Agencja Bezpieczeństwa Wewnętrznego

Raport kwartalny CERT.GOV.PL

kwiecień – czerwiec 2011

1. Informacje dotyczące zespołu CERT.GOV.PL

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.

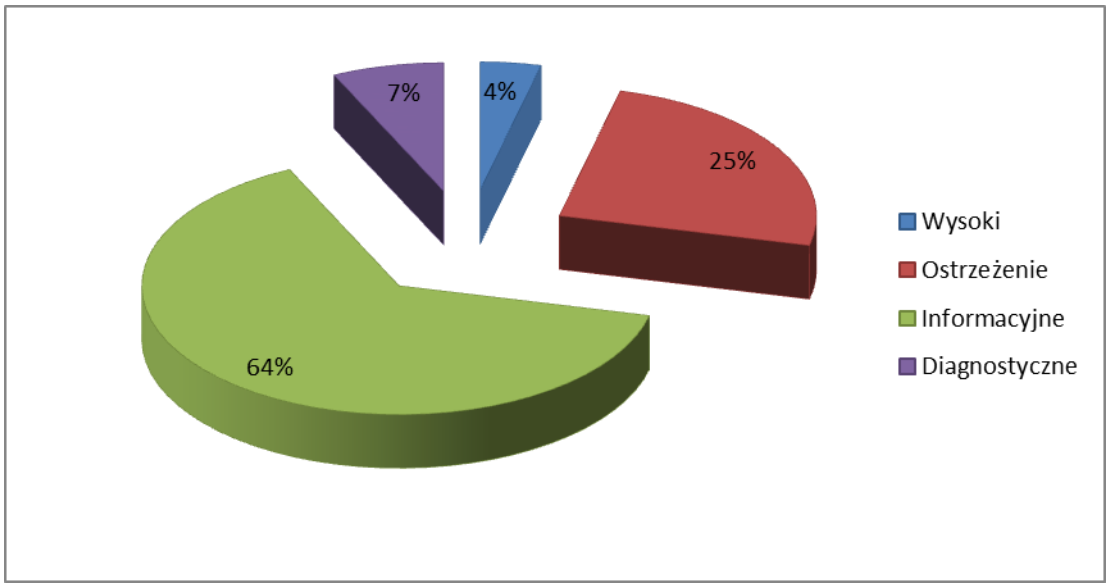
Dane kontaktowe:

- E-mail: cert@cert.gov.pl
- Telefon: +48 22 58 58 844
- Fax: +48 22 58 56 099

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

2. Statystyki systemu ARAKIS-GOV[1]

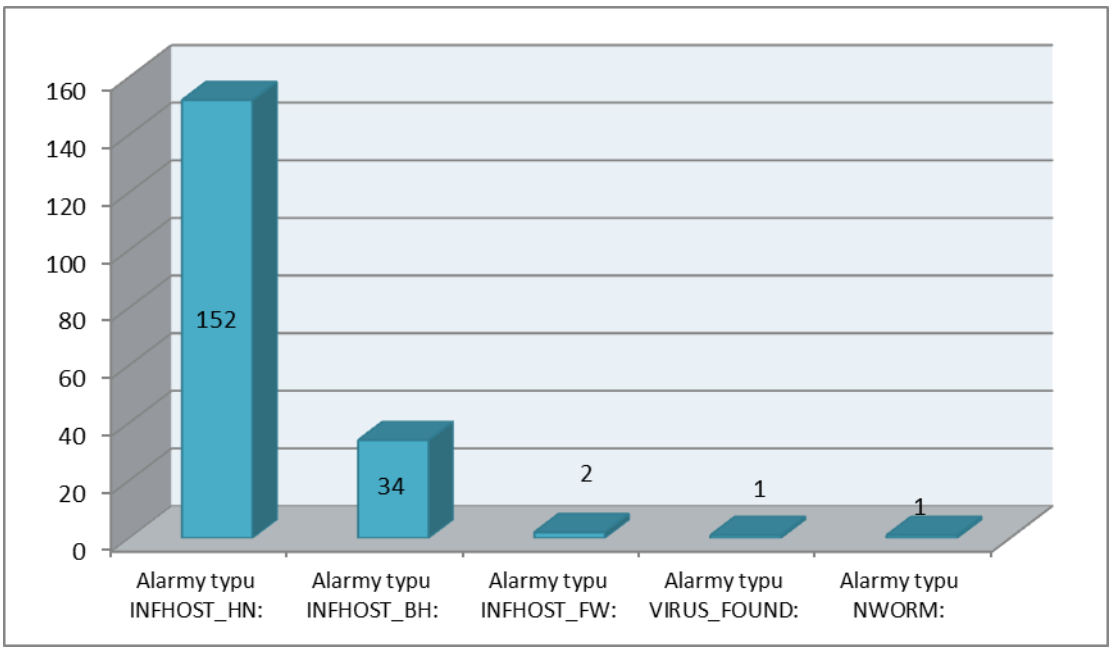
W drugim kwartale 2011 roku zdecydowaną większość stanowiły alarmy informacyjne, które stanowiły aż 64 procent wszystkich zarejestrowanych przez system ARAKIS-GOV. Alarmy o priorytecie średnim stanowiły 25%, natomiast alarmy diagnostyczne 7%. System zgłosił najmniej alarmów o priorytecie wysokim – 190 co stanowiło 4% wszystkich alarmów.



Rysunek 1 – Procentowy rozkład ważności alarmów.

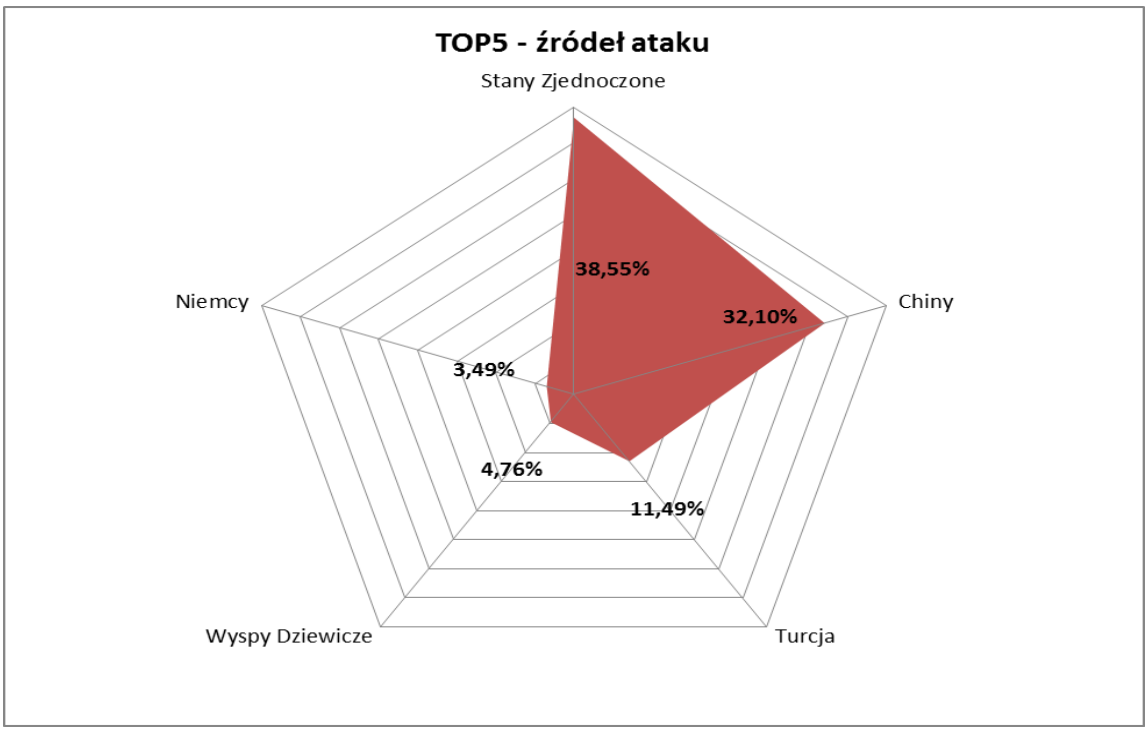
Wśród alarmów o priorytecie wysokim zaobserwowano 152 alarmów typu INFHOST_HN[2], 34 alarmów typu INFHOST_BH[3], 2 alarm typu VIRUS_FOUND[4], 2 alarmy typu INFHOST_FW[5] i 1 alarm typu NWORM[6].

[1] ARAKIS-GOV jest pasywnym systemem wczesnego ostrzegania o zagrożeniach w sieci Internet. W chwili obecnej został wdrożony w ponad 60 instytucjach państwowych.
[2] 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.
[3] Alarm INFHOST_BH oznacza wykrycie połączenia z domeną, która oznaczona została jako złośliwa tzn. przy pomocy której propagowane jest oprogramowanie złośliwe.
[4] 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
[5] 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.
[6] 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 2 – Statystyki alarmów o wysokim priorytecie.

