lub ataku

to w głównej mierze z dużej ilości zarejestrowanych incydentów w I kwartale 2012 roku związanych ze zjawiskiem tzw. „hacktywizmu".

Analizując kategorie incydentów można stwierdzić, że nadal bardzo powszechne są tradycyjne skanowania działających usług, bądź identyfikacja podatności oraz włamania do aplikacji typu WEB i po raz kolejny wiadomości typu SPAM. Warto odnotować, że relatywnie często zgłaszane są incydenty związane z oprogramowaniem szpiegowskim, typu Koń Trojański.

Szczegółowe informacje dotyczące statystyk zgłoszonych incydentów znajdują się w rozdziale „Statystyki incydentów" w załączniku technicznym do Raportu.

Na stronie internetowej Rządowego Zespołu Reagowania na Incydenty Komputerowe http://www.cert.gov.pl publikowane są stale specjalistyczne informacje o istotnych zagrożeniach, podatnościach oraz aktualizacjach w popularnych i najczęściej wykorzystywanych w administracji publicznej systemach i aplikacjach. Ponadto na witrynie zawarto informacje o najpopularniejszych formach ataków sieciowych oraz sposobach przeciwdziałania i neutralizowania ich skutków w formie zrozumiałej zarówno przez administratorów jak i użytkowników. Dodatkowo umieszczane są na bieżąco biuletyny bezpieczeństwa udostępnione przez producentów sprzętu i oprogramowania. Zawierają one w szczególności omówienie ostatnio wykrytych luk w bezpieczeństwie ich produktów oraz metody neutralizacji potencjalnych zagrożeń.

Specjalistyczne informacje opublikowane na witrynie www.cert.gov.pl w drugim kwartale 2012 roku to:

- 15 publikacji w kategorii „Poprawki i aktualizacje",
- 1 publikacja w kategorii „Zagrożenia i podatności",
- 3 publikacje w kategorii „Wiadomości ogólne".

Lista publikacji znajduje się w rozdziale „Istotne podatności, zagrożenia i biuletyny zabezpieczeń" w załączniku technicznym do Raportu.

W rozdziale „Testy bezpieczeństwa witryn WWW instytucji państwowych", w załączniku technicznym do Raportu zostały umieszczone informacje związane z realizowanym przez CERT.GOV.PL programem sukcesywnego badania stanu zabezpieczeń witryn internetowych należących do instytucji administracji publicznej. Działania te umożliwiają określenie poziomu bezpieczeństwa aplikacji WWW instytucji publicznych, a także usunięcie wykrytych nieprawidłowości. W drugim kwartale 2012 roku stwierdzono ogółem 213 błędów w tym:

- 31 błędy o bardzo wysokim poziomie zagrożenia[3],
- 45 błędów o wysokim poziomie zagrożenia,
- 86 błędy o niskim poziomie zagrożenia
- 51 błędów oznaczonych jako informacyjne.

Drugi kwartał 2012 roku przyniósł gwałtowny skok pozycji Polski w rankingu systemu ATLAS (Active Threat Level Analysis System – System Analizy Zagrożeń Internetowych obejmujący cały światowy Internet). Wyraźnie widać, iż pozycja zależy przede wszystkim od ilości URL-i phishingowych[4]. Gwałtowna zmiana w drugiej połowie maja była spowodowana przede wszystkim pełną publikacją informacji na temat luk w „PHP Address Book 7.0.0"

[3] Błędy o bardzo wysokiego poziomie zagrożenia mogą skutkować atakiem na strony który może przeprowadzić internauta bez specjalistycznej wiedzy, przy pomocy gotowego, dostępnego w sieci oprogramowania

[4] witryn wyłudzających informacje

oraz „PHP Volunteer Management System v 1.0.2”. Wykorzystanie tych podatności pozwalało między innymi na umieszczenie na atakowanej witrynie dowolnego pliku (np. pełnego systemu pozwalającego na zdalną kontrolę serwera). Opublikowano również gotowe skrypty mogące posłużyć do ataku na systemy wykorzystując wykryte podatności.

Sytuacja związana z wysoką ilością URL-i phishingowych dowodzi, że w polskiej cyberprzestrzeni pozostaje nadal znaczna liczba niewłaściwie zabezpieczonych serwerów WWW umożliwiając propagację „złych” witryn zagnieżdżonych w strukturze strony bez zmiany jej zawartości.

Ataki dominujące w II kwartale związane były głównie z usługami PHP oraz podatnościami typu „przepełnienie bufora” w Microsoft ASN.1 Library.

Drugi kwartał to przede wszystkim skanowania związane z aktywnością usług Microsoft-DS Active Directory na porcie 445 oraz usługi Microsoft SQL Server na porcie 1433. Standardowo także występowały skanowania związane z usługą http na porcie 80. Więcej informacji umieszczono w rozdziale „Informacje z systemów zewnętrznych - ATLAS” w załączniku technicznym do Raportu.

Pomimo wstępnego spadku pozycji Polski, w połowie kwartału zarejestrowano ponowny skok pod względem aktywności w wysyłce niechcianych przesyłek e-mailowych. Widać wyraźną korelację ze statystykami z systemu ATLAS. Jest to spowodowane tym, iż część przejętych systemów służy nie tylko do działań pasywnych (strony wyłudzające) lecz również aktywnych (spam i phishing e-mailowy).

Należy pamiętać, iż wszystkie działania aktywne są o wiele łatwiej zauważalne, przez co wiążą się z szybszymi zgłoszeniami incydentów, co prowadzi w rezultacie do szybszej likwidacji zagrożenia. Spadek pozycji Polski, wskazuje na to, iż działania zespołów bezpieczeństwa były pod tym względem skuteczne i aktualnie inne kraje wyprzedziły Polskę w tym obszarze, przez co w końcowym okresie raportowania przestała być ona klasyfikowana.

Rozkład pozycji Polski w funkcji czasu znajduje się w rozdziale „Informacje z innych systemów zewnętrznych” w załączniku technicznym do Raportu.

W drugim kwartale została rozpoczęta, pierwsza tego typu w Polsce, analiza stron administracji państwowej przeprowadzana przez zespół CERT.GOV.PL we współpracy z organami państwowymi w zakresie identyfikacji spełniania określonych zaleceń związanych z zapewnieniem dostępności, integralności oraz poufności witryn w domenie gov.pl.

Na podstawie przygotowanej przez Zespół CERT.GOV.PL, a następnie wypełnionej przez instytucje państwowe ankiety, uzyskano przekrojowy obraz bezpieczeństwa witryn internetowych w domenie gov.pl pozwalający na określenie kierunku działań w zakresie zwiększenia bezpieczeństwa teleinformatycznego usług instytucji. Należy wspomnieć tutaj, że przeanalizowano nadesłane wyniki obejmujące 400 witryn należących do 55 podmiotów administracji. Informacje w tym zakresie i wyniki analizy zostały umieszczone w rozdziale „Informacja na temat stanu bezpieczeństwa witryn internetowych GOV.PL” w załączniku technicznym do Raportu.

ZAŁĄCZNIK TECHNICZNY DO RAPORTU KWARTALNEGO CERT.GOV.PL KWIECIEŃ – CZERWIEC 2012

Spis treści

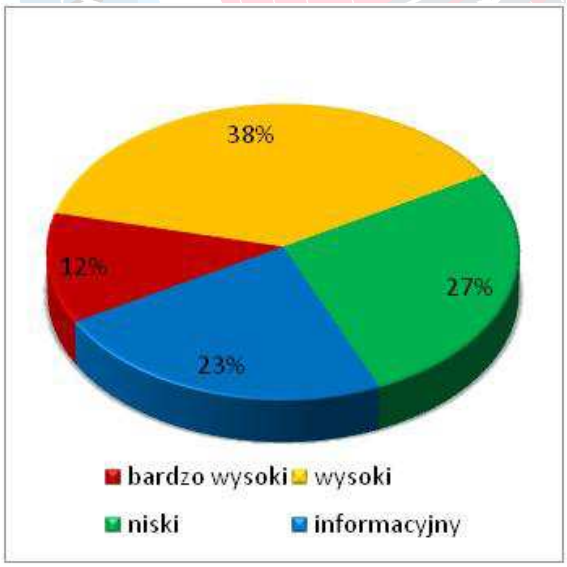
1 Działania CERT.GOV.PL w zakresie bezpieczeństwa Mistrzostw Europy w Piłce Nożnej EURO 2012

Rządowy Zespół Reagowania na Incydenty Komputerowe CERT.GOV.PL brał czynny udział w organizacji oraz w zapewnieniu prawidłowego przebiegu Mistrzostw Europy w Piłce Nożnej EURO 2012 w cyberprzestrzeni. Prowadzono liczne działania zmierzające do zapewnienia bezpieczeństwa teleinformatycznego w zakresie m.in. koordynacji reagowania na incydenty komputerowe oraz obsługi zdarzeń w sieciach instytucji odpowiedzialnych za prawidłowy przebieg Mistrzostw.

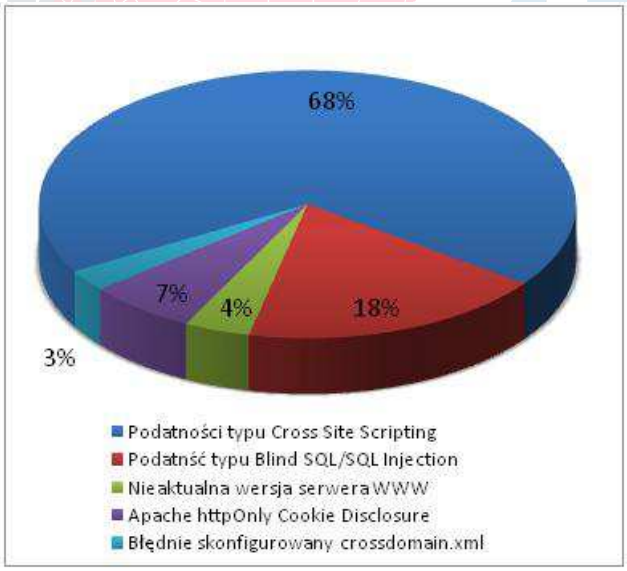
1.1 Działania podejmowane przed rozpoczęciem mistrzostw

W związku z coraz częstszym ujawnianiem błędów zabezpieczeń witryn internetowych, skutkujących włamaniami oraz nieautoryzowanymi zmianami zawartości publikowanych treści CERT.GOV.PL zwrócił się z propozycją przeprowadzenia testów bezpieczeństwa kluczowych stron WWW na UEFA EURO 2012.

Przetestowano 10 witryn. Stwierdzono ogółem 108 błędów w tym: 13 błędów o bardzo wysokim poziomie zagrożenia, 41 błędów o wysokim poziomie zagrożenia, 29 błędów o niskim poziomie zagrożenia i 25 błędów informacyjnych. Wszystkie z badanych stron posiadały podatności o wysokim poziomie zagrożenia.



Rysunek 1-1 Statystyka wykrytych podatności



Rysunek 1-2 Procentowy rozkład najpoważniejszych błędów

1.2 Działania podejmowane w trakcie przebiegu mistrzostw

W trakcie Mistrzostw Europy w Piłce Nożnej EURO 2012 od 8 czerwca do 1 lipca 2012 roku, Rządowy Zespół Reagowania na Incydenty Komputerowe CERT.GOV.PL prowadził w trybie zmia-

nowym stały monitoring polskiej przestrzeni adresowej administracji RP, a także witryn bezpośrednio związanych z tematyką Mistrzostw.

Zespół CERT.GOV.PL, pełniąc funkcję między innymi organu doradczego w zakresie zapewnienia bezpieczeństwa teleinformatycznego w trakcie EURO 2012, zorganizował całodobowy punkt kontaktowy dla administratorów systemów i sieci TI.

W ramach prowadzonych czynności, analizowano podejrzane przesyłki mailowe pod kątem ewentualnych ataków ukierunkowanych. Ponadto, wykryto i przekazano do wiadomości zainteresowanych instytucji informacje o próbach połączeń wykonywanych z komputerów mogących być elementami tzw. sieci botnet – komputerów zombie.

2 Istotne ataki odnotowane przez Rządowy Zespół Reagowania na Incydenty Komputerowe CERT.GOV.PL

2.1 Ataki na witryny internetowe administracji publicznej

W drugim kwartale 2012 roku odnotowana została znacząca ilość ataków mających na celu podmianę zawartości strony głównej. Pomimo działań prowadzonych przez Rządowy Zespół Reagowania na Incydenty Komputerowe CERT.GOV.PL niestety w dalszym ciągu poziom bezpieczeństwa wielu witryn jest niezadowalający.

