Raport kwartalny CERT.GOV.PL
kwiecień – czerwiec 2010

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

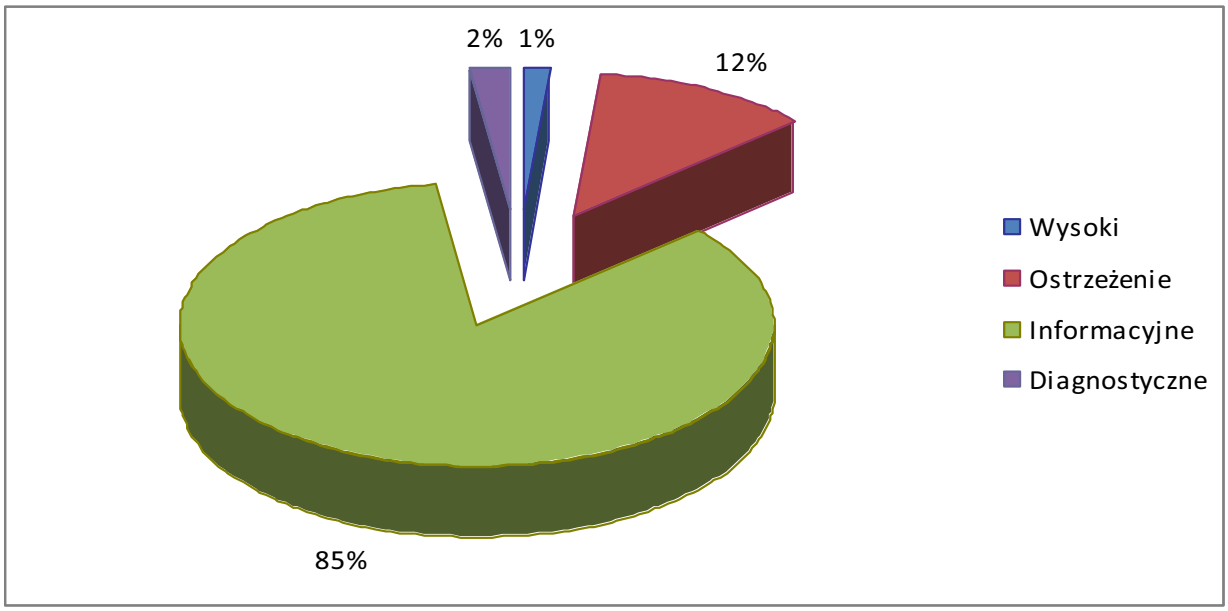
Dane kontaktowe:

- 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]

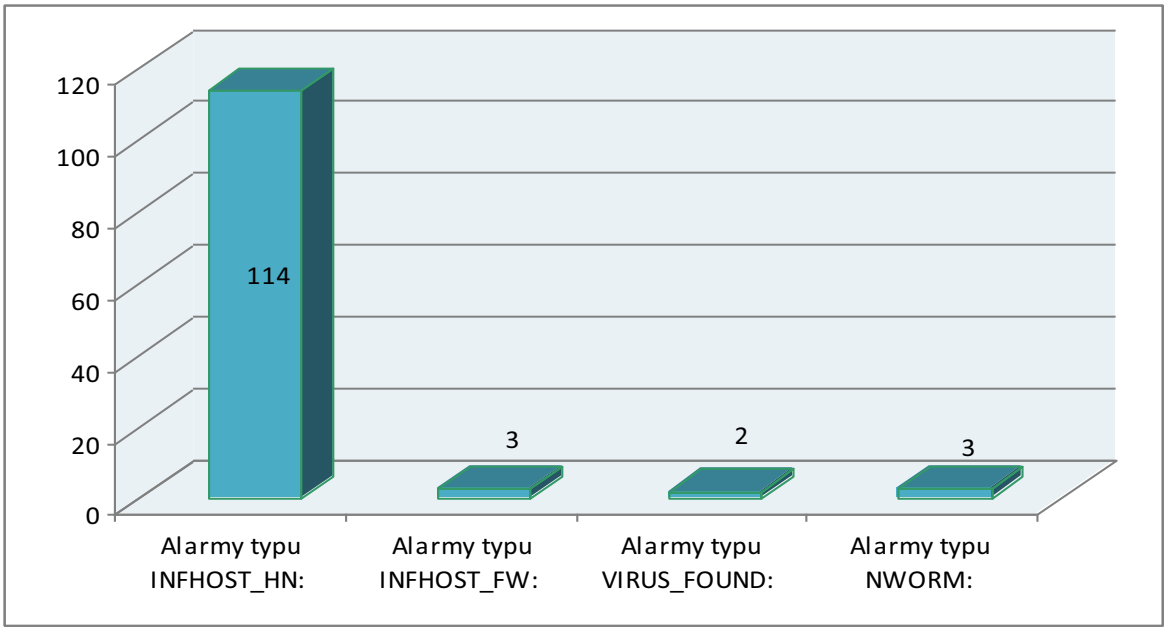
Drugi kwartał 2010 roku to zdecydowana większość alarmów informacyjnych, które stanowiły aż 85 procent wszystkich zarejestrowanych przez system ARAKIS-GOV. Alarmy o priorytecie średnim stanowiły 12%, natomiast alarmy diagnostyczne 2%. System zgłosił najmniej alarmów o priorytecie wysokim – 122 (o 11 alarmów więcej niż w I kwartale 2010 roku), co stanowiło 1% wszystkich alarmów.