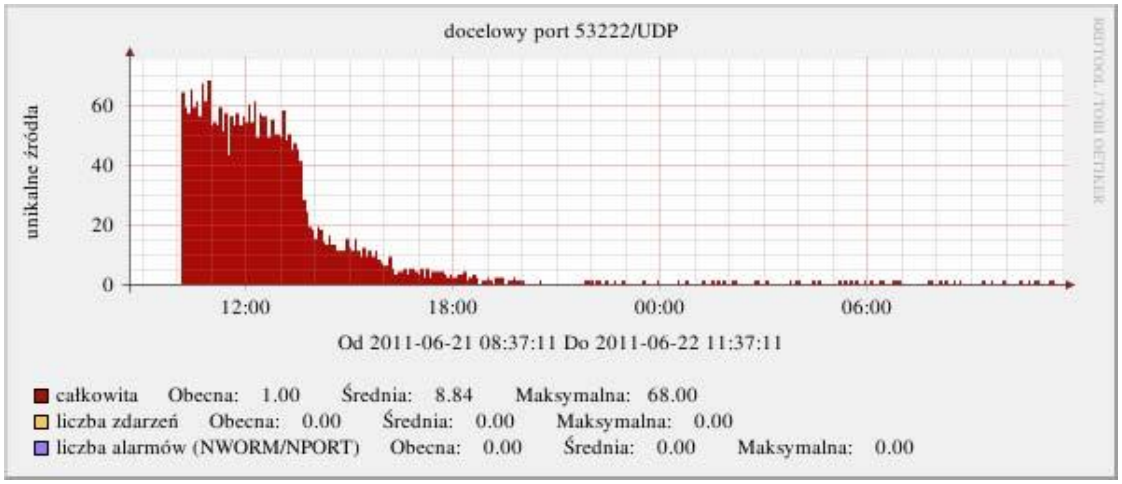
W wyniku analizy zarejestrowanych połączeń stwierdzono, iż w większości źródłem ataku były sieci komputerowe przypisane do Stanów Zjednoczonych, Chin, Turcji, Wysp Dziewiczych oraz Niemiec. Jednakże mając na uwadze specyfikę protokołu TCP/IP, nie można bezpośrednio łączyć źródła pochodzenia pakietów 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.



Rysunek 3 – Rozkład geograficzny źródeł wykrytych ataków (wg liczby przepływów).

Analiza zjawisk zaobserwowanych przez system ARAKIS-GOV

W czerwcu system ARAKIS-GOV zaobserwował wzrost ruch UDP na port 53222.

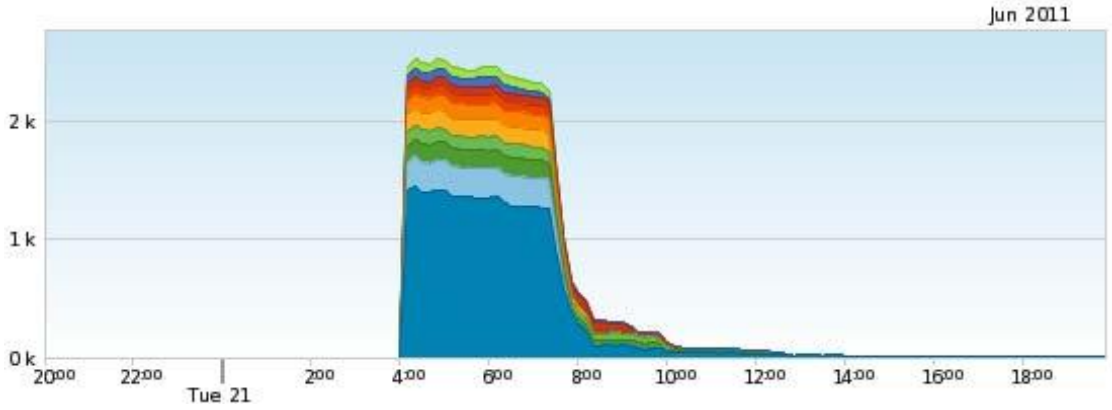


Charakterystyczną cechą powyższego ruchu był fakt, iż wszystkie pakiety sieciowe miały identyczna strukturę, tj. port źródłowy 62362, brak ustawionej sumy kontrolnej oraz następującą zawartość:

```
10:10:22.621228 IP 159.217.144.112.62362 > 193.19.73.61.53222: UDP, length
23

        0x0000:  4500 0033 2e88 0000 f611 5b97 9fd9 9070  E..3......[....p

        0x0010:  c113 493d f39a cfe6 001f 0000 4d61 7474  ..I=........Matt

        0x0020:  6869 6575 2e4c 6174 6170 7940 6c69 7036  hieu.Latapy@lip6

        0x0030:  2e66 72                                  .fr.fr
```

Występujący w przepływach adres email należy do Matthieu Latapy, pracownika instytutu badawczego LIP6 (http://www.lip6.fr/?LANG=en). Na podstawie powyższych faktów można przypuszczać, że odnotowane przez system ARAKIS-GOV zjawisko ma charakter skanowania adresów IP pod kątem identyfikacji działających zasobów.

Ruch na porcie 53222/UDP o bardzo podobnej charakterystyce został również zanotowany w systemie ATLAS.



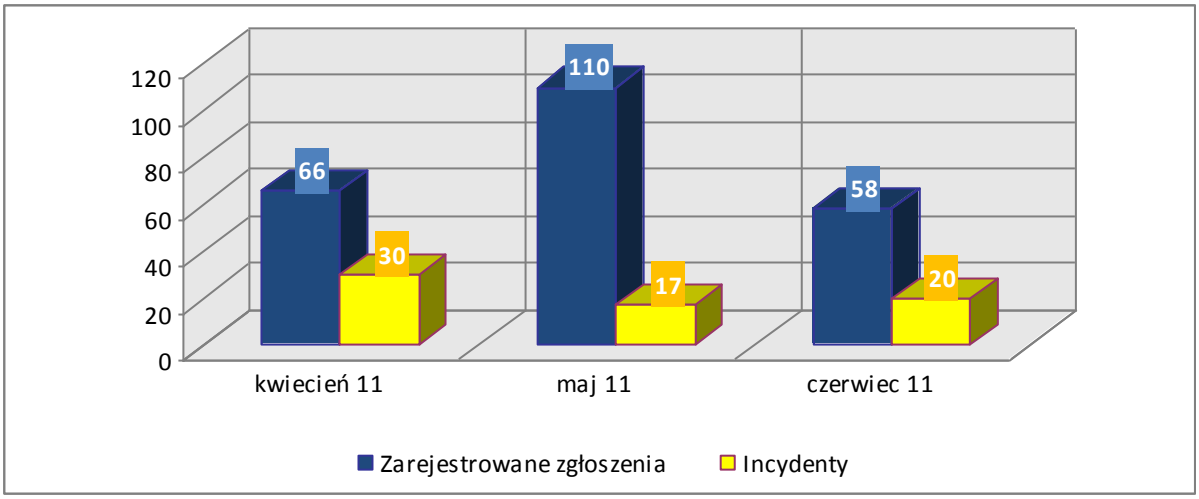
Żadna z sond darknet oraz jedynie ok. połowa sond honeynet należących do systemu ARAKIS otrzymało pakiety na tym porcie, wiec do skanowania zostały wybrane tylko niektóre zakresy adresów.

W sumie system ARAKIS-GOV odnotował łącznie 4863 pakietów będących efektem skanowania. Zostały one wysłane z 69 różnych adresów IP. Źródłowe adresy IP są w zdecydowanej większości przydzielone instytucjom edukacyjnym lub badawczym, co pozwala przypuszczać, ze skanowanie jest fragmentem projektu badawczego, w którym bierze udział duża liczba organizacji.

Nie zaobserwowano zależności miedzy adresami źródłowymi a docelowymi, ponadto te same adresy docelowe w honeynetach były skanowane wielokrotnie, z różnych IP. Na każdy z przeskanowanych adresów w honeynecie zostało wysłanych średnio 34, minimalnie 10, a maksymalnie 46 pakietów. Powtarzające się przepływy powodują, ze trudno określić, jaki był cel skanowania — jeśli chodziłoby wyłącznie o sprawdzenie osiągalności adresu, wystarczyłby jedynie jeden pakiet na adres.

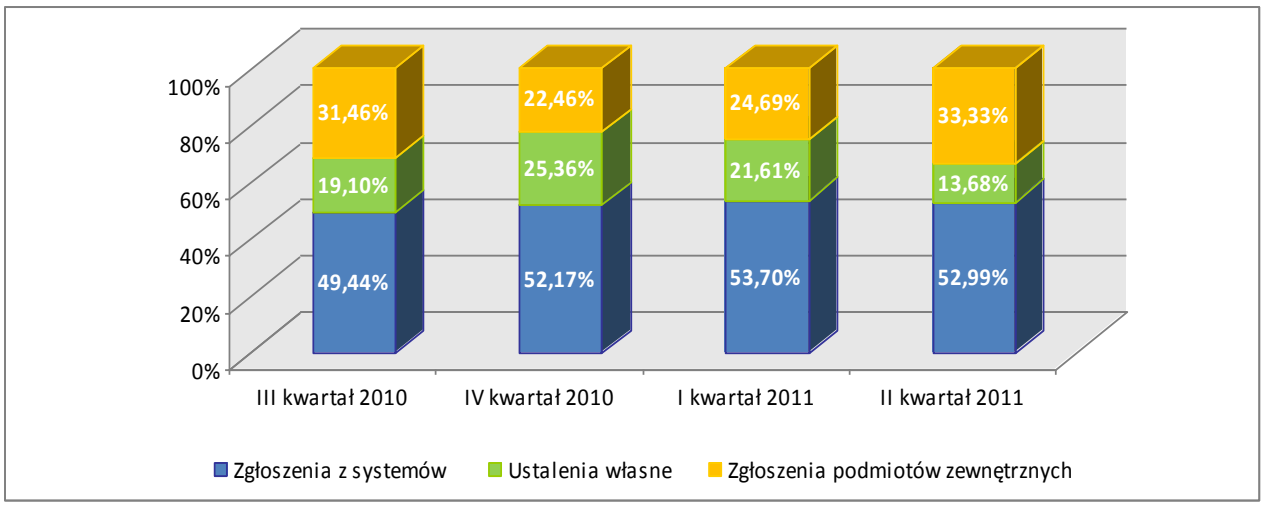
3. Statystyki incydentów

W drugim kwartale 2011 roku do zespołu CERT.GOV.PL wpłynęło 234 zgłoszeń, przy czym tylko 67 z nich zostały zakwalifikowane jako faktyczne incydenty.