2.1.1 Kwiecień

Na przełomie marca oraz kwietnia 2012 roku miały miejsce działania, grup występujących jako Anonymous, o nazwie „FuckGovFriday". W ich wyniku podmienionych zostało kilka witryn internetowych należących do administracji państwowej oraz upublicznione zostały informacje pobrane z baz danych serwerów.

Lista stron, których zawartość została podmieniona:

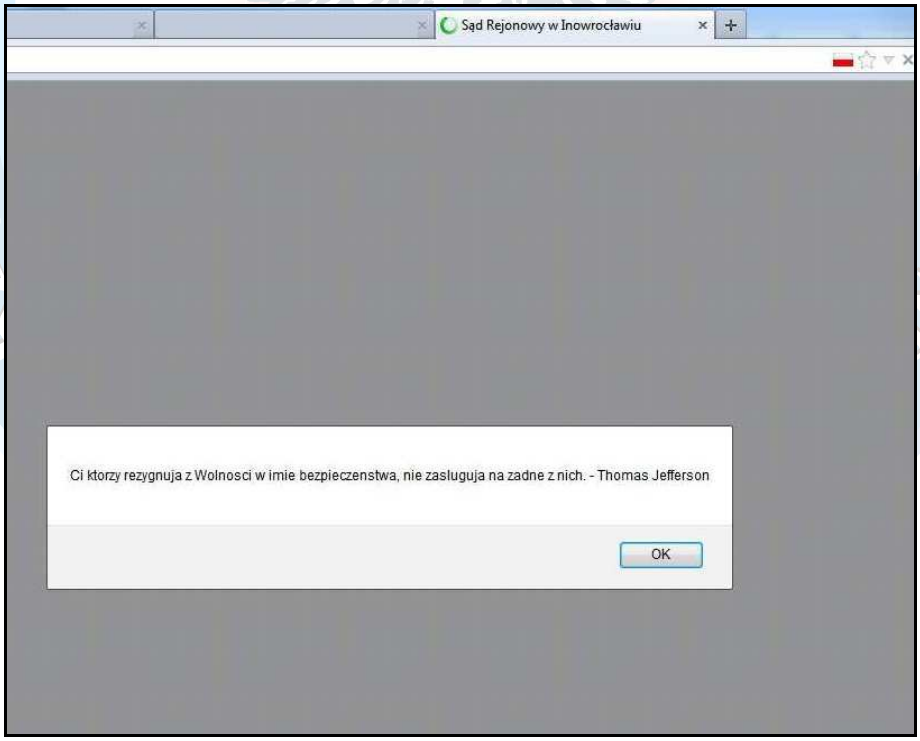
- mogilno.sr.gov.pl
- tuchola.sr.gov.pl
- bydgoszcz.sr.gov.pl
- naklo.sr.gov.pl
- szubin.sr.gov.pl
- inowroclaw.sr.gov.pl
- poznan.po.gov.pl
- bialystok.pa.gov.pl
- nfz.gov.pl

Lista stron, z których dane zostały upublicznione:

- bialystok.pa.gov.pl
- ngo.czestochowa.um.gov.pl
- poznan.po.gov.pl
- szubin.sr.gov.pl
- inowroclaw.sr.gov.pl

W każdym z powyższych przypadków administratorzy witryn oraz osoby, których dane zostały upublicznione zostali poinformowani o incydentach oraz poinstruowani odnośnie sposobów minimalizacji ich skutków.

Rysunek 2-1: Wygląd podmienionej witryny Sądu Rejonowego w Bydgoszczy



Rysunek 2-2: Wygląd podmienionej witryny Sądu Rejonowego w Inowrocławiu

2.1.2 Maj

Na początku maja 2012 roku miało miejsce upublicznienie na jednym z portali internetowych bazy danych użytkowników (imię, nazwisko, email oraz skrót „*hash*" hasła) pochodzących ze strony Głównego Inspektoratu Sanitarnego.

W dniu 11 maja miała miejsce podmiana dwóch witryn internetowych należących do administracji państwowej:

- Agencji Rynku Rolnego http://www.arr.gov.pl,
- Ministerstwa Edukacji Narodowej http://www.men.gov.pl.

Atak został dokonany poprzez wykorzystanie luki występującej w systemie zarządzania treścią Joomla. Poniżej przedstawiony został wygląd podmienionych stron.

Rysunek 2-3: Wygląd podmienionych stron arr.gov.pl oraz men.gov.pl

W dniu 20.05 2012 roku miała miejsce podmiana witryny Centralnej Komisji Egzaminacyjnej. Włamania dokonano poprzez występujący na stronie błąd typu SQL Injection. Dane autoryzacyjne (login oraz hasło) do panelu zarządzającego treścią strony upublicznione zostały na jednej ze stron internetowych. Na witrynie www.cke.gov.pl zamieszczone zostały wulgarne filmy, zdjęcia ośmieszające system edukacji oraz papieża Jana Pawła II. Poniżej znajduje się wygląd podmienionej strony Centralnej Komisji Egzaminacyjnej.

Rysunek 2-4: Wygląd podmienionej witryny Centralnej Komisji Egzaminacyjnej

2.1.3 Czerwiec

W dniu 14 czerwca 2012 roku miała miejsce podmiana witryny Instytutu Biologii Doświadczalnej im. M. Nenckiego w Warszawie http://neurogene.nencki.gov.pl. Poniżej przedstawiony został wygląd podmienionej strony.

Rysunek 2-5: Wygląd podmienionej witryny Instytutu Biologii Doświadczalnej im. M. Nenckiego w Warszawie

W dniu 22 czerwca 2012 roku miała miejsce podmiana strony należącej do Zespołu Szkół Sportowych w Dąbrowie Górniczej http://www.zssdg.edu.pl/. Poniżej przedstawiony został wygląd podmienionej strony.

Rysunek 2-6: Wygląd podmienionej witryny Zespołu Szkół Sportowych w Dąbrowie Górniczej

2.2 Inne ważne incydenty zarejestrowane przez Rządowy Zespół Reagowania na Incydenty Komputerowe CERT.GOV.PL

Poza wymienionymi powyżej, w drugim kwartale 2012 roku Rządowy Zespół Reagowania na Incydenty Komputerowe CERT.GOV.PL obsługiwał zgłoszenia, które dotyczyły między innymi:

- rozsyłania zainfekowanych załączników użytkownikom poczty elektronicznej urzędów administracji centralnej. Należy zauważyć, że zaobserwowano także tendencję dotycząca pojawiania się korespondencji elektronicznej pochodzącej od nadawców podszywających się pod pracowników instytucji Unii Europejskiej, posługujących się m.in. adresami wskazującymi na Komisję Europejską tj. domeny ec.europa.eu. Korespondencja wskazująca na tego typu nadawców zawierała zainfekowane załączniki do poczty elektronicznej w formacie „*.doc” wykorzystujące jedną z podatności pakietu Microsoft Office opisaną jako MS Office CVE-2012-0158 opisaną na stronie http://technet.microsoft.com/pl-pl/security/bulletin/ms12-027. Przedmiotowa podatność była krytyczna dla pakietu Microsoft Office i umożliwia zdalne wykonanie kodu. W wyniku właściwej reakcji zespołu CERT.GOV.PL oraz współpracy administratorów nie doszło do infekcji stacji roboczych,

- błędów SQL Injection na witrynie szczepienia.info oraz witrynie Serwisu Urzędów Pracy. Błędy związane były z brakiem właściwej walidacji danych wprowadzanych poprzez stronę do formularza oraz ustawieniami domyślnymi zastosowanymi w konfiguracji silnika PHP,

- błędów PHP/SQL występujących na stronie Sądu Rejonowego w Nowym Dworze Mazowieckim,

- podatności XSS występujących na witrynach ewidencja.archiwa.gov.pl oraz Rządowe Wrota Celne – http://celina.krakow.uc.gov.pl,

- publikacji baz danych użytkowników pochodzących z witryn należących do administracji państwowej na portalach internetowych. Administratorzy oraz osoby, których dane udostępniono, zostali o tym fakcie poinformowani oraz poinstruowani o sposobie minimalizacji zagrożenia,

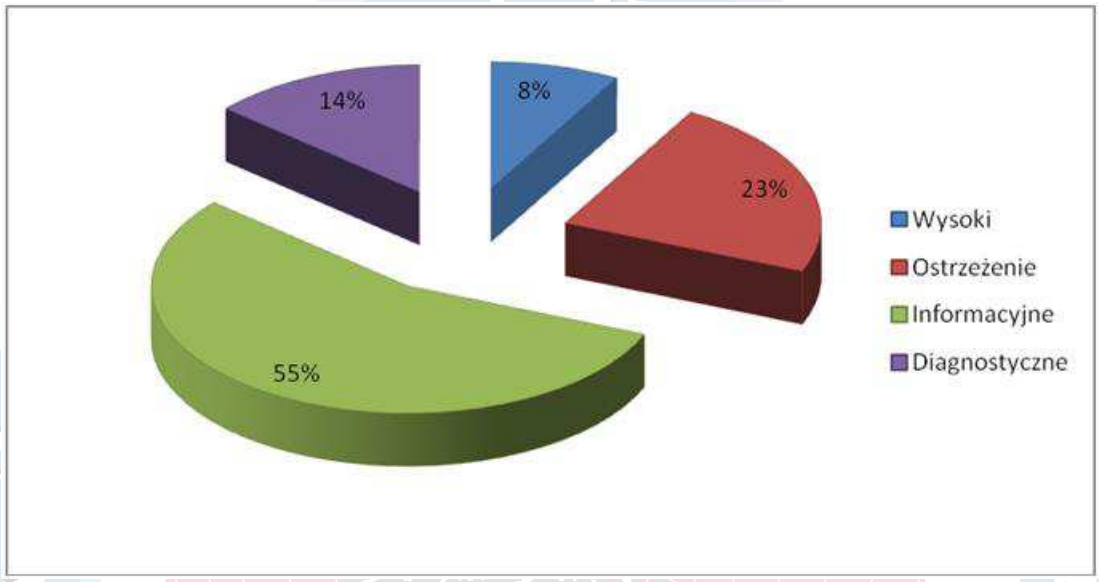
- komputerów „zombie" przynależących do bonetów:
  - Kelihos.B,
  - Rustock,

  oraz infekcji oprogramowaniem złośliwym m. in.:
  - ZEUS,
  - Slenfbot,
  - Dnschanger,
  - Ramnit.

  W rezultacie obsługi incydentów, zidentyfikowano skompromitowane hosty i dokonano dezaktywacji złośliwego oprogramowania.

3 Statystyki systemu ARAKIS-GOV[5]

W drugim kwartale 2012 roku, podobnie jak to miało miejsce w poprzednich kwartałach, niezmiennie zdecydowaną większość stanowiły alarmy informacyjne. Stanowiły one 55 procent wszystkich zarejestrowanych przez system ARAKIS-GOV. Alarmy o priorytecie średnim stanowiły 23%, natomiast alarmy diagnostyczne 14%. System zgłosił najmniej alarmów o priorytecie wysokim – 323, co stanowiło 8% wszystkich alarmów.



Rysunek 3-1: Procentowy rozkład ważności alarmów

Wśród alarmów o priorytecie wysokim zaobserwowano 305 alarmów typu INFHOST_HN[6], 4 alarmów typu INFHOST_BH[7] oraz 14 alarmów typu INFHOST_FW[8]. Nie odnotowano alarmów typu VIRUS_FOUND[9] i NWORM[10].

[5] ARAKIS-GOV jest pasywnym systemem wczesnego ostrzegania o zagrożeniach w sieci Internet. W chwili obecnej zostały wdrożone 74 sądy głownie w instytucjach państwowych.