Rysunek 1 – Procentowy rozkład ważności alarmów.

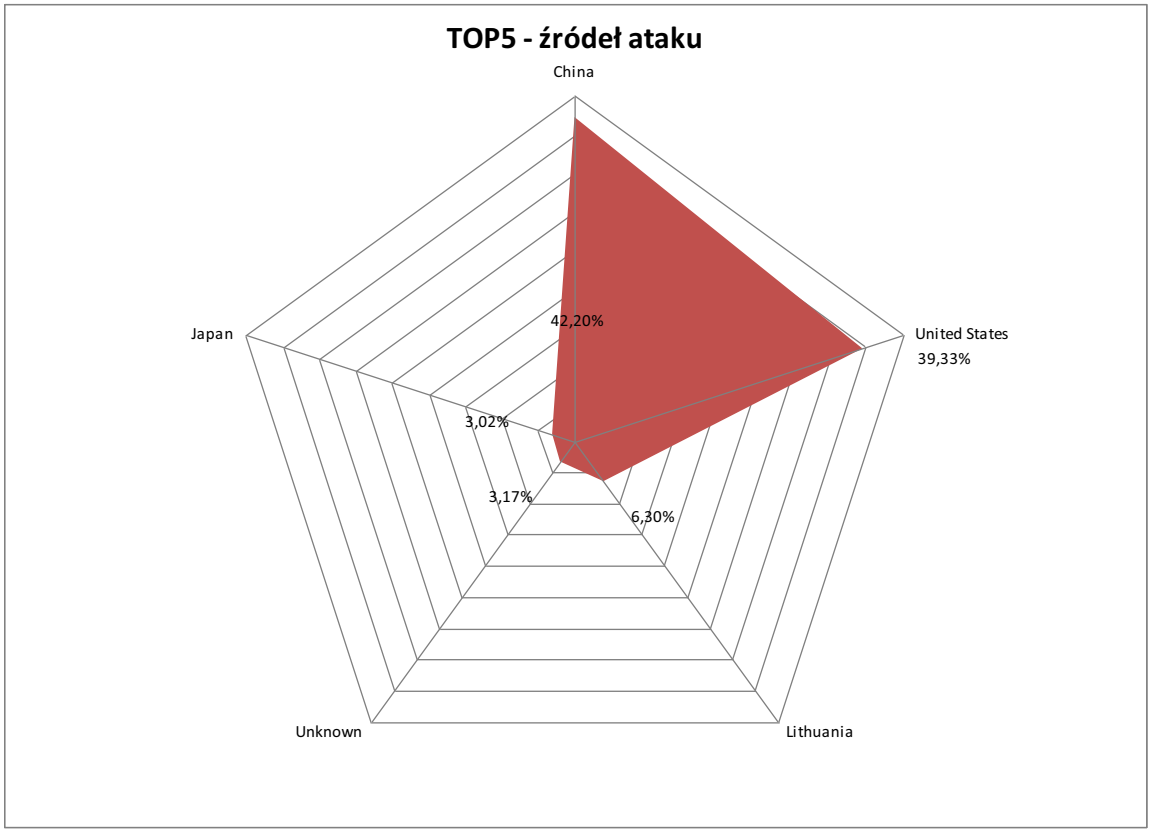
Wśród alarmów o priorytecie wysokim zaobserwowano 114 alarmów typu INFHOST_HN[2], 2 alarmy typu VIRUS_FOUND[3], 3 alarmy typu INFHOST_FW[4] a także 3 alarmy typu NWORM[5].