Rysunek 4 - Liczba zgłoszeń oraz faktycznych incydentów w poszczególnych miesiącach drugiego kwartału 2011

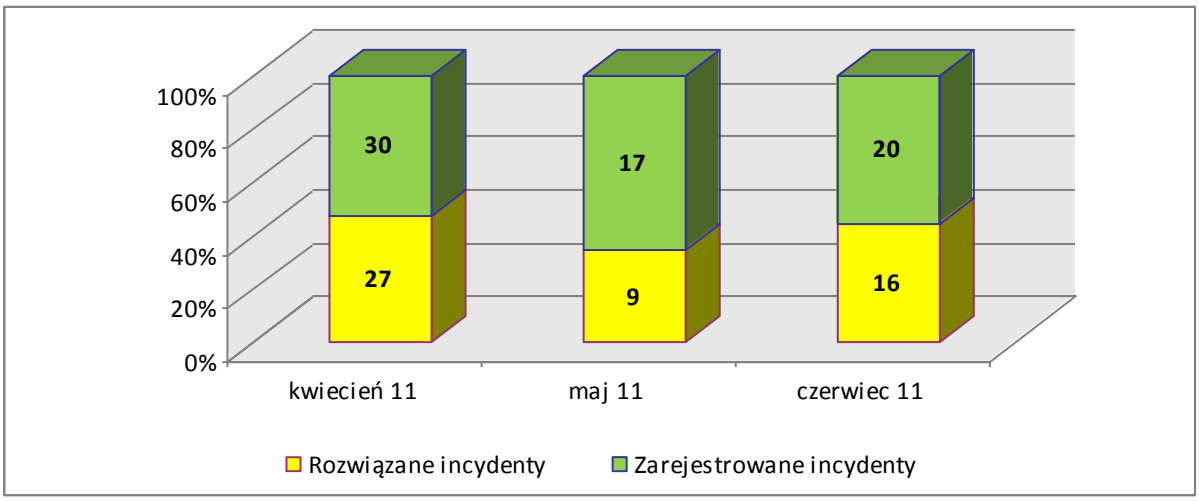
Szczegółowe statystyki źródeł zgłoszeń incydentów trafiających do CERT.GOV.PL przedstawia poniższy wykres.



Rysunek 5 - Źródła zgłoszeń incydentów

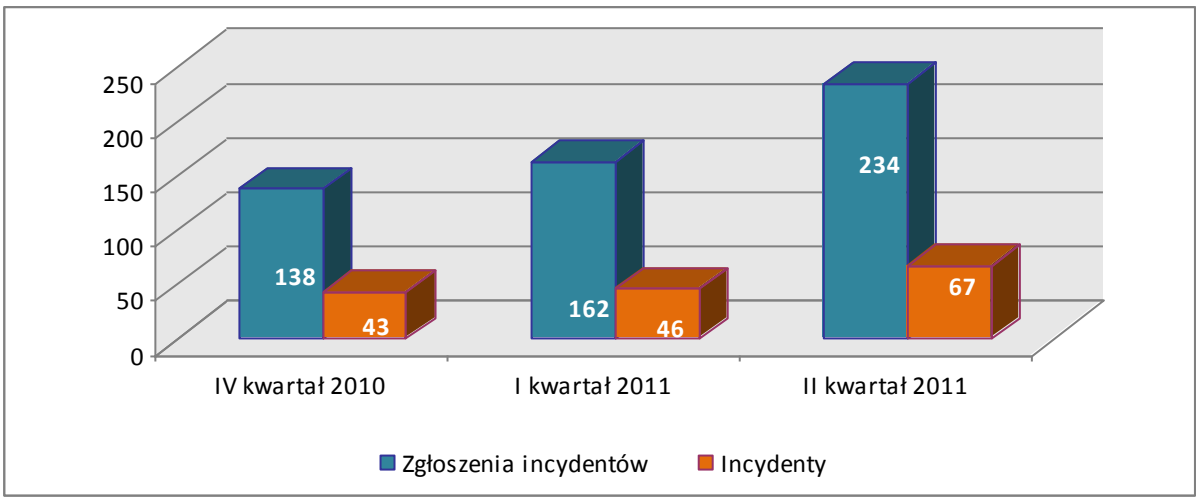
Rozkład miesięczny incydentów zarejestrowanych i incydentów, które zostały rozwiązane, przedstawia się następująco: w kwietniu 2011 zarejestrowano 30 incydentów, rozwiązanych natomiast zostało 27, w maju 2011 odnotowano 17 incydentów, z czego 9 zostało rozwiązanych, jednocześnie w czerwcu 2011 przyjęto do realizacji

20 incydentów, z czego 16 jeszcze w tym samym miesiącu zostało zakończonych. Pozostałe incydenty są w trakcie dalszej analizy.



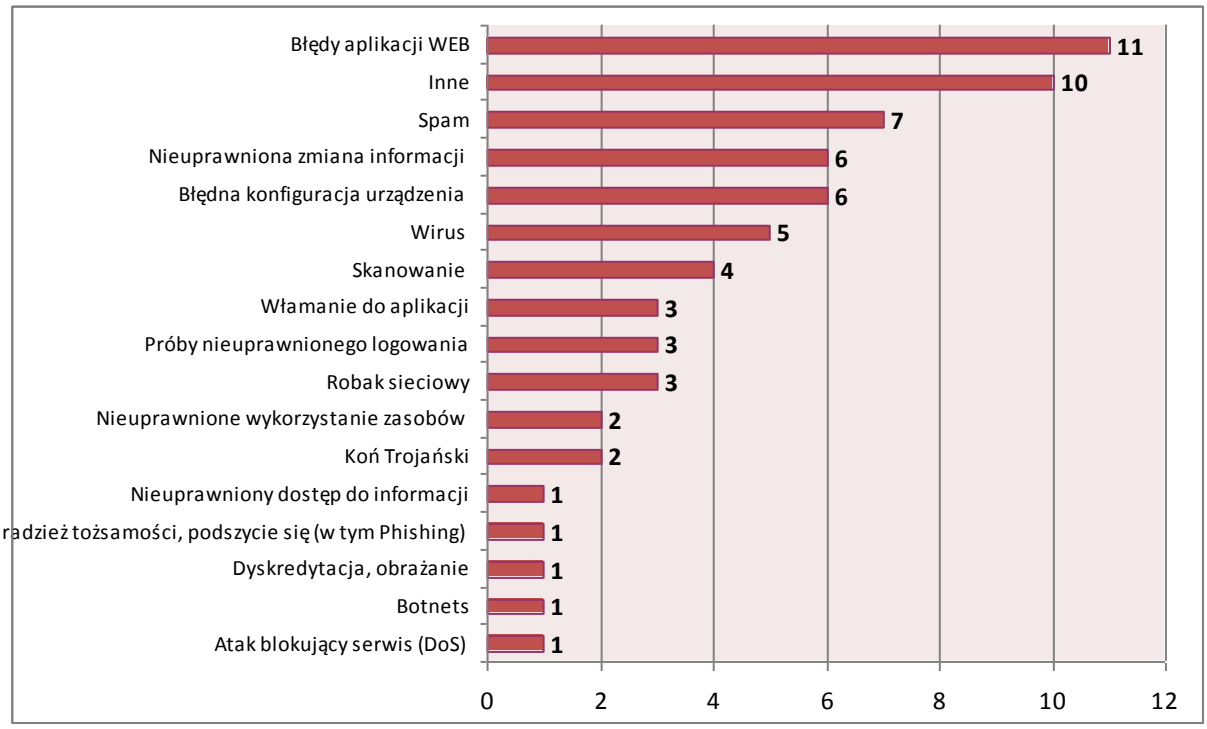
Rysunek 6 - Porównanie liczby incydentów otwartych i zamkniętych w poszczególnych miesiącach drugiego kwartału

Poniższy wykres obrazuje stale utrzymującą się tendencję wzrostową ilości zgłoszeń oraz faktycznych incydentów od IV kwartału 2010 roku do II kwartału 2011 roku.



Rysunek 7 – Porównanie ilości zgłoszeń incydentów i incydentów w ostatnich trzech kwartałach

Podział zarejestrowanych incydentów na kategorie przedstawia się następująco:



Rysunek 8 - Statystyka incydentów z podziałem na kategorie

Istotne ataki odnotowane przez Rządowy Zespół Reagowania na Incydenty Komputerowe CERT.GOV.PL w II kwartale 2011 r.:

- W kwietniu jeden z Urzędów Miasta wysłał zawiadomienie do zespół CERT.GOV.PL informując o bezprawnym naruszeniu integralności swojego systemu IT. Szczegółowa analiza powyższego zdarzenia wykazała, że włamania dokonano w wyniku eksploitacji starej wersji serwera WWW utrzymującego serwis. Ponadto, zalecono także zaatakowanemu podmiotowi dokonanie aktualizacji do najnowszej wersji oprogramowania oraz ponowną weryfikacje złożoności haseł.
- W kwietniu zespół CERT.GOV.PL uzyskał informację, że jeden z centralnych organów administracji państwowej padł ofiarą złośliwego oprogramowania o nazwie „SpyEye". W wyniku prowadzonych ustaleń zabezpieczone zostały skompromitowane konta, zainfekowane stacje robocze natomiast niezwłocznie odłączono od sieci.
- W tym miesiącu zespół CERT.GOV.PL zlokalizował także podatności typu Cross Site Scripting (XSS) na kilku witrynach w domenie .gov.pl. Mając na uwadze fakt, że wykryte luki umożliwiały wysłanie złośliwego kodu (zazwyczaj Javascript) poprzez podatną aplikację WWW do innego użytkownika. Poinformowano administratorów stron, którzy wprowadzili niezbędne zabezpieczenia chroniące przed powyższym zagrożeniem.