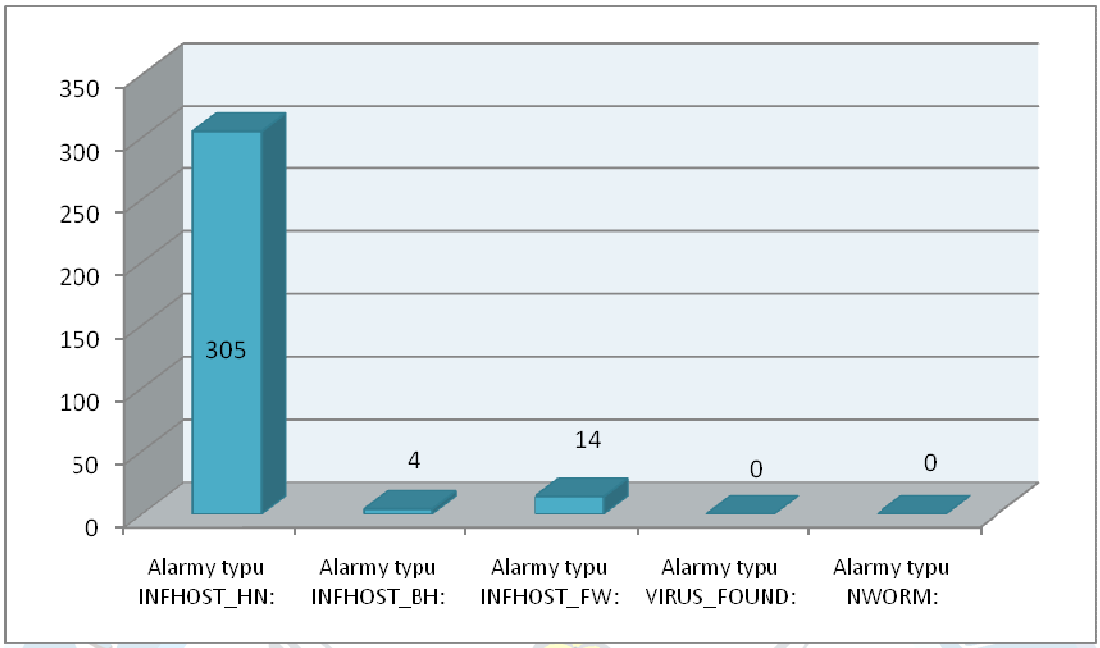
[6] Alarm INFHOST_HN oznacza potencjalne wykrycie zainfekowanego hosta w sieci wewnętrznej instytucji chronionej systemem ARAKIS-GOV. Alarm ten generowany jest na podstawie analizy danych z systemów typu honeypot.

[7] Alarm INFHOST_BH oznacza wykrycie połączenia z domeną, która oznaczona została jako złośliwa tzn. przy pomocy której propagowane jest oprogramowanie złośliwe.

[8] Alarm INFHOST_FW oznacza potencjalne wykrycie zainfekowanego hosta w sieci wewnętrznej instytucji chronionej systemem ARAKIS-GOV. Alarm ten generowany jest na podstawie analizy logów systemów zaporowych.

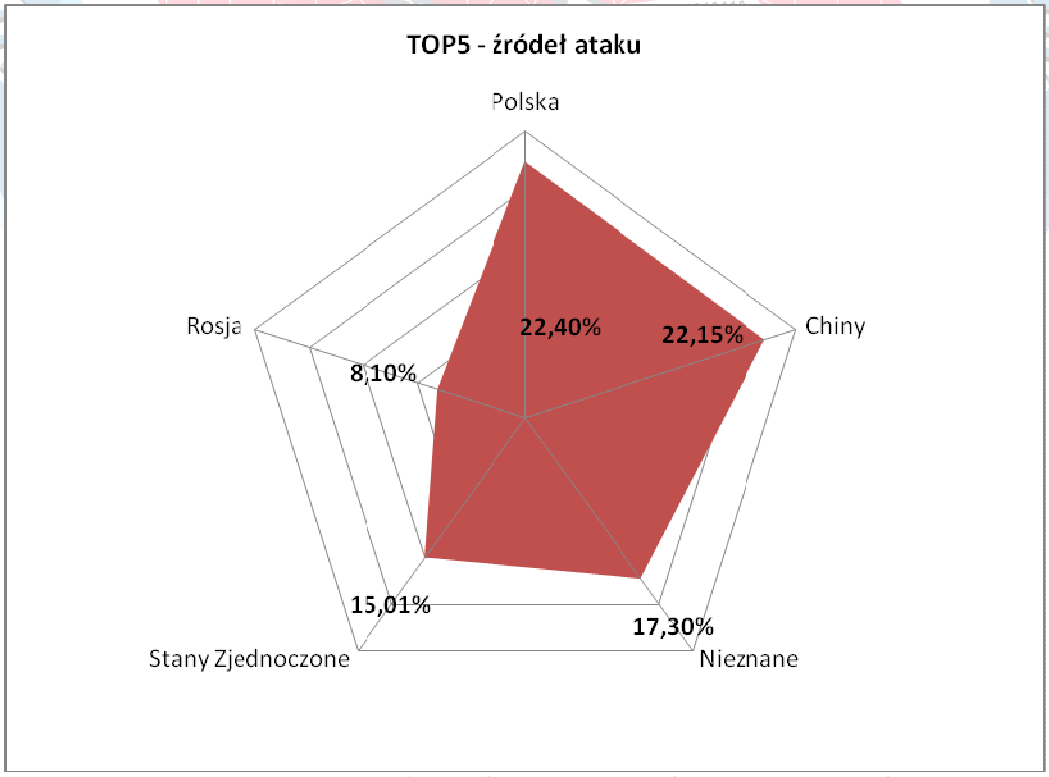
[9] Alarm VIRUS_FOUND oznacza wykrycie infekcji wirusowej w sieci wewnętrznej chronionej instytucji. Alarm ten generowany jest na podstawie informacji pochodzących ze skanerów antywirusowych serwerów pocztowych

[10] Alarm NWORM oznacza potencjalne wykrycie nowego, szybko rozprzestrzeniającego się zagrożenia sieciowego (robaka sieciowego) – w tym przypadku wszystkie 3 alarmy były alarmami fałszywymi (false-positive)



Rysunek 3-2: Statystyki alarmów o wysokim priorytecie.

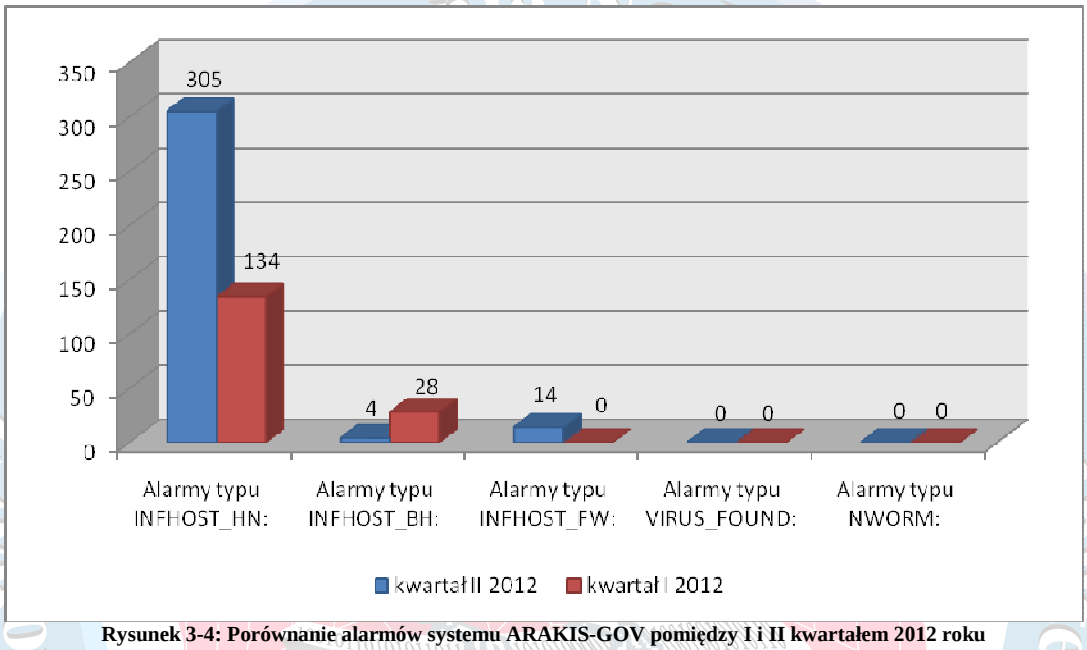
W wyniku analizy zarejestrowanych połączeń stwierdzono, iż w większości źródłem ataku były sieci komputerowe przypisane do Polski, Chin, Stanów Zjednoczonych i Rosji. W statystykach liczny udział miały też połączenia, których adresy źródłowe zostały zidentyfikowane jako „Nieznane", co spowodowane jest brakiem przypisania adresu do podmiotu w bazie RIPE. Sytuacja taka ma najczęściej miejsce w przypadku podszywania się pod adresy IP.



Rysunek 3-3: Rozkład geograficzny źródeł wykrytych ataków (wg liczby przepływów)

Należy pamiętać, że specyfika protokołu TCP/IP, powoduje, że nie można bezpośrednio łączyć źródła pochodzenia pakietów z faktyczną lokalizacją wykonawcy ataku. Wynika to z faktu, iż w celu ukrycia swej tożsamości i fizycznej lokalizacji atakujący wykorzystują serwery pośredniczące (proxy) lub słabo zabezpieczone komputery, nad którymi wcześniej przejmują kontrolę.

W drugim kwartale zaobserwowano wzrost liczby alarmów o wysokim poziomie istotności typu INFHOST_HN w stosunku do pierwszego kwartału 2012 roku. Poniżej przedstawiony został wykres porównawczy alarmów o priorytecie wysokim.



Rysunek 3-4: Porównanie alarmów systemu ARAKIS-GOV pomiędzy I i II kwartałem 2012 roku

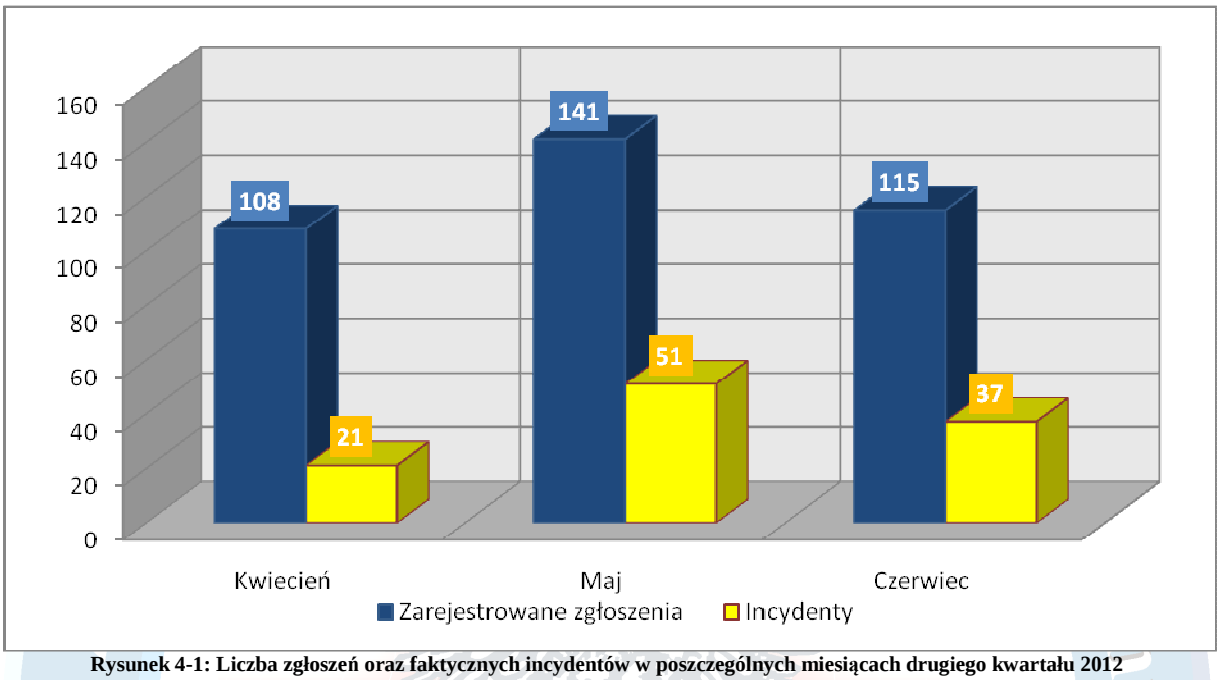
Sytuacja taka związana jest z zarejestrowanym zjawiskiem przez system ARAKIS-GOV dotyczącym wzrostu aktywności w sieci µTorrent. Na podstawie analizy danych odnotowanych w alertach informujących o możliwej infekcji chronionych węzłów stwierdzono, iż adresy IP zawarte w pakietach połączeń były spoofowane ze względu na fakt, iż wskazywały na zainicjowanie połączenia pomiędzy dwoma składnikami systemu ARAKIS-GOV rozlokowanymi w dwóch różnych instytucjach chronionych systemem. Powyższa sytuacja jest z punktu widzenia budowy systemu niemożliwa, gdyż sondy systemu nie generują same z siebie ruchu a jedynie odpowiadają na zainicjowane połączenie zewnętrzne.