[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 VIRUS_FOUND oznacza wykrycie infekcji wirusowej w sieci wewnętrznej chronionej instytucji. Alarm ten generowany jest na podstawie informacji pochodzących ze skanerów antywirusowych serwerów pocztowych
[4] 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.
[5] 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.

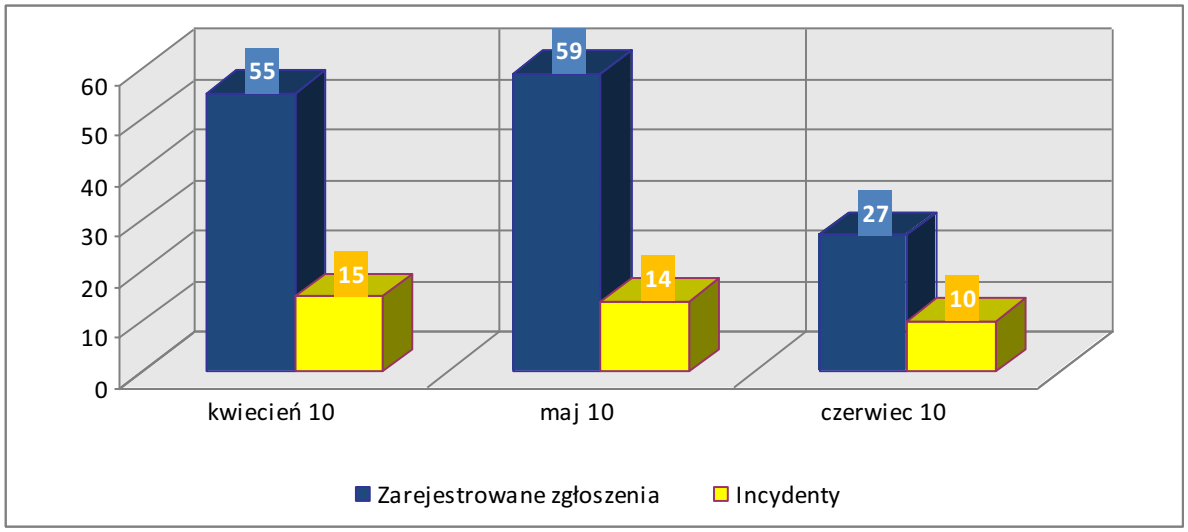
W wyniku analizy zarejestrowanych połączeń stwierdzono, iż w większości źródłem ataku były sieci komputerowe przypisane do Chin, Stanów Zjednoczonych, Litwy oraz Japonii. Jednakże mając na uwadze specyfikę protokołu TCP/IP, nie można bezpośrednio łączyć źródła pochodzenia pakietów z faktyczną lokalizacją 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).

3. Statystyki incydentów

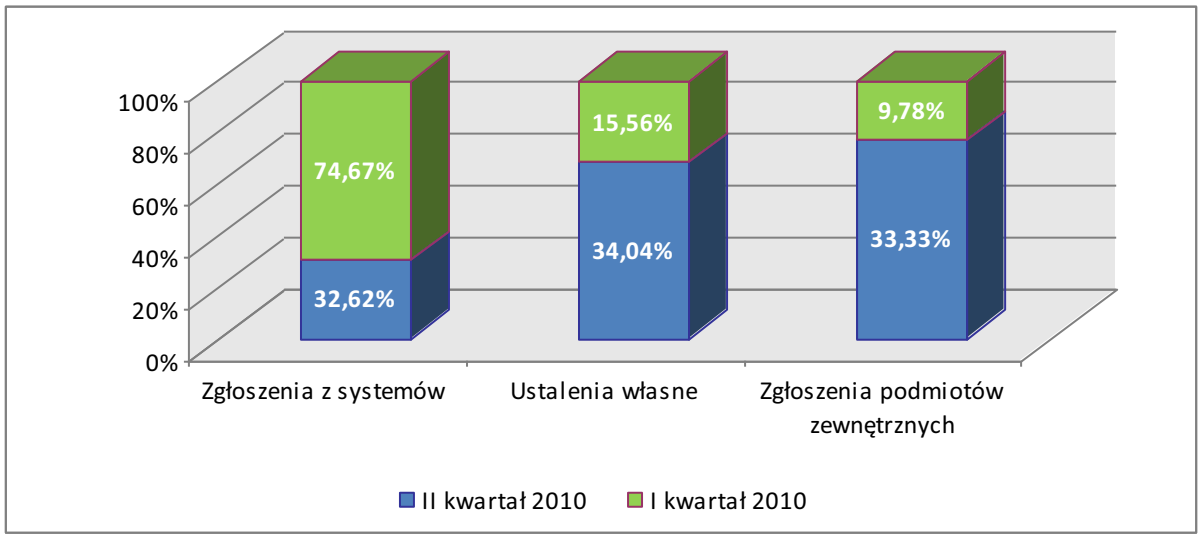
W drugim kwartale 2010 roku do zespołu CERT.GOV.PL wpłynęło 141 zgłoszeń, przy czym tylko 39 z nich zostały zakwalifikowane jako faktyczne incydenty.