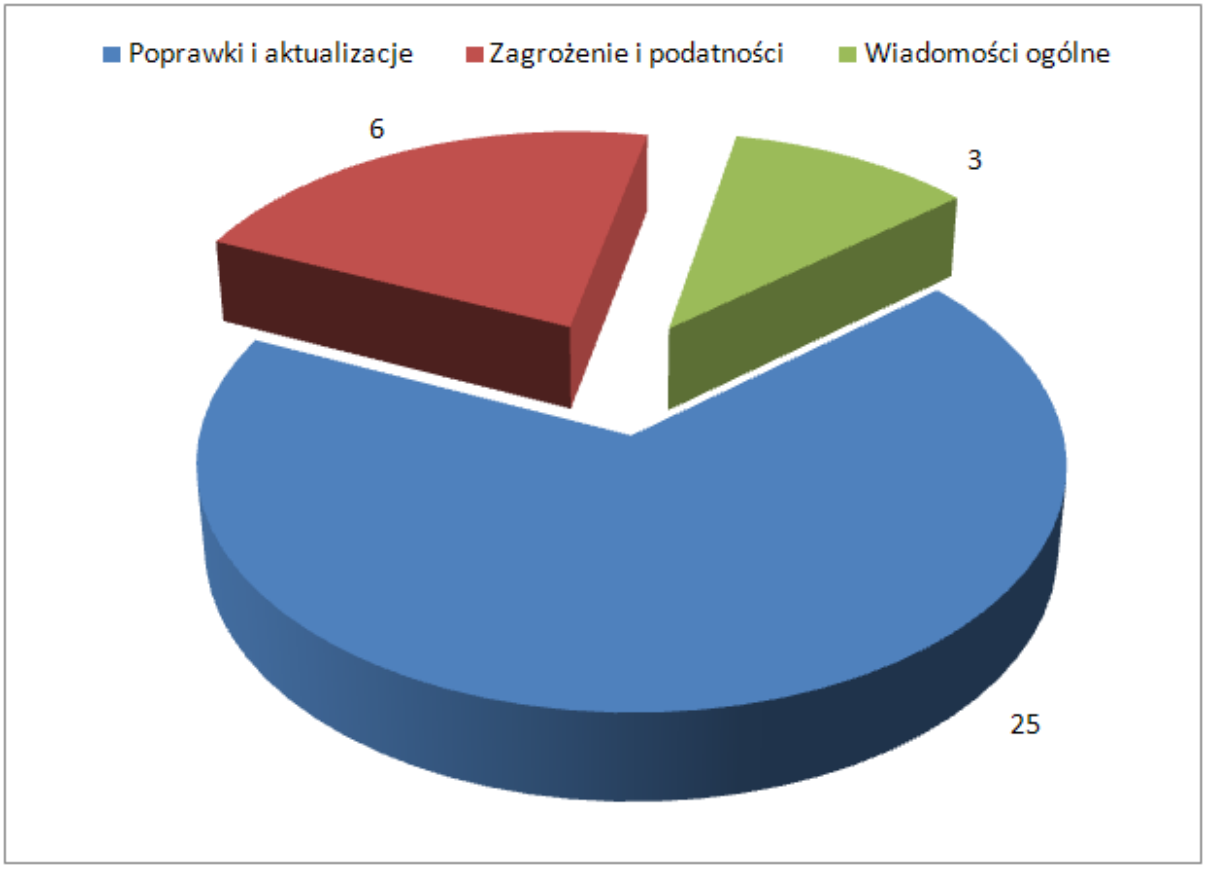
- W maju zespół CERT.GOV.PL otrzymał listę adresów IP należących do polskiej administracji rządowej, podejrzewanych o zainfekowanie złośliwym oprogramowaniem. Administratorzy zainteresowanych instytucji poinformowani zostali o powyższym fakcie oraz poproszeni zostali o weryfikację czy faktycznie nietypowe połączenia miały miejsce. Zlecono również zablokowanie wszelkich połączeń wychodzących jak i przychodzących na urządzeniach zaporowych do zainfekowanych domen przesłanych w liście z informacją od źródła.
- W drugiej połowie maja zespół CERT.GOV.PL otrzymał informację o wykryciu zainfekowanego pliku .xls, ukierunkowanego na pracowników jednego z Ministerstw. Plik ten był próbą eksploracji wykrytej podatności (Microsoft Security Bulletin MS09-067), która pozwalała na wykonanie dowolnego kodu z uprawnieniami aktualnie zalogowanego użytkownika. Podmiot został szczegółowo poinformowany o możliwym zagrożeniu, jak również uzyskał zalecenia w przypadku dalszego ponownego ataku tego typu.
- W tym miesiącu zespół CERT.GOV.PL zlokalizował także błędy typu SQL Injection na witrynach w domenie .gov.pl. Z uwagi na fakt, że wykryte luki umożliwiały nieautoryzowany, bezpośredni dostęp do silnika baz danych, co groziło przejęciem kontroli nad serwerem bazodanowym. Poinformowano administratorów stron, którzy wprowadzili niezbędne zabezpieczenia chroniące przed powyższym zagrożeniem.
- W czerwcu zespół CERT.GOV.PL uzyskał informację o ataku, który miał miejsce na przedsiębiorcę telekomunikacyjnego działającego na obszarze południowo-zachodniej Polski. Sprawcy zaatakowali centralę telefoniczną VoIP wyżej wymienionej firmy. Wykorzystując zaatakowaną centralę VoIP wykonali liczne połączenia zagraniczne, generując tym samym duże straty finansowe.
- W czerwcu zespół CERT.GOV.PL wykrył incydent dotyczący włamania na stronę jednego z Urzędów Miasta. Zgodnie z kompetencjami wysłane zostało zapytanie dotyczące wsparcia w przeprowadzeniu analizy powłamaniowej celem ustalenia sprawcy incydentu, określenia jego sposobu działania a także wykorzystania podatności zaatakowanych systemów.

4. Istotne podatności, zagrożenia i biuletyny zabezpieczeń

Witryna http://www.cert.gov.pl jest źródłem 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 2011 roku na witrynie www.cert.gov.pl dodano:

- 25 publikacji w kategorii „Poprawki i aktualizacje”,
- 6 publikacji w kategorii „Zagrożenia i podatności”,
- 3 publikacje w kategorii „Wiadomości ogólne”.



Rysunek 9 - Statystyka publikacji na stronie CERT.GOV.PL

Najistotniejsze publikacje dotyczące zagrożeń w pierwszym kwartale 2011 roku dotyczyły:

- **Nowych zagrożeń w plikach PDF**

Dnia 06.04.2011 Rządowy Zespół Reagowania na Incydenty Komputerowe CERT.GOV.PL poinformował, iż dzięki współpracy polskich zespołów bezpieczeństwa, związanych inicjatywą Abuse-Forum udało się wykryć oraz przeanalizować nowe zagrożenie. Od 03.04.2011 do polskich internautów trafia wiadomość e-mail zawierająca w załączniku złośliwy dokument PDF. Z analiz przeprowadzonych przez CERT Polska wynika, że po otwarciu załączonego pliku PDF komputer zostaje zainfekowany złośliwym oprogramowaniem SpyEye wykradającym poufne informacje wprowadzane przez użytkownika na stronach internetowych. Ponadto na podstawie przeprowadzonej przez zespół CERT.GOV.PL analizy, stwierdzono, iż plik PDF działa tylko pod oprogramowaniem Adobe Acrobat Reader w wersji 8.x.

- **Wykorzystywania przez cyberprzestępów śmierci Osamy Bin Ladena**

Dnia 05.05.2011 Na stronie http://www.cert.gov.pl Rządowy Zespół Reagowania na Incydenty Komputerowe poinformował, że zainteresowanie informacjami o śmierci Osamy Bin Ladena, jest wykorzystywane przez cyberprzestępców do rozsyłania specjalnie spreparowanych wiadomości e-mail mających na celu zainfekowanie i w wielu przypadkach przejęcie kontroli nad komputerem odbiorcy. Istnieje również zagrożenie związane z możliwością tworzenia stron zawierających szkodliwy kod lub infekujących złośliwym oprogramowaniem. Strony te mogą być indeksowane na wysokich pozycjach w wyszukiwarkach internetowych, co może skutkować masowym zarażaniem komputerów osób szukających najnowszych informacji związanych z przedmiotowym zdarzeniem.

- **Comiesięcznych biuletynów bezpieczeństwa firmy Microsoft**

Kwietniowy biuletyn bezpieczeństwa

Kwietniowy Biuletyn Bezpieczeństwa informował o wydaniu siedemnastu aktualizacji. Dziewięć oznaczono jako „krytyczny", pozostałe zostały sklasyfikowane jako „ważny".