Prawdopodobną przyczyną zaobserwowanej aktywności przez system ARAKIS-GOV jest celowe zatruwanie sieci BitTorrent przez koncerny multimedialne w celu ochrony przed współdzieleniem plików multimedialnych (audio, wideo itp.) – ochrona praw autorskich. Jednakże należy wziąć pod uwagę fakt, iż powyższa teza jest tylko przypuszczeniem, prawdopodobnym jest również, iż widziany ruch jest próbą eksploitacji aplikacji klienckich µTorrent w celu przejęcia kontroli nad komputerem użytkownika.

Na chwilę obecną powyższa sytuacja traktowana jest jako anomalia w sieci zaobserwowana przez system ARAKIS-GOV i w dalszym ciągu będzie badana. Bardziej szczegółowa analiza techniczna anomalii została opracowana przez zespół CERT Polska i jest dostępna pod adresem: http://www.cert.pl/news/5365/langswitch_lang/pl.

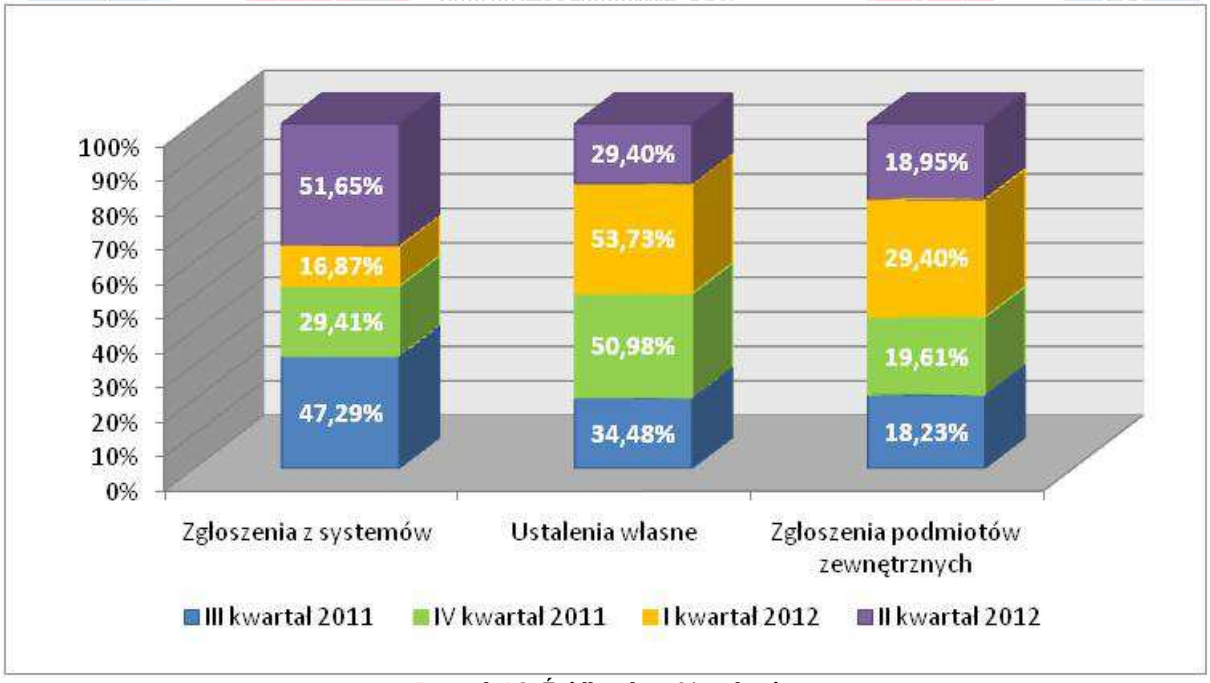
4 Statystyki incydentów

W drugim kwartale 2012 roku do zespołu CERT.GOV.PL wpłynęły 364 zgłoszenia, z których 109 zostało zakwalifikowanych jako incydenty.



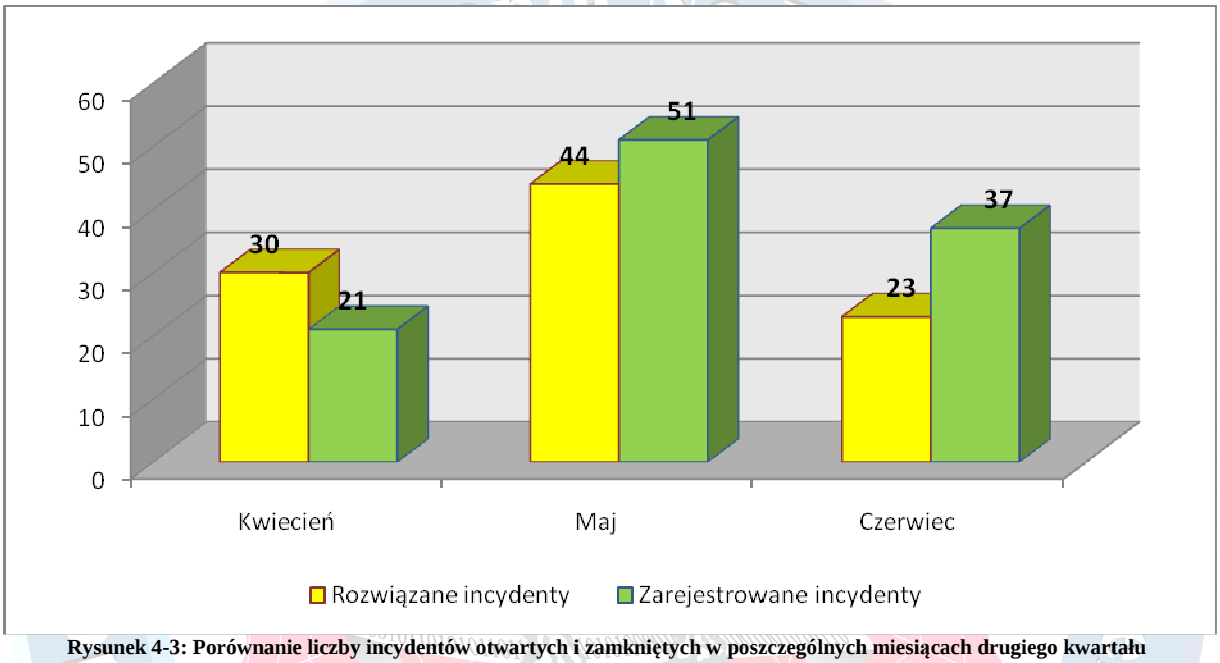
Rysunek 4-1: Liczba zgłoszeń oraz faktycznych incydentów w poszczególnych miesiącach drugiego kwartału 2012

Szczegółowe statystyki źródeł zgłoszeń incydentów trafiających do CERT.GOV.PL przedstawia poniższy wykres.



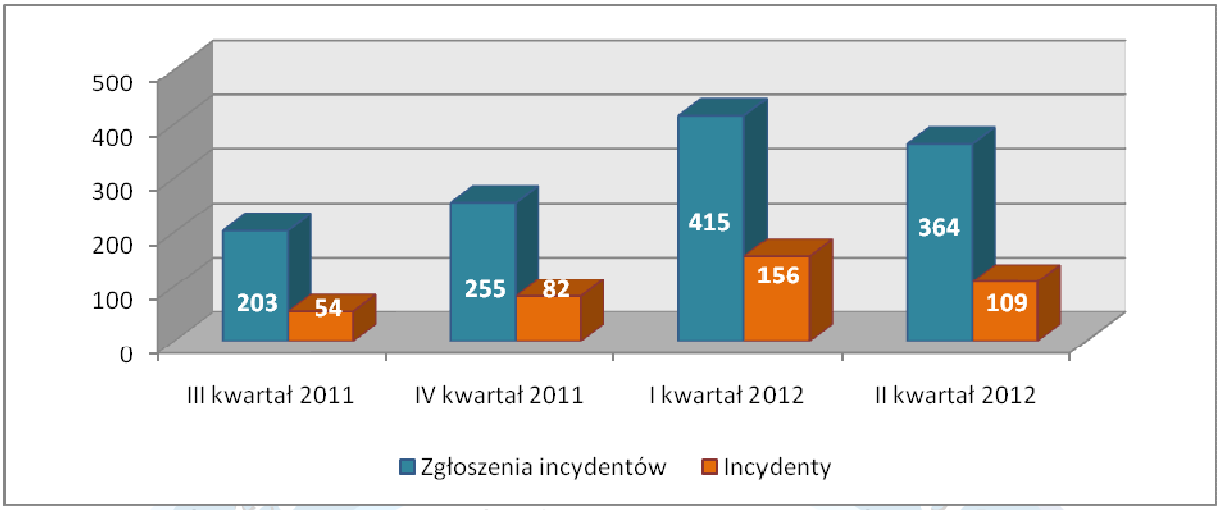
Rysunek 4-2: Źródła zgłoszeń incydentów

Rozkład miesięczny incydentów zarejestrowanych, jak i wszystkich rozwiązanych z drugiego kwartału 2012 roku przedstawia się następująco: w kwietniu 2012 roku zarejestrowano 21 incydentów, rozwiązano natomiast 30, w maju 2012 odnotowano 51 incydentów, a rozwiązano 44. W czerwcu natomiast przyjęto do realizacji 37 incydentów, zakończono zaś 23. Pozostałe incydenty są w trakcie dalszej analizy. Na uwagę zasługuje fakt, że kwiecień był miesiącem większej ilości incydentów zamkniętych, niż zarejestrowanych. Jest to wynikiem rozwiązywania incydentów jeszcze z początku roku i efekt protestów internetowych związanych z umową ACTA.



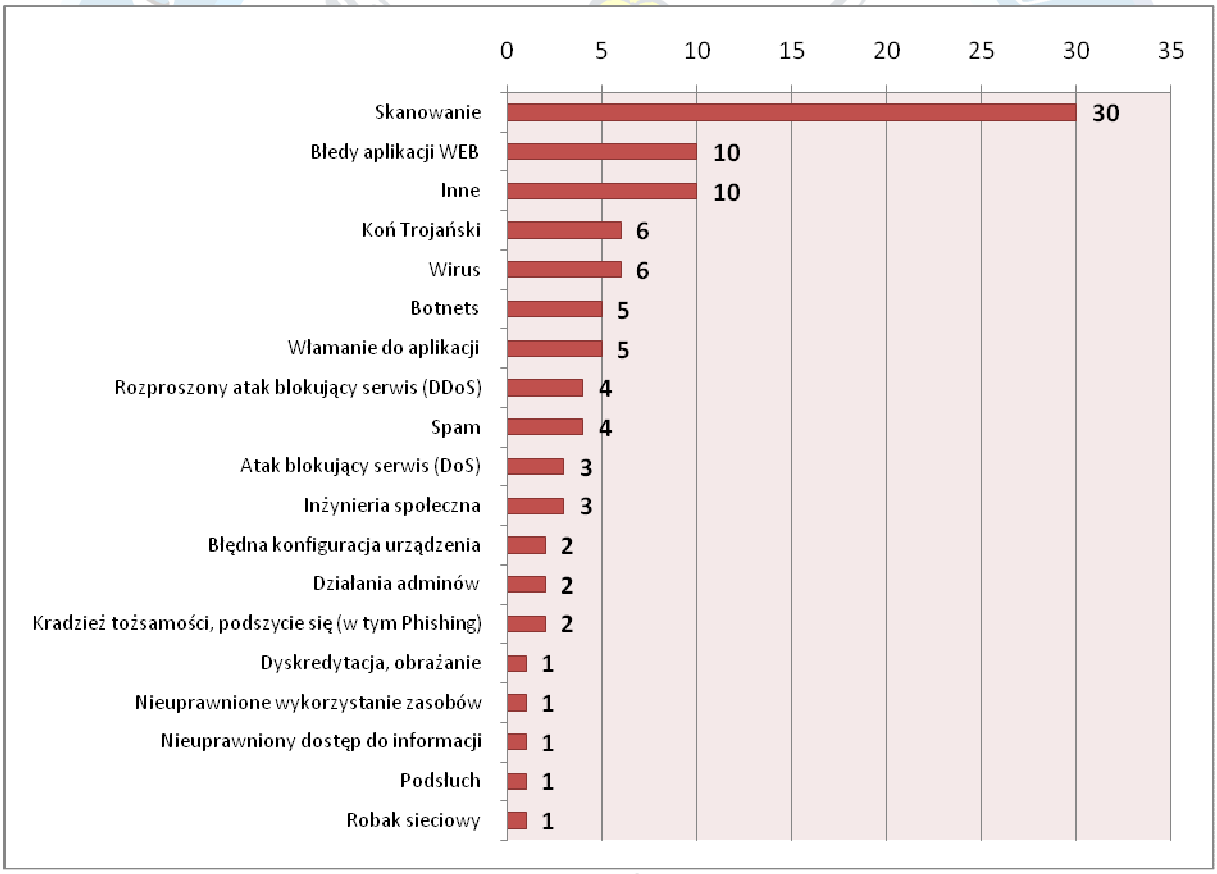
Rysunek 4-3: Porównanie liczby incydentów otwartych i zamkniętych w poszczególnych miesiącach drugiego kwartału

Wykres zaprezentowany poniżej obrazuje porównanie ilości zgłoszeń na tle faktycznych incydentów, rozpatrywanych kwartalnie na przestrzeni ostatnich dwunastu miesięcy. Na uwagę zasługuje fakt, że na początku 2012 roku zanotowano rekordowy wzrost ilości zgłoszeń, jak i samych incydentów. Drugi kwartał 2012 to już relatywnie mniejsza odnotowana liczba zgłoszeń oraz incydentów, jednakże i tak znacznie przewyższająca analogicznie wartości z poprzedniego roku.