Rysunek 1 - Liczba zgłoszeń oraz faktycznych incydentów w poszczególnych miesiącach drugiego kwartału 2010

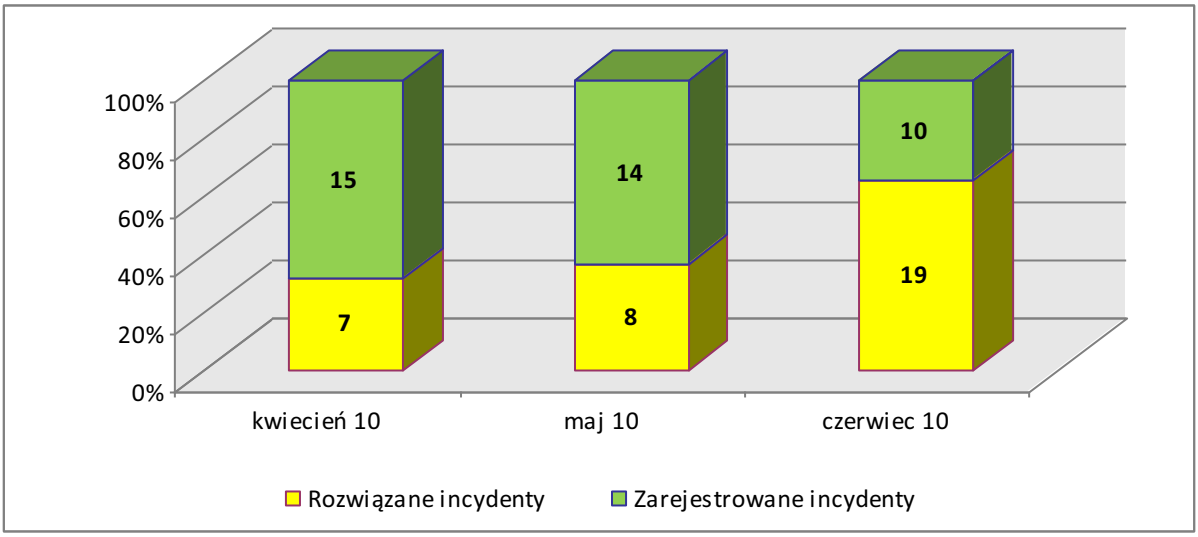
W stosunku do poprzedniego kwartału znacznie zmalała ilość zgłoszeń z systemów automatycznych – tych faktycznych, jak i tzw. „false-positive". Wynika to z uaktualnionej konfiguracji urządzeń brzegowych w jednej z instytucji biorącej udział w projekcie ARAKIS-GOV (sytuacja opisana w raporcie kwartalnym I/2010). Natomiast, co warte podkreślenia, znacznie wzrosła ilość zgłoszeń zarejestrowanych w wyniku ustaleń własnych jak i tych otrzymanych z podmiotów zewnętrznych.