- MS11-018 – biuletyn dotyczący podatności w programie Internet Explorer- krytyczny
- MS11-019 – biuletyn dotyczący podatności w kliencie i serwerze SMB - krytyczny

- MS11-020 – biuletyn dotyczący podatności w kliencie i serwerze SMB - krytyczny
- MS11-027 – biuletyn dotyczący podatności w komponentach Active X - krytyczny
- MS11-028 – biuletyn dotyczący podatności w .NET Framework – krytyczny
- MS11-029 – biuletyn dotyczący podatności w GDI+ - krytyczny
- MS11-030 – biuletyn dotyczący podatności w mechanizmie DNS resolution w Windows - krytyczny
- MS11-031 – biuletyn dotyczący podatności w środowisku JScript oraz VBScript – krytyczny
- MS11-032 – biuletyn dotyczący podatności w sterowniku OpenType Compact Font Format – krytyczny
- MS11-021 – biuletyn dotyczący podatności w Microsoft Excel - ważny
- MS11-022 – biuletyn dotyczący podatności w Microsoft PowerPoint - ważny
- MS11-023 – biuletyn dotyczący podatności w Microsoft Office - ważny
- MS11-024 – biuletyn dotyczący podatności w Fax Cover Page Editor - ważny
- MS11-025 – biuletyn dotyczący podatności w bibliotece Microsoft Foundation Class - ważny
- MS11-026 – biuletyn dotyczący podatności w MHTML - ważny
- MS11-033 – biuletyn dotyczący podatności w WordPad - ważny
- MS11-033 – biuletyn dotyczący podatności w Windows Kernel-Mode Drivers- ważny

Majowy biuletyn bezpieczeństwa

Majowy Biuletyn Bezpieczeństwa informował o usunięciu dwóch błędów. Otrzymały one status „krytyczny” i „ważny”

- MS11-035 – biuletyn dotyczący luk w zabezpieczeniach protokołu WINS - krytyczny
- MS11-036 – biuletyn dotyczący luk w zabezpieczeniach programu Microsoft Powerpoint - ważny

Czerwcowy biuletyn bezpieczeństwa

Czerwcowy Biuletyn Bezpieczeństwa informował o usunięciu szesnastu błędów w produktach Microsoft. Dziewięć aktualizacji posiada status „krytyczny”, natomiast siedem zostało sklasyfikowanych jako „ważny”.

- MS11-038 - biuletyn dotyczący podatności w OLE Automation - krytyczny
- MS11-039 - biuletyn dotyczący podatności w w .NET Framework oraz w Microsoft Silverlight - krytyczny
- MS11-040 - biuletyn dotyczący podatności w Threat Management Gateway Firewall Client - krytyczny
- MS11-041 - biuletyn dotyczący podatności w Windows Kernel-Mode - krytyczny
- MS11-042 - biuletyn dotyczący podatności w Microsoft Distributed File System - krytyczny
- MS11-043 - biuletyn dotyczący podatności w Microsoft SMB Client - krytyczny
- MS11-044 - biuletyn dotyczący podatności w .NET Framework - krytyczny
- MS11-050 - biuletyn dotyczący zbiorczej aktualizacja zabezpieczeń dla Internet Explorer - krytyczny
- MS11-052 - biuletyn dotyczący podatności w Vector Markup Language - krytyczny
- MS11-037 - biuletyn dotyczący podatności w MHTML - ważny
- MS11-045 - biuletyn dotyczący podatności w Microsoft Excel - ważny
- MS11-046 - biuletyn dotyczący podatności w Ancillary Function - ważny
- MS11-047 - biuletyn dotyczący podatności w Hyper-v - ważny
- MS11-048 - biuletyn dotyczący podatności w SMB Server - ważny
- MS11-049 - biuletyn dotyczący podatności w Microsoft XML Editor - ważny
- MS11-051 - biuletyn dotyczący podatności w Active Directory Certificate Services Web Enrollment - ważny

- **Biuletynów bezpieczeństwa dla produktów Adobe**

Rządowy Zespół Reagowania na Incydenty Komputerowe informował o:

- Biuletynie bezpieczeństwa Adobe Security Bulletin APSB11-12 dotyczącym wykrycia poważnych luk w programie Adobe Flash Player. Wykryte podatności mogą pozwolić osobie atakującej na zdalne wykonanie kodu, dostęp do niektórych informacji lub uszkodzenie pamięci.
- Biuletynie bezpieczeństwa Adobe Security Bulletin APSB11-13 dotyczącym wykrycia luk w programie Adobe Flash Player. Wykryte podatności umożliwiają

przeprowadzenie ataku typu Cross-site scripting, w sytuacji, gdy użytkownik odwiedzi zainfekowaną stronę.

- Biuletynie bezpieczeństwa Adobe Security Bulletin APSB11-16 dotyczącym wykrycia błędów w programach Adobe Reader oraz Adobe Acrobat. Wykryte podatności mogą spowodować zawieszenie się aplikacji i umożliwienie atakującemu przejęcie kontroli nad zaatakowanym systemem.
- Biuletynie bezpieczeństwa Adobe Security Bulletin APSB11-17 dotyczącym wykrycia błędów w programie Adobe Shockwave Player. Wykryte podatności sklasyfikowane jako "krytyczne" mogą pozwolić osobie atakującej na wykonanie w zaatakowanym systemie dowolnego kodu.
- Biuletynie bezpieczeństwa Adobe Security Bulletin APSB11-18 dotyczącym wykrycia luki w programie Adobe Flash Player. Wykryta podatność sklasyfikowana jako "krytyczna" może być przyczyną awarii pozwalającej atakującemu na przejęcie kontroli nad zaatakowanym systemem. Podatność jest wykorzystywana do przeprowadzania ataków ukierunkowanych za pomocą zainfekowanych stron.

- **Poprawek do oprogramowania zarządzającego sieciami komputerowymi CISCO**

Zespół CERT.GOV.PL informował na swojej stronie m.in. o podatnościach w następujących produktach firmy CISCO.

- Poradnik bezpieczeństwa cisco-sa-20110427-cucm - opisuje podatności występujące w Cisco Unified Communications Manager znanego wcześniej jako Cisco CallManager, które pozwalają atakującemu na wykonanie ataku Denial of Servise (DoS) w usłudze SIP, Directory Traversal oraz SQL Injection.
- Poradnik bezpieczeństwa cisco-sa-20110601-mxe - opisuje podatności występujące w Cisco Media Experience Engine 5600, które pozwalają atakującemu na uzyskanie uprawnień administracyjnych.
- Poradnik bezpieczeństwa cisco-sa-20110601-ac - opisuje podatności występujące w Cisco AnyConnect Secure Mobility Klient znanego wcześniej jako Cisco AnyConnect VPN Client które pozwalają atakującemu na uzyskanie uprawnień administracyjnych.

- Poradnik bezpieczeństwa cisco-sa-20110601-cnr - opisuje podatności występujące w Cisco Network Registrar, które pozwalają atakującemu na uzyskanie uprawnień administracyjnych.
- Poradnik bezpieczeństwa cisco-sa-20110601-phone - opisuje podatności występujące w Cisco Unified IP Phones 7900 series, które pozwalają atakującemu na uzyskanie uprawnień administracyjnych.

- **Wykrytych podatnościach i poprawkach dla produktów VMware**

Na stronie http://www.cert.gov.pl opublikowano informacje na temat opublikowania przez VMware informacji bezpieczeństwa numer VMSA-2011-0009 informującej o występujących lukach w produktach firmy. Wykorzystanie tych podatności może prowadzić do wykonania niepożądanego kodu i spowodować atak typu DoS, obejście mechanizmów zabezpieczających, zwiększenie uprawnień w systemie oraz dostęp do danych wrażliwych.

- **Krytycznych poprawkach dla produktów Oracle**

Rządowy Zespół Reagowania na Incydenty Komputerowe poinformował na swojej stronie o zbiorze krytycznych poprawek wydanych przez firmę Oracle pod nazwą Critical Patch Update for April 2011. Poprawki usuwały błędy w niżej wymienionych programach:

1. Oracle Database Server – 6 poprawek bezpieczeństwa
2. Oracle Fusion Middleware – 9 poprawek bezpieczeństwa
3. Oracle Enterprise Manager Grid Control – 1 poprawka bezpieczeństwa
4. Oracle E-Business Suite – 4 poprawki bezpieczeństwa
5. Oracle Supply Chain Products Suite – 1 poprawka bezpieczeństwa
6. Oracle PeopleSoft and JDEdwards Suite – 14 poprawek bezpieczeństwa
7. Oracle JD Edwards Products – 8 poprawek bezpieczeństwa
8. Oracle Siebel CMR – 3 poprawki bezpieczeństwa
9. Oracle Industry Applications – 1 poprawka bezpieczeństwa
10. Oracle Sun Products Suite – 18 poprawek bezpieczeństwa
11. Oracle Open Office Suite – 8 poprawek bezpieczeństwa

Oraz o zbiorze 17 krytycznych aktualizacji wydanych pod nazwą Oracle Java SE Critical Patch Update Advisory for June 2011 dla następujących produktów firmy Oracle:

- JDK i JRE 6 Update 25 oraz wersje wcześniejsze
- JDK i JRE 5.0 Update 29 oraz wersje wcześniejsze
- SDK i JRE 1.4.2_31 oraz wersje wcześniejsze

- **Podatności serwerów Apache**

Zespół CERT.GOV.PL zamieścił na stronie informacje na temat podatności w serwerach Apache, które mogą zostać wykorzystane do przeprowadzenia ataku typu odmowa usługi (Denial of Service - DoS).

- Błąd w module mod_dav_svn może być wykorzystany przez atakującego do wyczerpania pamięci systemu za pomocą nieskończonej pętli. Usterka ta występuje w wersjach od 1.5.0 do 1.6.16.
- Błąd w wskaźniku NULL w module mod_dav_svn może zostać wykorzystany do spowodowania zawieszenia usługi. Podatność ta występuje w wersji 1.6.16 oraz wcześniejszych.

- **Podatności serwerów BIND**

Rządowy Zespół Reagowania na Incydenty Komputerowe poinformował na swojej stronie o zbiorze poprawek opublikowanych przez firmę Internet System Consortium (ISC), zawierają one aktualizacje do serwera BIND w wersjach od 9.4-ESV-R3, 9.6-ESV-R2, 9.6.3, 9.7.1 i 9.8.0. Wykorzystanie ujawnionych podatności serwera w postaci przetwarzania rekordów RRSIG RRsets może prowadzić do nieoczekiwanego zamknięcia procesu "named" w systemie.