Rysunek 4-4: Porównanie ilości zgłoszeń incydentów do faktyczne potwierdzonych incydentów w ostatnich czterech kwartałach

Podział zarejestrowanych incydentów na kategorie przedstawia się następująco:



Rysunek 4-5: Statystyka incydentów z podziałem na kategorie

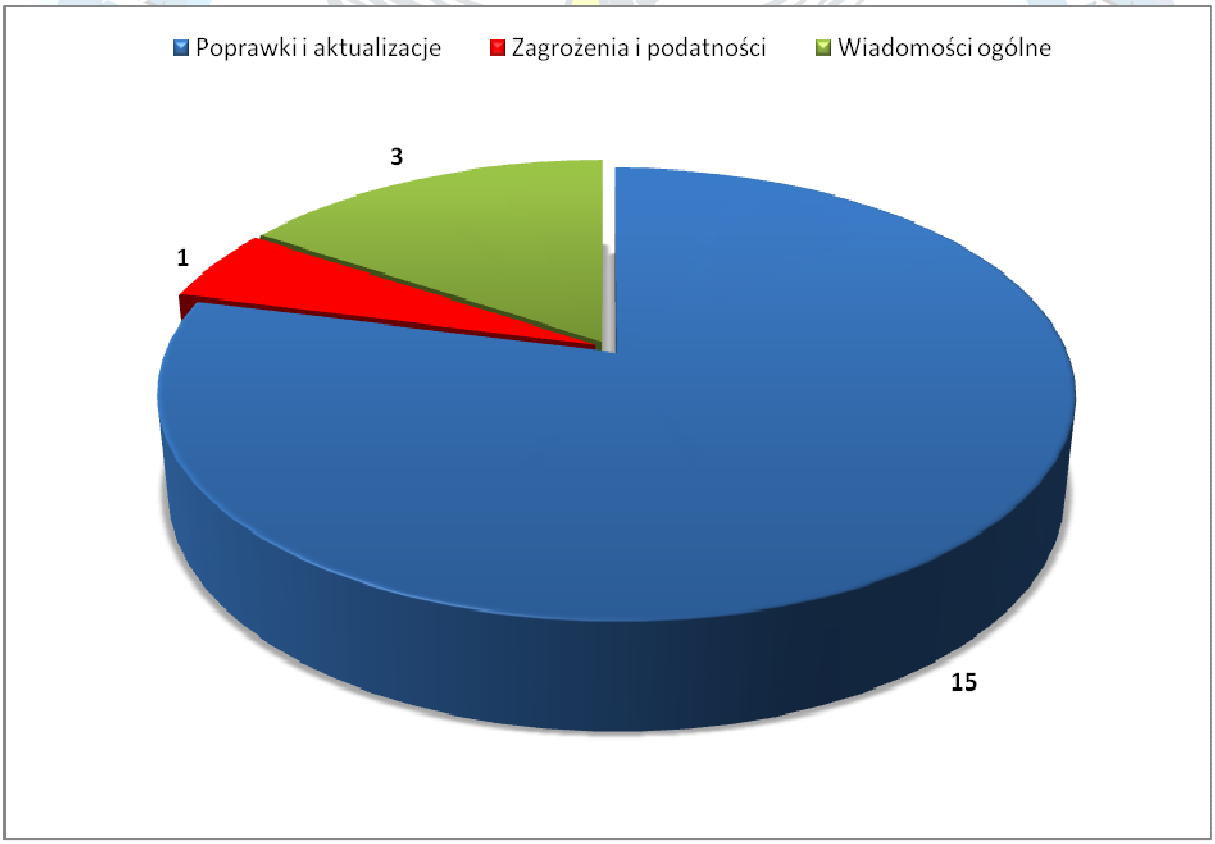
Analizując powyższy wykres, można stwierdzić, że zdecydowaną większość obsługiwanych incydentów stanowią tradycyjne skanowania w poszukiwaniu usług. „Popularne" są jak zwykle błędy w aplikacjach WEB, czy wiadomości typu SPAM. Również często rejestrowany były incydenty związane z oprogramowaniem szpiegowskim, typu Koń Trojański.

5 Istotne podatności, zagrożenia i biuletyny zabezpieczeń

Witryna http://www.cert.gov.pl stanowi, dla administratorów systemów, źródło specjalistycznych danych związanych z bezpieczeństwem teleinformatycznym. Publikowane są tam między innymi aktualne informacje o istotnych zagrożeniach, nowych podatnościach w popularnych systemach i aplikacjach, najpopularniejszych formach ataków sieciowych oraz sposobach ochrony. Dodatkowo na powyższej witrynie umieszczane są biuletyny bezpieczeństwa udostępnione przez producentów sprzętu i oprogramowania.

W drugim kwartale 2012 roku na witrynie www.cert.gov.pl umieszczono:

- 15 publikacji w kategorii „Poprawki i aktualizacje”,
- 1 publikację w kategorii „Zagrożenia i podatności”,
- 3 publikacje w kategorii „Wiadomości ogólne”.



Rysunek 5-1: Statystyka publikacji na stronie CERT.GOV.PL w II kwartale 2012 roku

5.1 Najistotniejsze publikacje dotyczące zagrożeń w II kwartale 2012 roku:

- **Adobe Security Bulletin**

Firma Adobe opublikowała aktualizację dla programów Adobe Reader oraz Acrobat łatającą wiele luk w zabezpieczeniach. Wykorzystanie tych podatności może pozwolić atakującemu na spowodowanie ataku typu odmowa usługi DoS lub wykonanie dowolnego kodu.

Podatne wersje:

- Adobe Reader X (10.1.2) oraz wersje wcześniejsze dla systemów Windows oraz Macintosh;
- Adobe Reader 9.4.6 oraz wersje wcześniejsze dla systemu Linux;
- Adobe Acrobat X (10.1.2) oraz wersje wcześniejsze dla systemów Windows and Macintosh.

- **Microsoft Security Bulletin 4/2012**

Firma Microsoft opublikowała w kwietniu biuletyn bezpieczeństwa informujący o usunięciu sześciu błędów w swoich produktach.

Biuletyny określone jako "krytyczne":

- MS12-023 – dotyczy zbiorczej aktualizacji zabezpieczeń dla oprogramowania Internet Explorer.
- MS12-024 – dotyczy podatności w zabezpieczeniach Microsoft Windows.
- MS12-025 – dotyczy błędów w zabezpieczeniach .NET Framework.
- MS12-027 – dotyczy podatności w Windows Common Control.

Biuletyny określone jako "ważne":

- MS12-026 – dotyczy podatności w zabezpieczeniach Microsoft Forefront UAG Server.
- MS12-028 – dotyczy błędów w oprogramowaniu Micosoft Office.

- **Flashback Malware Removal Tool od Apple**

Firma Apple udostępniła narzędzie do usuwania najpopularniejszych wariantów szkodliwego oprogramowania typu Flashback. Jeśli malware zostanie wykryty, narzędzie usunie szkodliwe oprogramowanie automatycznie a następnie powiadomi o tym fakcie użytkownika.

- **Oracle Critical Patch Update Kwiecień 2012**

Firma Oracle wydała kwietniowy Critical Patch Update zawierający 88 poprawek dla wielu swoich produktów. Luki występujące w niezaktualizowanych wersjach programów mogą pozwolić atakującemu na kradzież informacji, manipulowanie danymi czy przeprowadzenie ataku DoS.

Aktualizacja zawiera poprawki dla następujących produktów:

- 6 dla Oracle Database Server;
- 11 dla Oracle Fusion Middleware;
- 6 dla Oracle Enterprise Manager Grid Control;
- 4 dla Oracle E-Business Suite;
- 5 dla Oracle Supply Chain Product Suite;
- 15 dla Oracle PeopleSoft Products;
- 2 dla Oracle Industry Applications;
- 17 dla Oracle Financial Services Software;
- 1 dla Oracle Primavera Product Suite;
- 15 dla Oracle Sun Product Suite;
- 6 dla Oracle MySQL.

- **Biuletyn bezpieczeństwa Adobe Flash Player**

Firma Adobe opublikowała biuletyn bezpieczeństwa Adobe Security Bulletin APSB12-09 dotyczący podatności występujących w Adobe Flash Player. Wykorzystanie tych luk może pozwolić atakującemu na spowodowanie ataku DoS lub na przejęcie kontroli nad podatnym systemem.

Podatne wersje:

- Adobe Flash Player 11.2.202.233 i wersje wcześniejsze dla systemów Windows, Macintosh, Linux,
- Adobe Flash Player 11.1.115.7 i wersje wcześniejsze dla systemu Android 4.x,
- Adobe Flash Player 11.1.111.8 i wcześniejsze dla Android 3.x and 2.x.

- **Microsoft Security Bulletin 5/2012**

Firma Microsoft opublikowała w maju biuletyn bezpieczeństwa informujący o usunięciu siedmiu błędów w swoich produktach.

Biuletyny określone jako "krytyczne":

- MS12-029 – dotyczy błędów w zabezpieczeniach programu Microsoft Word.
- MS12-034 – dotyczy zbiorczej aktualizacji zabezpieczeń dla pakietu Microsoft Office.
- MS12-035 – dotyczy podatności w zabezpieczeniach systemu .NET Framework.

Biuletyny określone jako "ważne":

- MS12-030 – dotyczy luki w zabezpieczeniach pakietu Microsoft Office.
- MS12-031 – dotyczy błędów w zabezpieczeniach programu Microsoft Visio Viewer 2010.
- MS12-032 - dotyczy problemu w zabezpieczeniach stosu TCP/IP w systemie Windows.
- MS12-033 - dotyczy podatności w Menedżerze partycji systemu Windows.

- **Biuletyny Bezpieczeństwa Adobe**

Firma Adobe opublikowała biuletyny bezpieczeństwa dla programów Adobe Illustrator oraz Adobe Photoshop usuwające wiele luk w zabezpieczeniach. Wykorzystanie tych podatności może pozwolić atakującemu na przejęcie kontroli nad systemem użytkownika.

Podatne wersje:

- Adobe Illustrator CS5 (15.0.x) dla systemów Windows oraz Macintosh;
- Adobe Illustrator CS5.5 (15.1) dla systemów Windows oraz Macintosh;
- Adobe Photoshop CS5 (12.0) dla systemów Windows and Macintosh;
- Adobe Photoshop CS5.1 (12.1) dla systemów Windows and Macintosh.

- **Microsoft Security Bulletin 6/2012**

Firma Microsoft opublikowała w czerwcu biuletyn bezpieczeństwa informujący o usunięciu siedmiu błędów w swoich produktach.

Biuletyny określone jako "krytyczne":

- MS12-036 - dotyczy podatności Microsoft Windows w usłudze Remote Desktop Protocol.

- MS12-037 - dotyczy grupy krytycznych poprawek dla Internet Explorer.
- MS12-038 - dotyczy podatności w Microsoft .NET Framework.

Biuletyny określone jako "ważne":

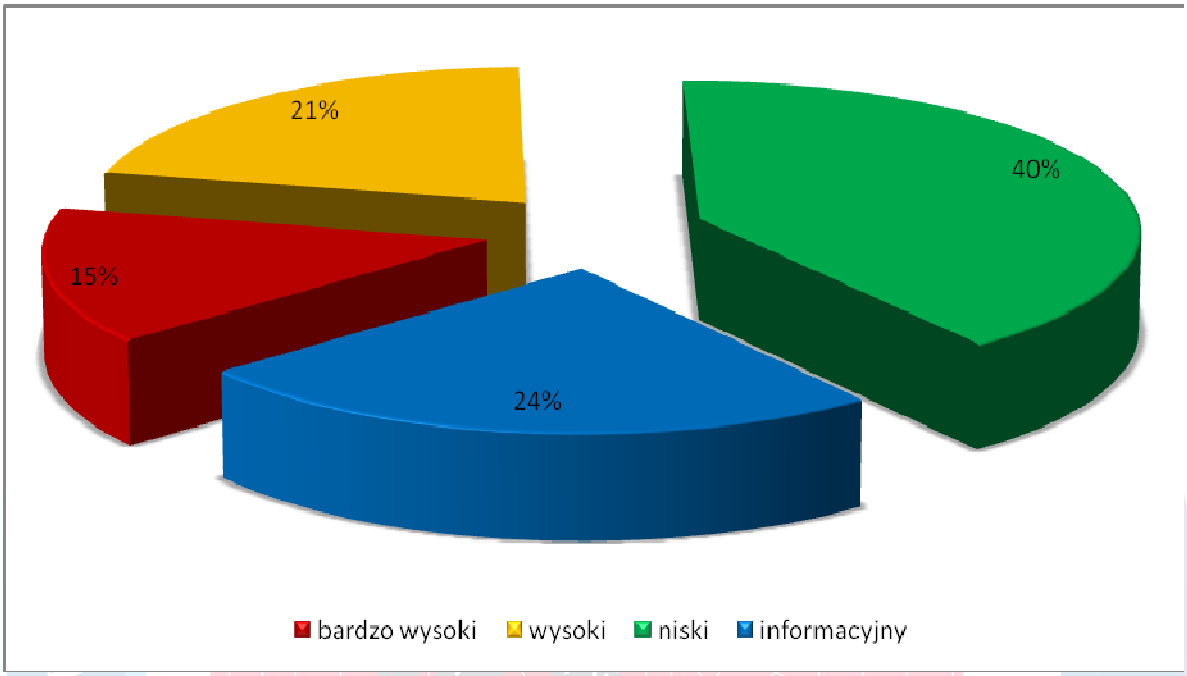
- MS12-039 - dotyczy podatności w Microsoft .Lync.
- MS12-040 - dotyczy podatności w Microsoft Dynamics AX Enterprise Portal.
- MS12-041 - dotyczy podatności w Microsoft Windows Mode Drivers Portal.
- MS12-042 - dotyczy podatności w Windows Kernel.

- **Podatność w Cisco AnyConnect Secure Mobility Client**

Firma Cisco opublikowała poradnik bezpieczeństwa informujący o wykryciu błędów w zabezpieczeniach AnyConnect Secure Mobility Client, które mogą zostać wykorzystane przez atakującego do wykonania dowolnego kodu, podwyższenia uprawnień systemowych lub skompromitowania podatnego systemu.

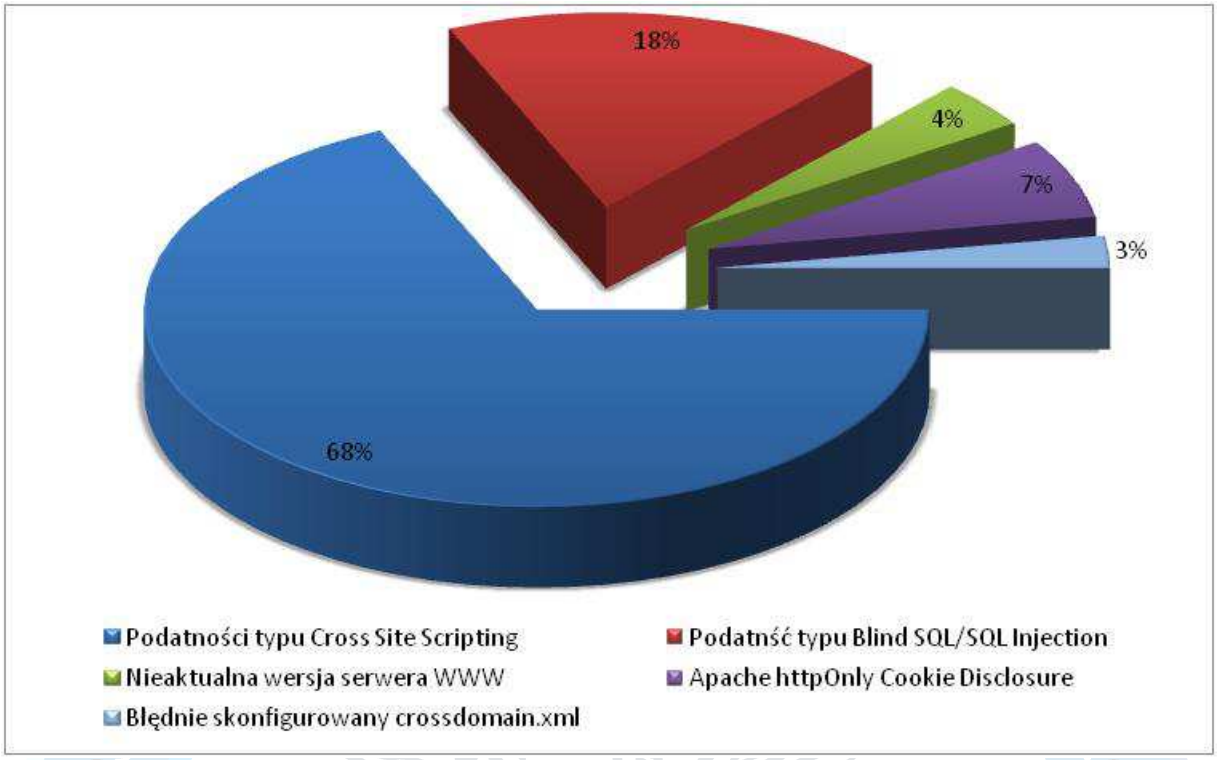
6 Testy bezpieczeństwa witryn WWW instytucji państwowych.

W II kwartale 2012 roku przebadano 20 witryn należących do 15 instytucji państwowych. Stwierdzono ogółem 213 błędów w tym: 31 błędów o bardzo wysokim poziomie zagrożenia, 45 błędów o wysokim poziomie zagrożenia, 86 błędów o niskim poziomie zagrożenia i 51 błędów oznaczonych jako informacyjne.



Rysunek 6-1: Statystyka wykrytych podatności w witrynach WWW należących do instytucji państwowych (według poziomu zagrożenia)

Wśród podatności o wysokim lub bardzo wysokim poziomie zagrożenia przeważają błędy typu Cross Site Scripting oraz Blind SQL Injection/SQL Injection. Istotnym problemem jest również wykorzystywanie w serwerach produkcyjnych nieaktualnych wersji oprogramowania.

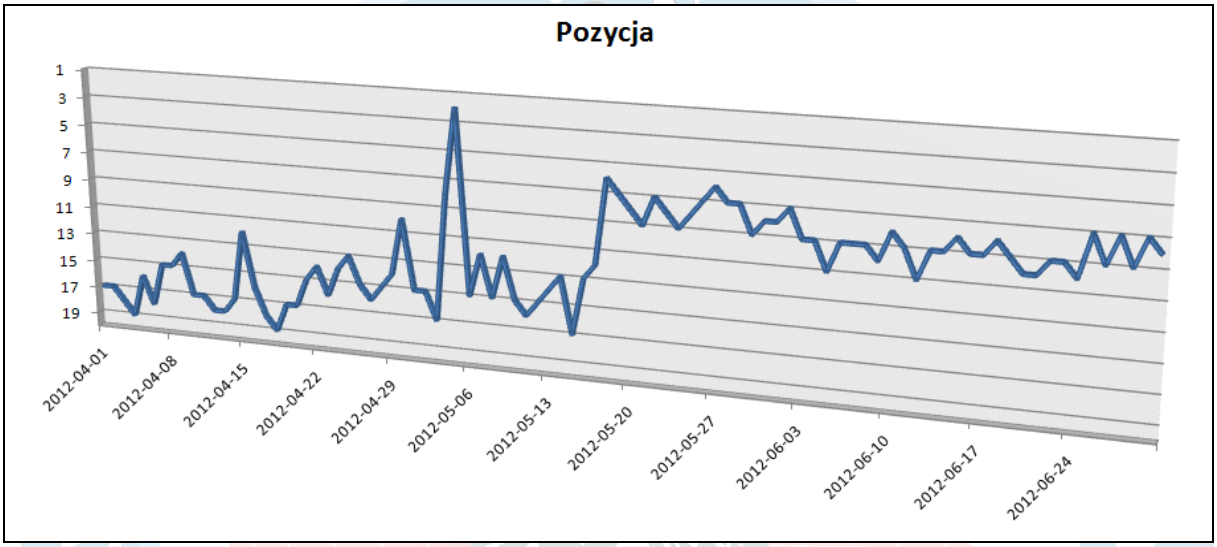


Rysunek 6-2: Procentowy rozkład najpoważniejszych błędów

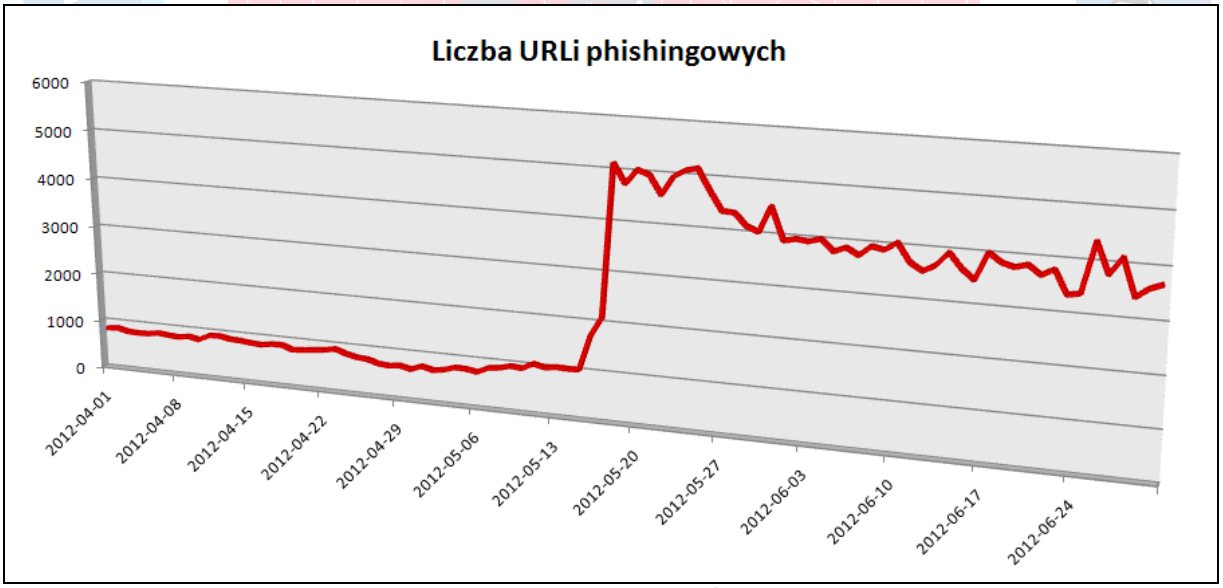
Należy zwrócić uwagę, iż ujawnione podatności krytyczne najczęściej znajdują się w warstwie usługowej systemu (np. serwerze WWW czy frontendzie do bazy danych), a nie w warstwie systemu operacyjnego. Jak widać, obecnie największe zagrożenie dla bezpieczeństwa stanowią błędy w aplikacjach, do których ma dostęp użytkownik zewnętrzny i które bardzo często nie są budowane, konfigurowane i utrzymywane przez lokalnych administratorów w instytucjach.

7 Informacje z systemów zewnętrznych - ATLAS

System ATLAS[11] prowadzony przez firmę ARBOR gromadzi istotne informacje na temat zagrożeń teleinformatycznych w sieci Internet i agreguje je pod względem m.in. klas adresowych poszczególnych państw oraz poszczególnych typów zagrożeń. Na podstawie tych danych każdemu z krajów przydzielane jest miejsce w statystyce pokazującej ryzyko dla bezpieczeństwa teleinformatycznego, jakie dane państwo stanowi.