- **Poprawkach dla produktów firmy Mozilla**

Na stronie http://www.cert.gov.pl opublikowano informacje na temat wypuszczenia przeglądarki internetowej Mozilla Firefox w wersji 3.6.17. Oprogramowanie usuwa szereg podatności pozwalających miedzy innymi na zdalne wykonanie kodu przez atakującego, uzyskanie dostępu do zasobów przechowywanych w systemie użytkownika oraz na dostęp do informacji przechowywanych w historii przeglądarki.

Zespół CERT.GOV.PL zamieścił na stronie również informacje dotyczące opublikowała przez firmę Mozilla biuletynów bezpieczeństwa, w których informuje ona występowaniu luk w zabezpieczeniach programów Mozilla Firefox oraz Mozilla Thunderbird, które mogą zostać wykorzystane przez atakującego do obejścia zabezpieczeń w systemie użytkownika.

Biuletyny o wysokim priorytecie:

- MFSA 2011-19 - Biuletyn dotyczący błędów bezpieczeństwa pamięci w silniku przeglądarki używanym w Firefox oraz w innych produktach Mozilli.
- MFSA 2011-20 - Biuletyn dotyczący przeglądania przez użytkownika dokumentu XUL z wyłączonym JavaScript.
- MFSA 2011-21 - Biuletyn dotyczący możliwości naruszenia bloku pamięci spowodowanej awarią w multipart/x-mixed-replace images.
- MFSA 2011-22 - Biuletyn dotyczący możliwości wykonania kodu za pomocą metody Array.reduceRight().
- MFSA 2011-23 - Biuletyn dotyczący błędów występujących w wskaźniku.
- MFSA 2011-26 - Biuletyn dotyczący błędów występujących w kodzie WebGL.

Biuletyny o średnim priorytecie:

- MFSA 2011-24 - Biuletyn dotyczący błędów obsługi plików cookie.
- MFSA 2011-25 - Biuletyn dotyczący możliwości załadowania obrazu pochodzącego z innej domeny do tekstury WebGL.
- MFSA 2011-27 - Biuletyn dotyczący nieprawidłowego dekodowania HTML wewnątrz elementów SVG.

Biuletyny o niskim priorytecie:

- MFSA 2011-28 - Biuletyn dotyczący możliwości wywołania XPInstall.

- **Poprawkach dla użytkowników przeglądarki Chrome**

Rządowy Zespół Reagowania na Incydenty Komputerowe informował o:

- Stabilnej wersji przeglądarki internetowej Google Chrome 11.0.696.57. Usunięto w niej 25 luk w zabezpieczeniach, w tym szesnaście błędów związanych z wysokim ryzykiem ataku oznaczonych jako "High", sześć luk określonych mianem "Medium"

oraz trzy podatności posiadające niskie prawdopodobieństwo wystąpienia ataku "Low".

- Ukazaniu się przeglądarki internetowej Chrome w wersji 11.0.696.68. Oprogramowanie usuwało szereg podatności oraz zawierało Adobe Flash Player 10.3 który zwiększał stabilność, poziom bezpieczeństwa oraz ochronę prywatności użytkowników.
- Ujawnieniu podatności w przeglądarce Google Chrome starszej niż 11.0.696.71, które mogą zostać wykorzystane do ominięcia określonych zabezpieczeń na komputerze użytkownika. Podatności te dotyczą:
    1. Błędu umożliwiającego ominięcie blokady okienek typu "pop-up";
    2. Błędu prowadzącego do niewłaściwej dynamicznej alokacji pamięci;
    3. Błędu prowadzącego do naruszenia zawartości pamięci;
    4. Błędu prowadzącego do zapisu danych poza wyznaczonym obszarem;
- Wydaniu przez firmę Google nowej wersji przeglądarki internetowej Chrome 12.0.742.91. Naprawiono w niej 15 błędów, z czego aż sześć określono jako bardzo poważne "High". Luki te m.in. pozwalają osobie atakującej na wykonanie dowolnego kodu w systemie, w którym pracuje aplikacja, wykraść różnego rodzaju dane użytkownika, omijać zabezpieczenia lub spowodować awarię przeglądarki.
- Ukazaniu się przeglądarki internetowej Chrome w wersji 12.0.742.100. Luki występujące w poprzednich wersjach przeglądarki mogą pozwolić atakującemu na przejęcie kontroli nad systemem.
- Wydaniu przeglądarki internetowej Chrome w wersji 12.0.742.112. Luki występujące w poprzednich wersjach przeglądarki mogą pozwolić atakującemu na wykonanie dowolnego kodu.

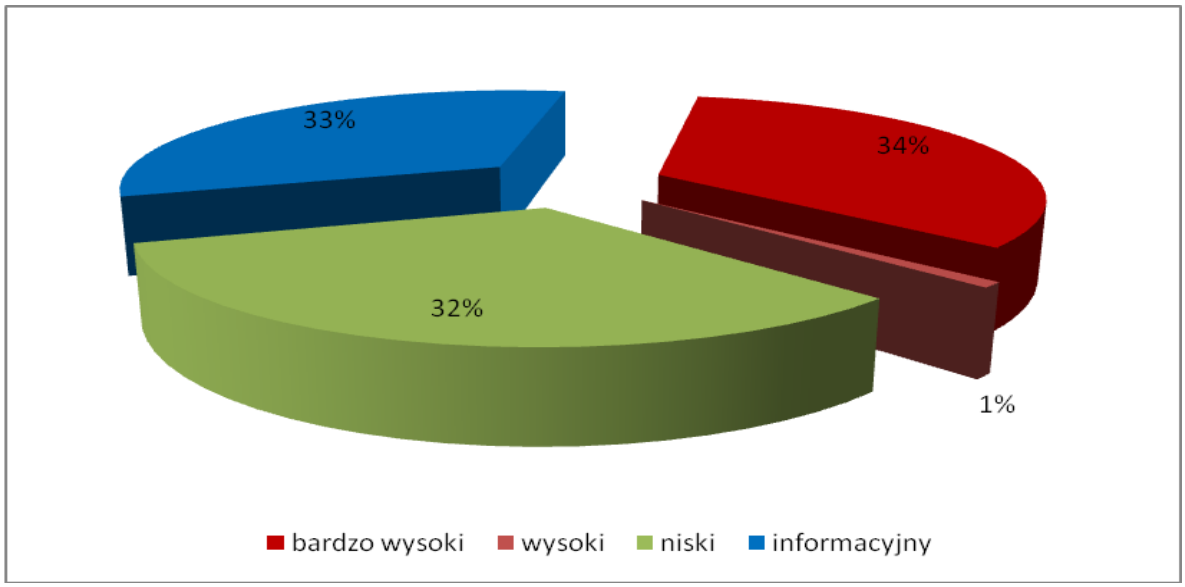
- **Poprawkach dla użytkowników przeglądarki Opera**

Na stronie http://www.cert.gov.pl opublikowano informacje na temat pojawienia się przeglądarki Opera w wersji 11.50. Luki występujące w poprzednich wersjach mogą pozwolić atakującemu na ominięcie niektórych zabezpieczeń.

5. Testy bezpieczeństwa witryn WWW instytucji państwowych

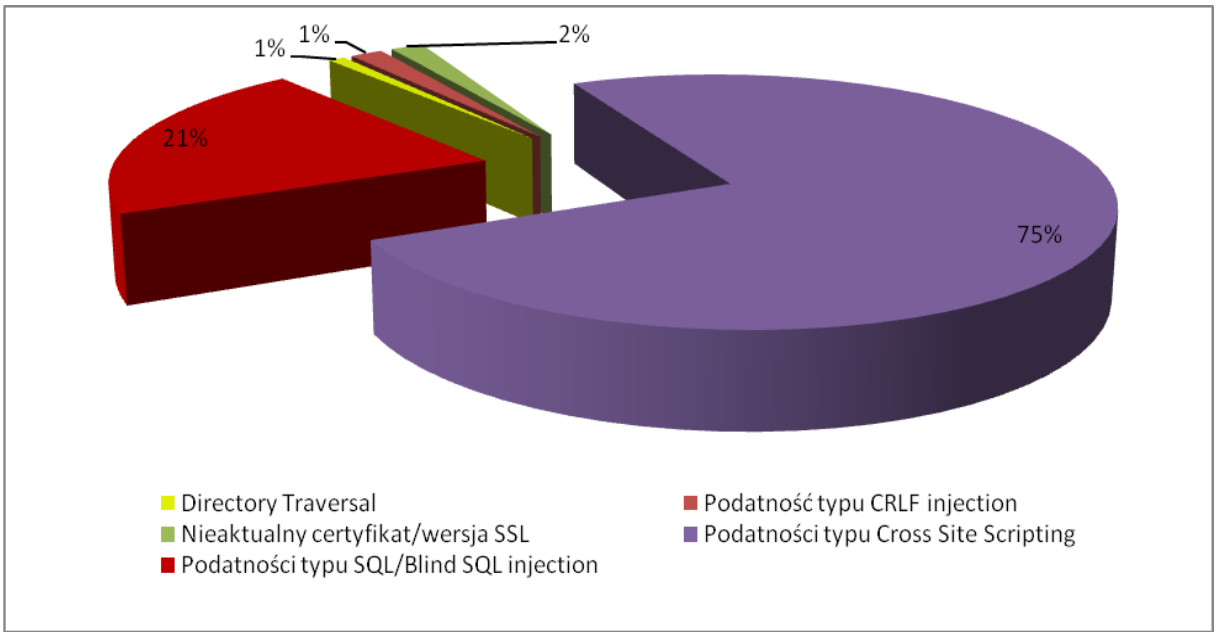
Zespół CERT.GOV.PL kontynuował testy bezpieczeństwa witryn WWW należących do instytucji państwowych.

W II kwartale 2011 roku przebadano 39 witryn należących do 10 instytucji państwowych. Stwierdzono ogółem 355 błędów w tym: 120 błędów o bardzo wysokim poziomie zagrożenia, 3 błędy o wysokim poziomie zagrożenia, 116 błędów o niskim poziomie zagrożenia i 116 błędów oznaczonych jako informacyjne.