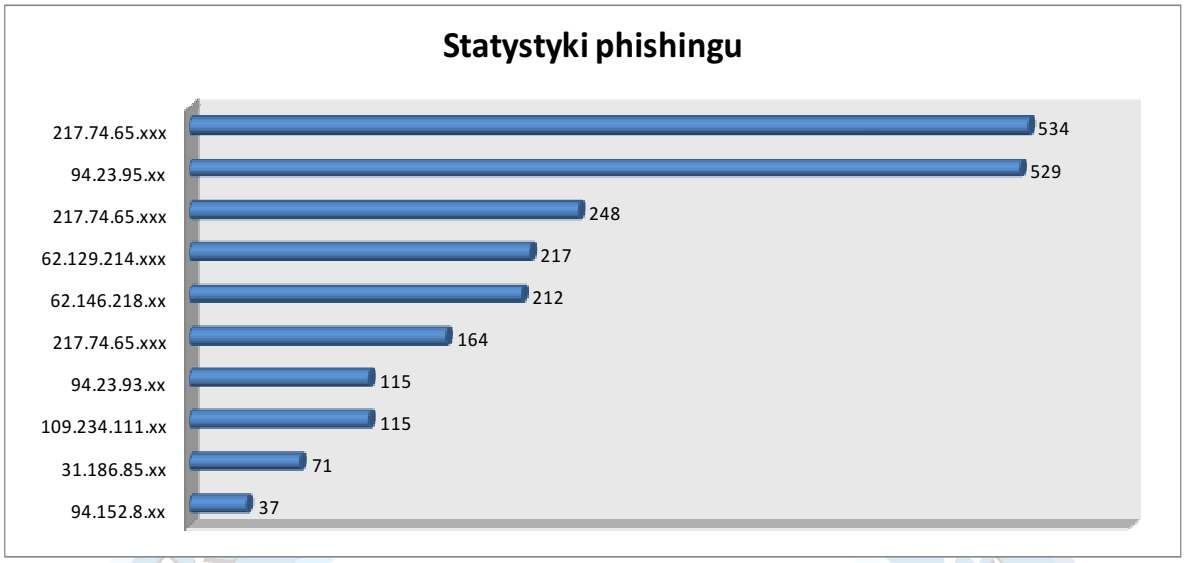


Rysunek 7-1: Pozycja Polski w rankingu ATLAS



Rysunek 7-2: Liczba phishingowych adresów URL wg ATLAS

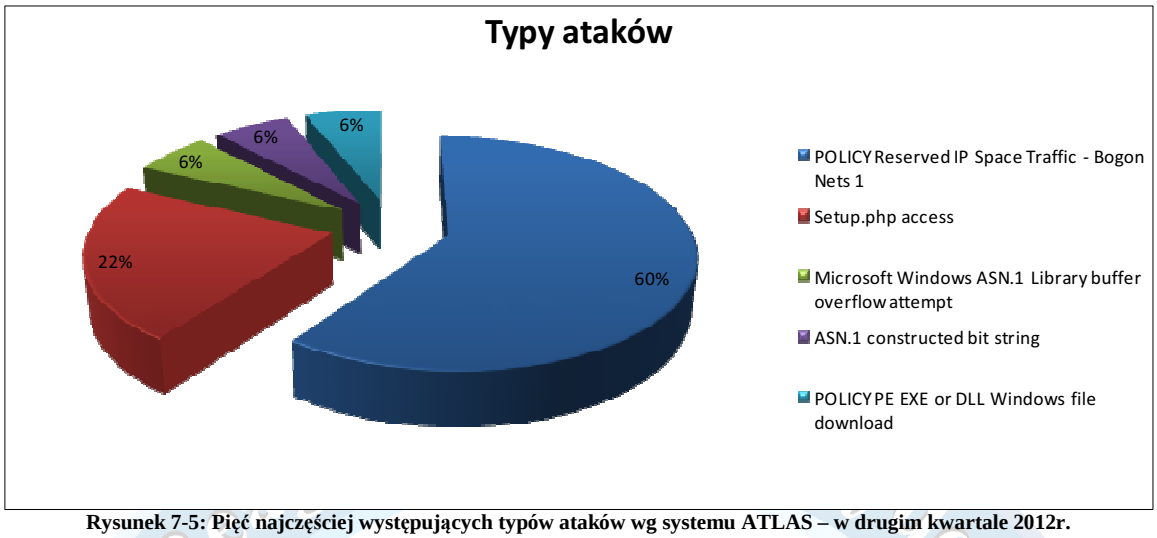
[11] http://atlas.arbor.net



Rysunek 7-3: Statystyki phishingu wg systemu Atlas – w drugim kwartale 2012r.
(ilości wystąpień najbardziej aktywnych hostów lub ich sumy dla wystąpień w ramach jednej podsieci)

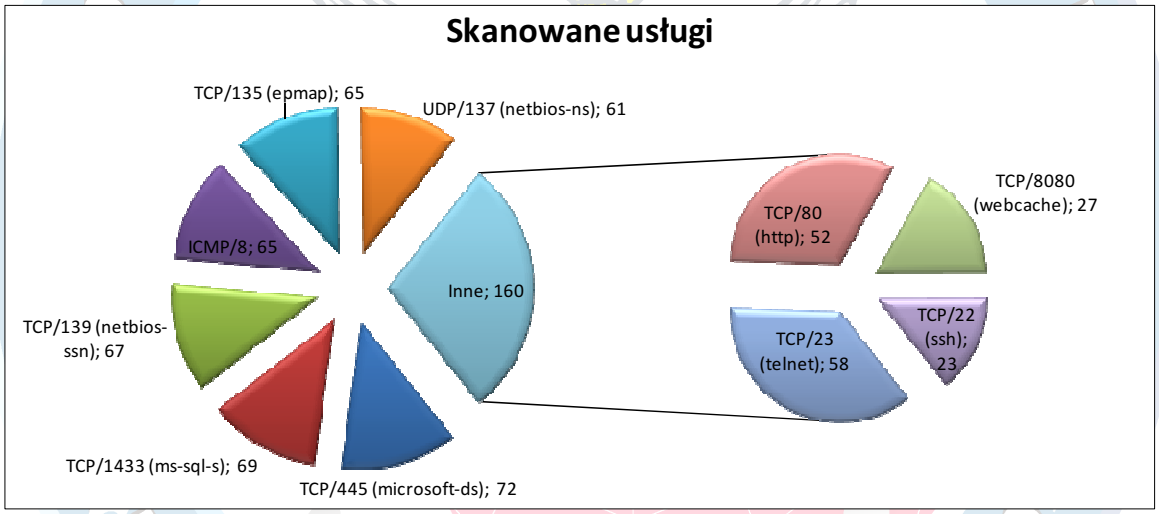
7.1 Statystyki ataków wg systemu Atlas (II kwartał 2012r.)

Rysunek 7-4: Najbardziej aktywne hosty w Polsce wg systemu ATLAS – w drugim kwartale 2012r.
(ilości wystąpień lub ich sumy dla hostów w jednej podsieci)

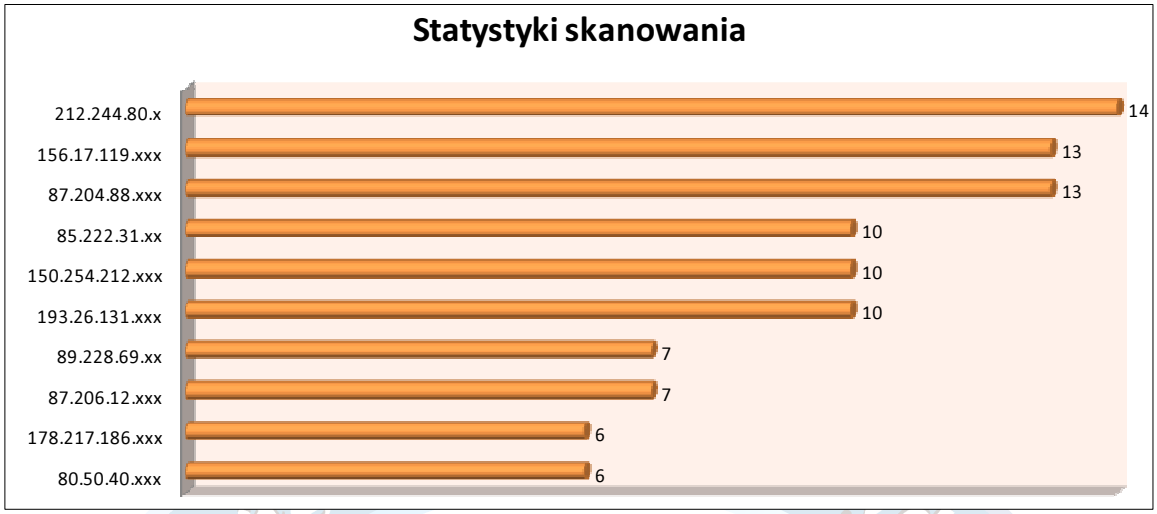


Rysunek 7-5: Pięć najczęściej występujących typów ataków wg systemu ATLAS – w drugim kwartale 2012r. (udział procentowy liczony tylko dla tych usług)

7.2 Statystyki skanowania wg systemu Atlas (II kwartał 2012r.)



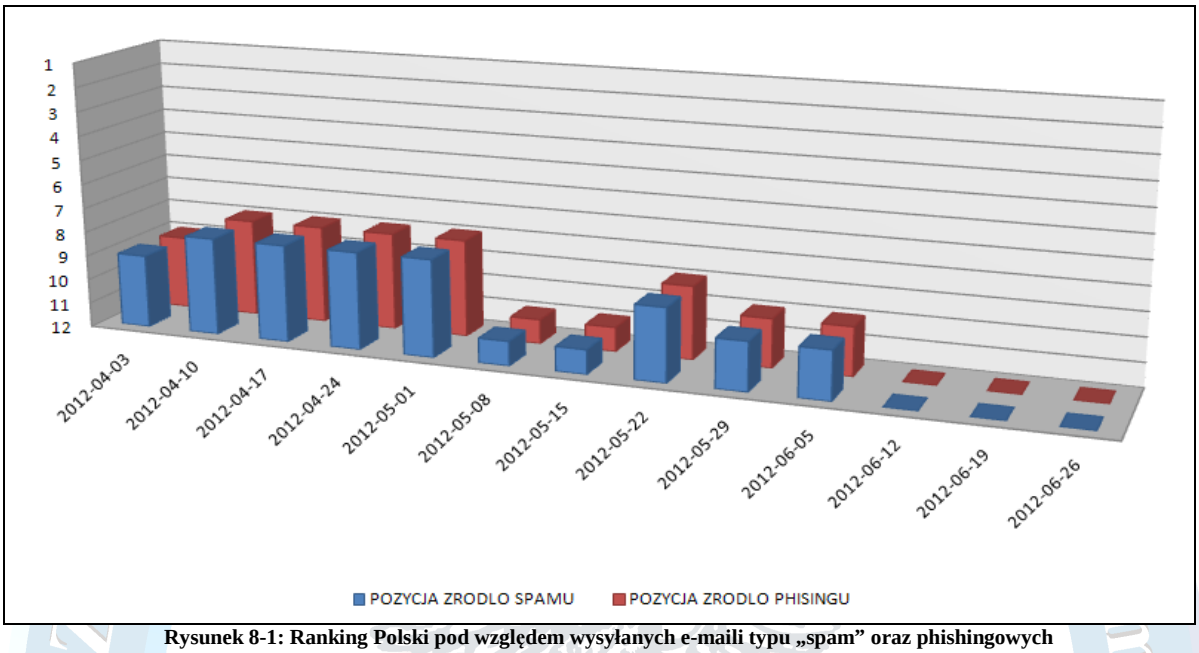
Rysunek 7-6: Najczęściej skanowane porty/usługi wg systemu ATLAS – w drugim kwartale 2012r. (odnotowane ilości wystąpień)



Rysunek 7-7: Najbardziej aktywne hosty w Polsce wg systemu ATLAS – w drugim kwartale 2012r. (ilości wystąpień lub ich sumy dla hostów w jednej podsieci)

8 Informacje z innych systemów zewnętrznych

Od początku 2010 r. zbierane są informacje na temat udziału Polski pod względem zawartości niechcianych przesyłek e-mailowych[12]



Rysunek 8-1: Ranking Polski pod względem wysyłanych e-maili typu „spam" oraz phishingowych (pozycje poniżej miejsca 12-go nie są raportowane)

Pomimo wstępnego spadku pozycji Polski, w drugiej połowie maja, znów pozycja powróciła do poziomu porównywalnego z poprzednimi kwartałami. Można zauważyć w tym momencie wyraźną korelację ze statystykami z systemu ATLAS.