Rysunek 10 - Statystyka wykrytych podatności w rządowych witrynach WWW według poziomu zagrożenia

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



Rysunek 11 - Procentowy rozkład najpoważniejszych błędów

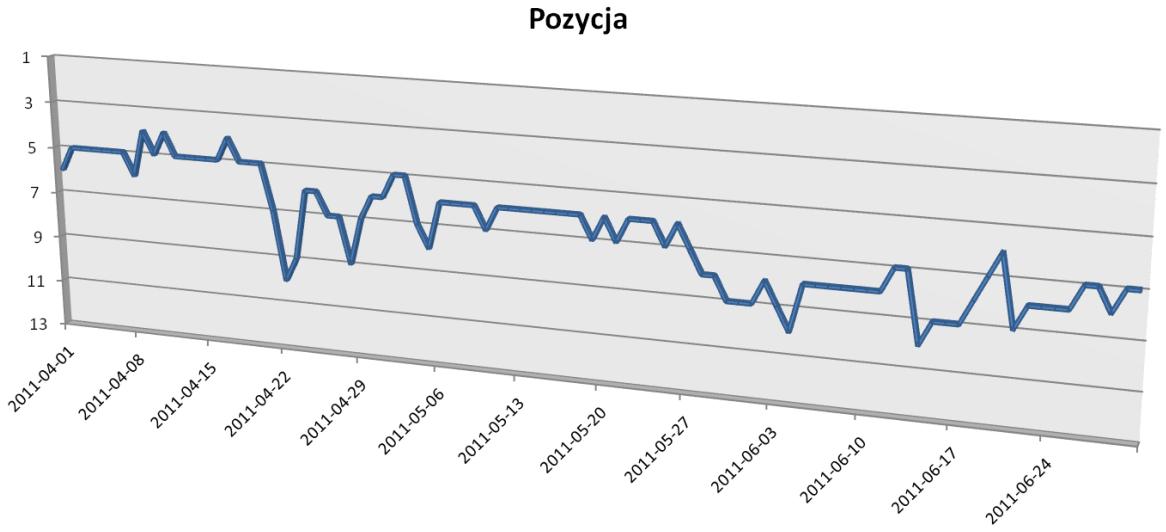
Należy zwrócić uwagę, iż podatności krytyczne najczęściej znajdują się w warstwie usługowej systemu (np. serwerze http czy frontendzie do bazy danych), a nie w warstwie systemu operacyjnego. Jak widać, obecnie największe zagrożenie dla bezpieczeństwa stanowią błędy w aplikacjach, które są budowane, konfigurowane i utrzymywane poza lokalną infrastrukturą instytucji państwowej.

6. Informacje z systemów zewnętrznych

6.1. System ATLAS

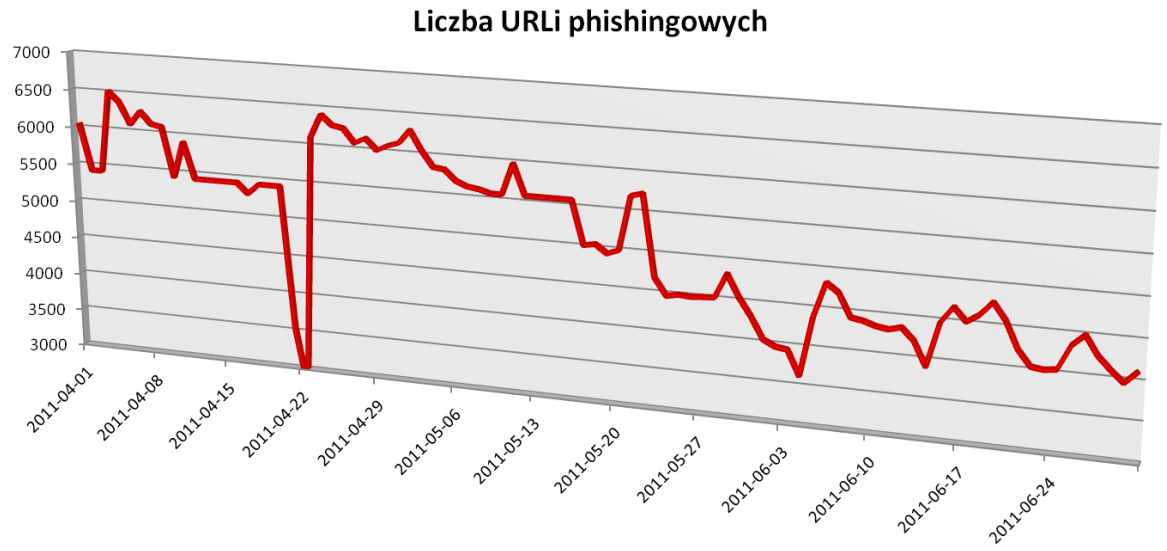
System ATLAS[7] gromadzi istotne informacje na temat zagrożeń teleinformatycznych w sieci Internet i agreguje je pod względem m.in. klas adresowych poszczególnych państw oraz poszczególnych typów niebezpieczeństw. Na podstawie tych danych każdemu z krajów przydzielane jest miejsce w statystyce pokazującej ryzyko dla bezpieczeństwa teleinformatycznego, jakie dane państwo stanowi.

W porównaniu do poprzedniego kwartału, pomimo tego, iż Polska w dalszym ciągu utrzymuje się dość wysoko w rankingu krajów stwarzających zagrożenie dla bezpieczeństwa Internetu to jednak można zauważyć powolną tendencję zniżkową. Jest to efekt ciągłych działań zespołów bezpieczeństwa. Ciągła walka ze strona służącymi do wyłudzania danych, przekłada się bezpośrednio na malejącą pozycję Polski.



Rysunek 12 - Pozycja Polski w rankingu ATLAS

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



Rysunek 13 – Liczba URLi phishingowych wg ATLAS

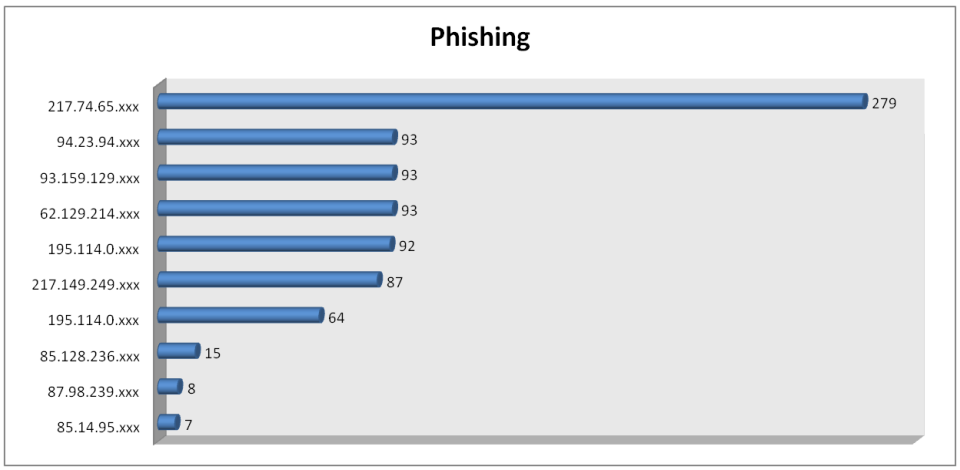
Plateau a następnie spadek w dniu 22 kwietnia zostały spowodowane awarią systemu po stronie dostawcy danych. Skoki w okolicach 20 maja oraz 3 czerwca są bezpośrednio powiązane z powstaniem exploitów na system zarządzania treścią Joomla.

Sytuacja powyższa, po raz kolejny, potwierdza opinię zespołu CERT.GOV.PL, iż liczba stron phishingowych w polskiej przestrzeni adresowej wynika z dużej ilości słabo zabezpieczonych witryn WWW (na których po przełamaniu zabezpieczeń włamywacze umieszczają nieautoryzowane treści), a nie z działalności w Polsce firm oferujących tzw. „kuloodporny hosting”[8].

W dalszym ciągu strony służące do wyłudzania informacji znajdują się w przeważającej ilości przypadków w prywatnych zasobach WWW. Zazwyczaj ich właściciele nie wiedzą o włamaniu, ponieważ treść phishingowa jest jedynie dodawana, bez zmiany dotychczasowej zawartości stron w danej witrynie, co pozwala ukryć przed właścicielem dodanie nielegalnych treści.

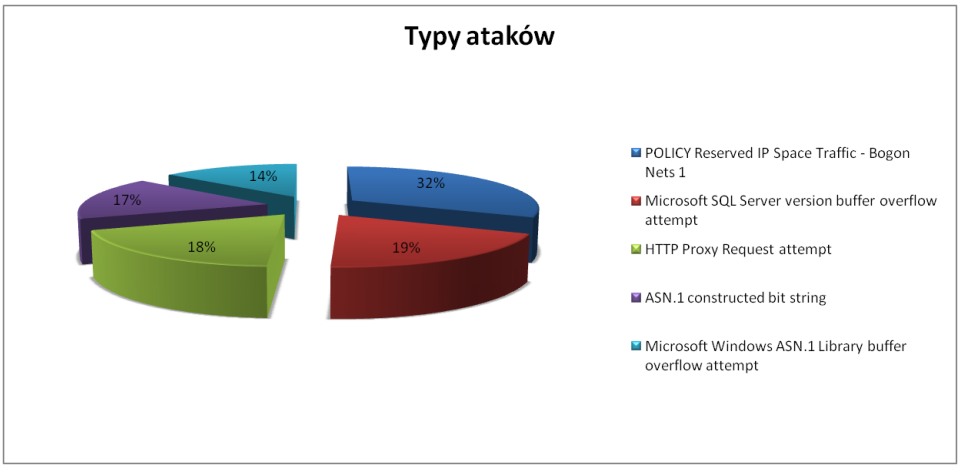
Działania zespołów bezpieczeństwa po stronie dostawców treści powodują tendencje zniżkową w ilości stron służących do wyłudzania informacji, leżących w polskiej przestrzeni adresowej.