Spadek pozycji Polski w czerwcu, wskazuje na to, iż pod względem wysyłki niechcianych informacji e-mailowych, skok w statystykach (zarówno w bieżącym jak i poprzednim kwartale) był sytuacją przejściową. Aktualnie inne kraje wyprzedziły Polskę w tym obszarze, przez co w końcowym okresie raportowania przestała być klasyfikowana.

[12] Informacje zbierane na podstawie tygodniowych raportów dostarczanych przez firmę M86 Security (http://www.m86security.com)

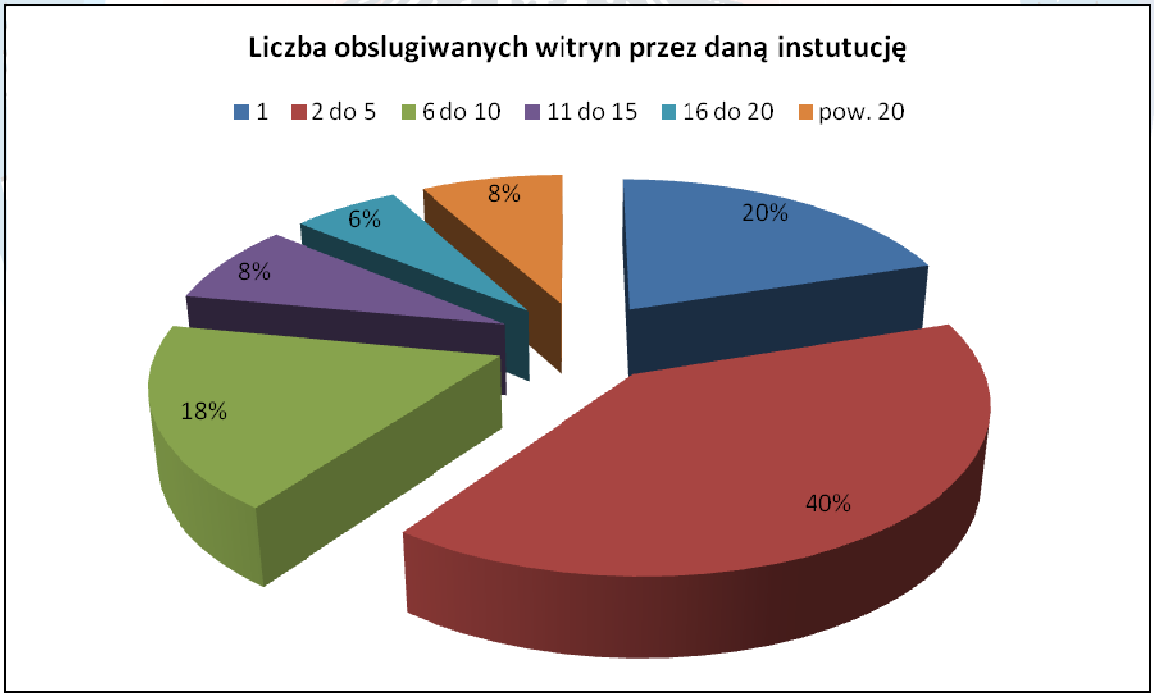
9 Informacja na temat stanu bezpieczeństwa witryn internetowych GOV.PL

Rządowy Zespół Reagowania na Incydenty Komputerowe CERT.GOV.PL mając na uwadze dużą różnorodność witryn, portali i stron internetowych działających w domenie gov.pl, przygotował zapytanie w formie ankiety do jednostek administracji państwowej z prośbą o dokonanie samooceny bezpieczeństwa teleinformatycznego posiadanych przez siebie systemów TI.

Otrzymane wyniki poddawane są analizie, która pozwoli docelowo na oszacowanie stanu bezpieczeństwa e-administracji państwowej w domenie gov.pl. Należy pamiętać, iż spełnienie wskazanych w ankiecie zaleceń jest deklaratywne i nie było weryfikowane przez Zespół CERT.GOV.PL poprzez testy bezpieczeństwa. Testy takie są prowadzone na zasadzie dobrowolności i jedynie na wniosek danej instytucji.

Poniższa statystyka ukazuje stan aktualny oraz planowany – stan docelowy 400 witryn należących do 55 podmiotów administracji państwowej.

Na poniższym wykresie wyraźnie widać, iż najczęściej jednostki administracji państwowej posiadają od 2 do 5 witryn, jednakże 1/5 wszystkich instytucji posiada tylko jedną stronę internetową.

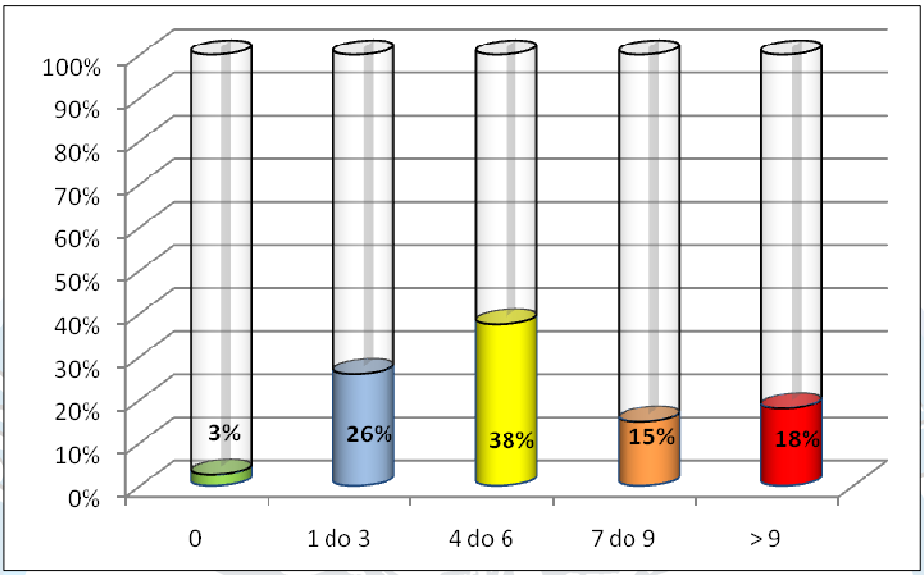


Rysunek 9-1: Liczba obsługiwanych witryn przez daną instytucję

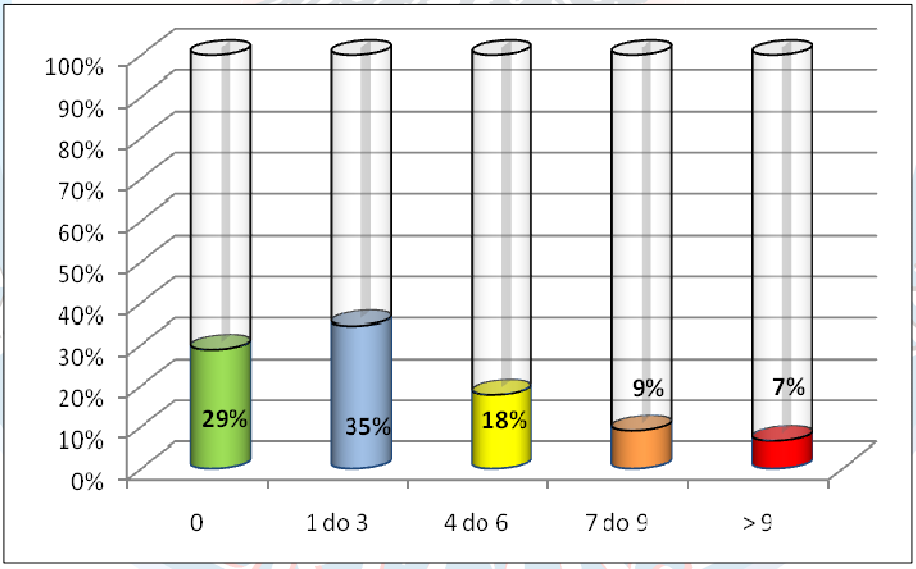
W obszarze gov.pl dominują dynamiczne strony internetowe o charakterze wyłącznie informacyjnym. Wedle deklaracji, udział ten docelowo się zmniejszy z 49% do 44% z uwagi na wdrażanie prostych e-usług. Charakterystyczne jest to, że część jednostek posiada wiedzę, że będzie zmieniało

typ strony, lecz jeszcze nie określiło na jaki docelowo (wzrost liczby stron o niesklasyfikowanym typie z 1% do 4%).

Poniższe wykresy przedstawiają oszacowanie bezpieczeństwa witryn w obszarze gov.pl w oparciu o spełnienie ilości zaleceń zespołu CERT.GOV.PL.



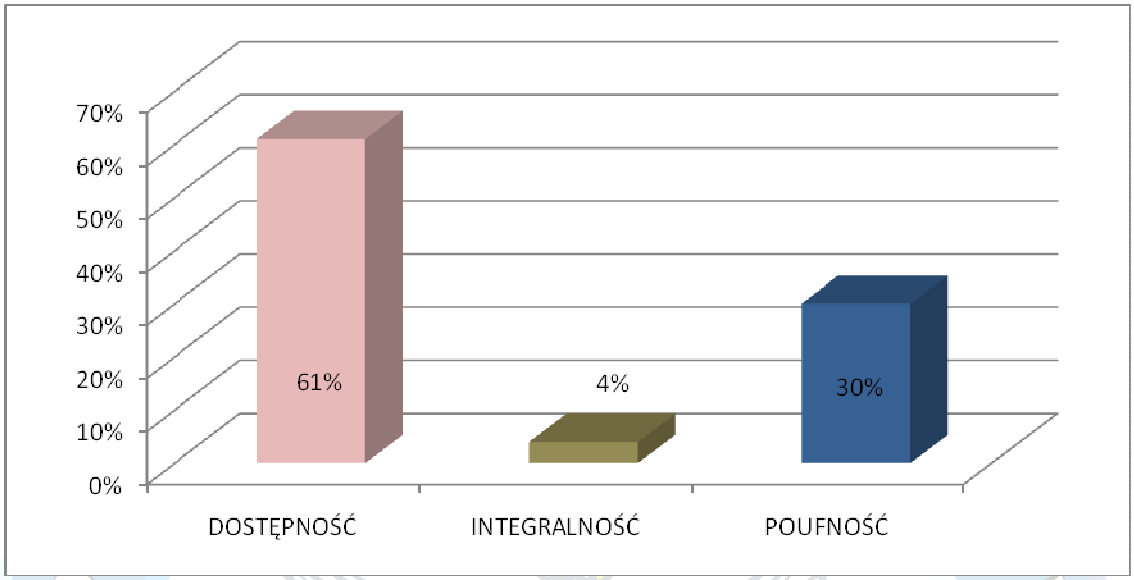
Rysunek 9-2: Liczba niespełnionych ilości zaleceń bezpieczeństwa – stan obecny



Rysunek 9-3: Liczba niespełnionych ilości zaleceń bezpieczeństwa – stan docelowy

Niestety wyraźnie widać, że większość witryn nie spełnia zaleceń CERT.GOV.PL dla witryn administracji. Niestety nawet docelowo, po planowanej rozbudowie witryn przez wszystkie jednostki administracji, nadal 36% stron nie będzie spełniało czterech lub więcej zaleceń w zakresie bezpieczeństwa.

Pod względem spełniania zaleceń CERT.GOV.PL, uwzględniając podział na poszczególne parametry bezpieczeństwa, stan witryn przedstawia się aktualnie następująco:



Rysunek 9-4: Stan witryn pod względem spełniania zaleceń CERT.GOV.PL

Jedynie pod względem dostępności sytuacja wygląda stosunkowo poprawnie (ponad połowa witryn spełnia zalecenia). Niestety jest to parametr bezpieczeństwa najmniej istotny w jawnych systemach e-administracji. Biorąc pod uwagę funkcjonalność witryn, które mają służyć obywatelowi jako źródło informacji, poziom zabezpieczenia i weryfikacji integralności danych prezentowanych na witrynach jest wyjątkowo niski.

Biorąc pod uwagę wyniki całości rezultatów ankiety należy wyraźnie stwierdzić, że poziom bezpieczeństwa witryn administracji jest bardzo niski. W wielu przypadkach naruszone zostały podstawowe zasady budowy bezpieczeństwa informacji w systemach teleinformatycznych. W niektórych przypadkach jednostki same nie dysponują wiedzą jakiego typu witryny są przez nie prowadzone.

Szczegółowe informacje zostaną przedstawione najważniejszym osobom w Państwie, w niejawnym raporcie opisującym stan bezpieczeństwa witryn internetowych domeny gov.pl.