[8] ang. b*ulletproof hosting* – usługa hostingowi polegająca na udostępnieniu przestrzeni dyskowej i łącza bez ograniczeń co do publikowanych przez usługobiorcę treści. Bardzo często tego typu hosting wykorzystywany jest przy phishingu, działaniach spamerskich lub publikacji pornografii. W przypadku tego typu usługi zapewnianej przez podziemie komputerowe, zapewniana jest także ochrona przez atakami typu DDoS.



Rysunek 14 Statystyki phishingu wg systemu Atlas

(najwyższe odnotowane udziały, najbardziej aktywnych hostów w drugim kwartale 2011r.)



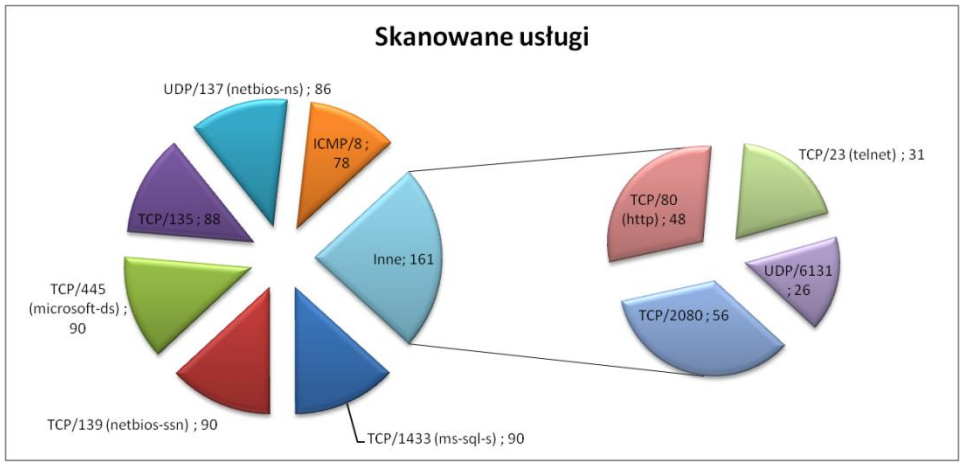
Rysunek 15 Statystyki ataków wg systemu Atlas (II kwartał 2011r.)

Pięć najczęściej występujących typów ataków wg systemu ATLAS – w drugim kwartale 2011r.

(udział procentowy liczony tylko dla tych usług)

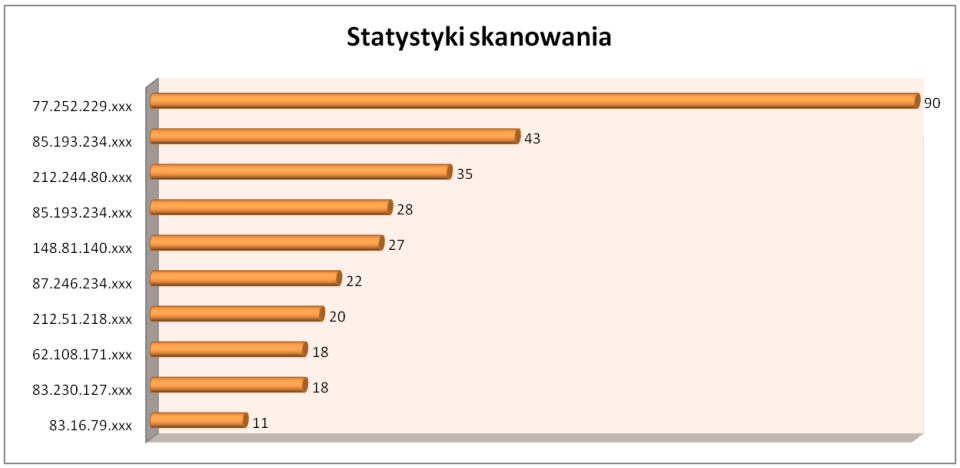
Rysunek 16 Najbardziej aktywne hosty w Polsce wg systemu ATLAS – w drugim kwartale 2011r.

(najwyższe odnotowane udziały procentowe w stosunku do pozostałych)



Rysunek 17 Statystyki skanowania wg systemu Atlas (II kwartał 2011r.)

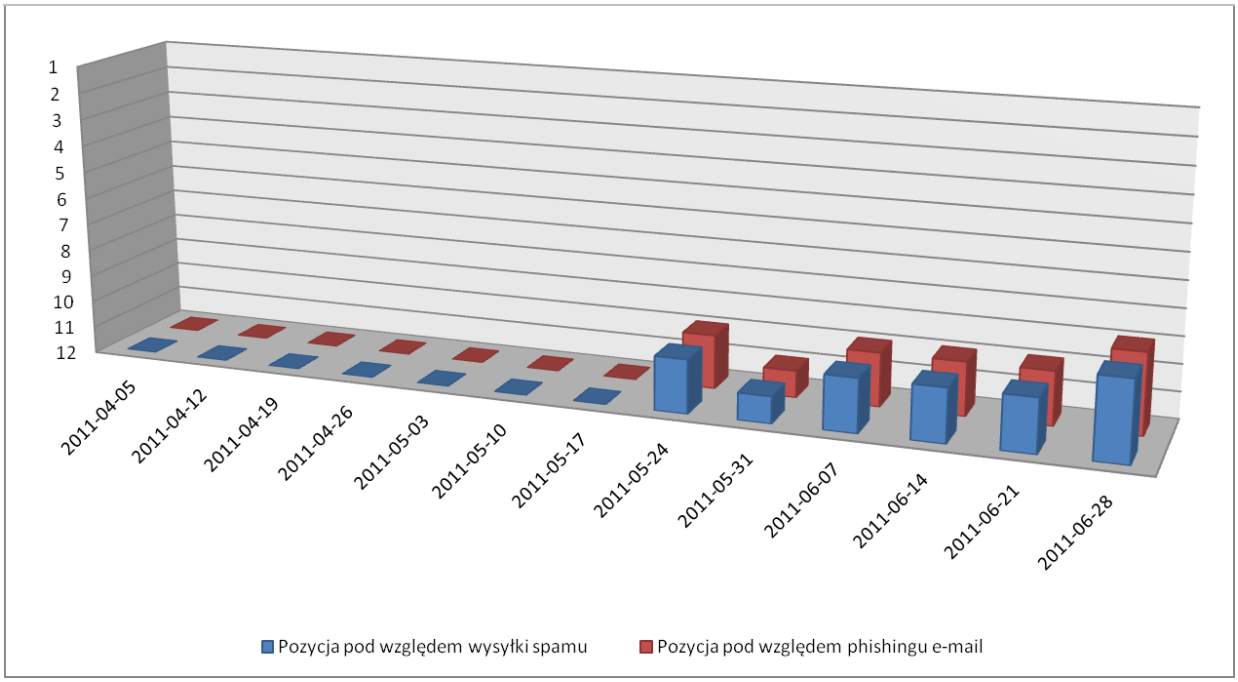
Najczęściej skanowane porty/usługi wg systemu ATLAS – w drugim kwartale 2011r.



Rysunek 18 Najbardziej aktywne hosty w Polsce wg systemu ATLAS – w drugim kwartale 2011r. (najwyższe odnotowane udziały procentowe w stosunku do pozostałych)

6.2. Inne systemy zewnętrzne

Od początku 2010 r. zbierane są informacje na temat udziału Polski pod względem zawartości niechcianych przesyłek e-mailowych[9]



Rysunek 19 – Ranking Polski pod względem wysyłanych e-maili typu „spam" oraz phishingowych (pozycje poniżej miejsca 12-go nie są raportowane)

Polska w dalszym ciągu plasuje się w dolnych częściach statystyki krajów, zarówno pod względem przesyłek phishingowych jak i ilości wysyłanego spamu. Niestety, w porównaniu do poprzednich miesięcy, wielkość niechcianego ruchu e-mail spowodowała, iż znów Polska zaklasyfikowana została w pierwszej 12-tce.

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

7. Inne działania CERT.GOV.PL

Funkcjonariusze z Rządowego Zespołu Reagowania na Incydenty Komputerowe CERT.GOV.PL w dalszym ciągu kontynuują rozpoczęty w 2010 roku cykl szkoleń z zakresu bezpieczeństwa teleinformatycznego dla środowisk szkół wyższych. Szkolenia te mają na celu podwyższanie wiedzy na temat zagrożeń pochodzących z Internetu oraz metod ich unikania. Zwiększanie bezpieczeństwa użytkowników końcowych wpływa bezpośrednio na ogólne bezpieczeństwo polskiej cyberprzestrzeni.

Po raz kolejny zespół CERT.GOV.PL wziął udział w międzynarodowych warsztatach International Cyber Defense Workshop. Warsztaty składały się zarówno z części wykładowych jak i praktycznych, a ich celem było zaznajomienie uczestników z aktualnymi trendami m.in. w zakresie najnowszych metod i sposobów stosowanych przez cyberprzestepców. Głównymi tematami były zagadnienia związane z budową, rozpowszechnianiem a także analizą plików PDF zawierających złośliwe elementy, ataków na urządzenia sterowania instalacjami przemysłowymi w świetle zagrożeń dla infrastruktury krytycznej, jakie spowodował robak Stuxnet, działań typu „man–in-the-middle" z wykorzystaniem protokołu IPv6 jak również rosnących zagrożeń dla urządzeń mobilnych.