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



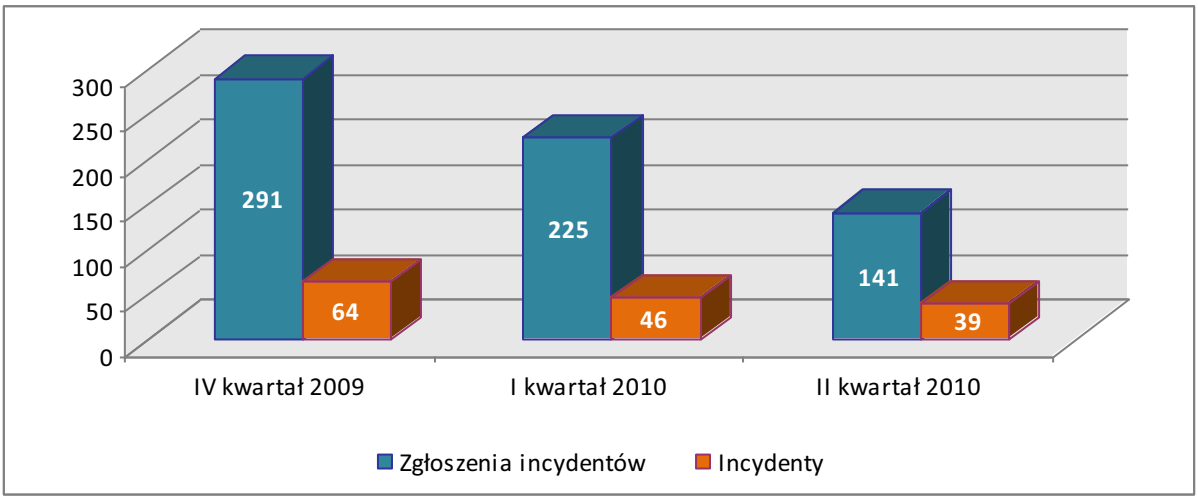
Rysunek 2 - Źródła zgłoszeń incydentów

Rozkład miesięczny incydentów zarejestrowanych i incydentów, które zostały rozwiązane, przedstawia się następująco: w kwietniu 2010 zarejestrowano 15 incydentów, z czego rozwiązano 7, w maju 2010 odnotowano 14 incydentów, z czego 8 zostało rozwiązanych, natomiast w czerwcu 2010 przyjęto do realizacji 10 incydentów z czego 19 jeszcze w tym samym miesiącu zostało zakończonych. Pozostałe incydenty są w trakcie dalszej analizy.



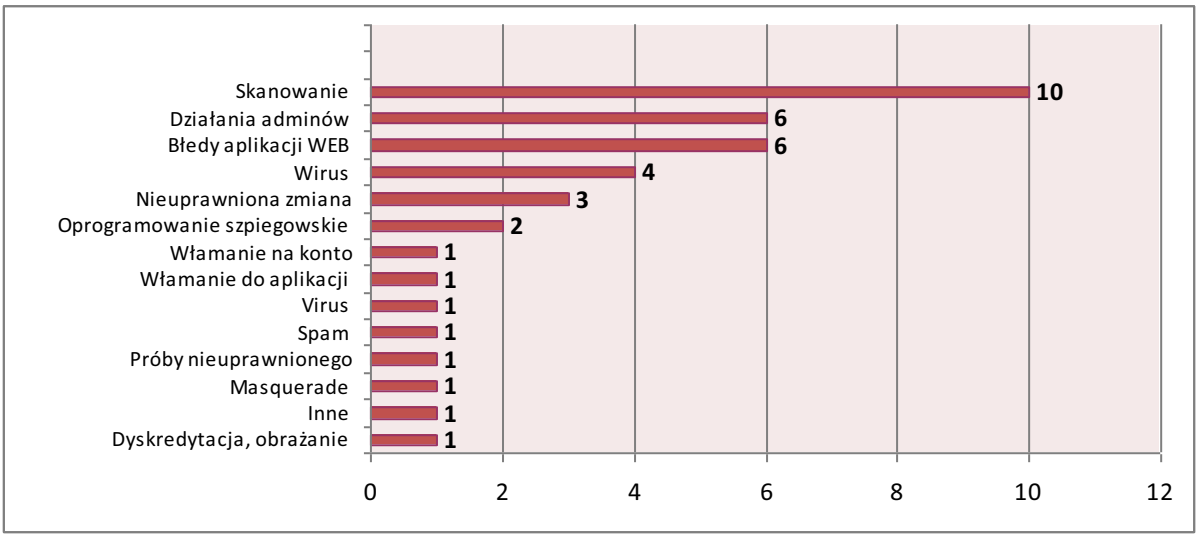
Rysunek 3 - Porównanie liczby incydentów otwartych i zamkniętych w poszczególnych miesiącach drugiego kwartału

Poniższy wykres obrazuje aktualnie utrzymującą się tendencję spadkową ilości zgłoszeń oraz faktycznych incydentów od IV kwartału 2009 roku do II kwartału 2010 roku.



Rysunek 4 – Porównanie ilości zgłoszeń incydentów i incydentów w ostatnich trzech kwartałach

Podział zarejestrowanych incydentów na kategorie przedstawia się następująco:



Rysunek 5 - Statystyka incydentów z podziałem na kategorie

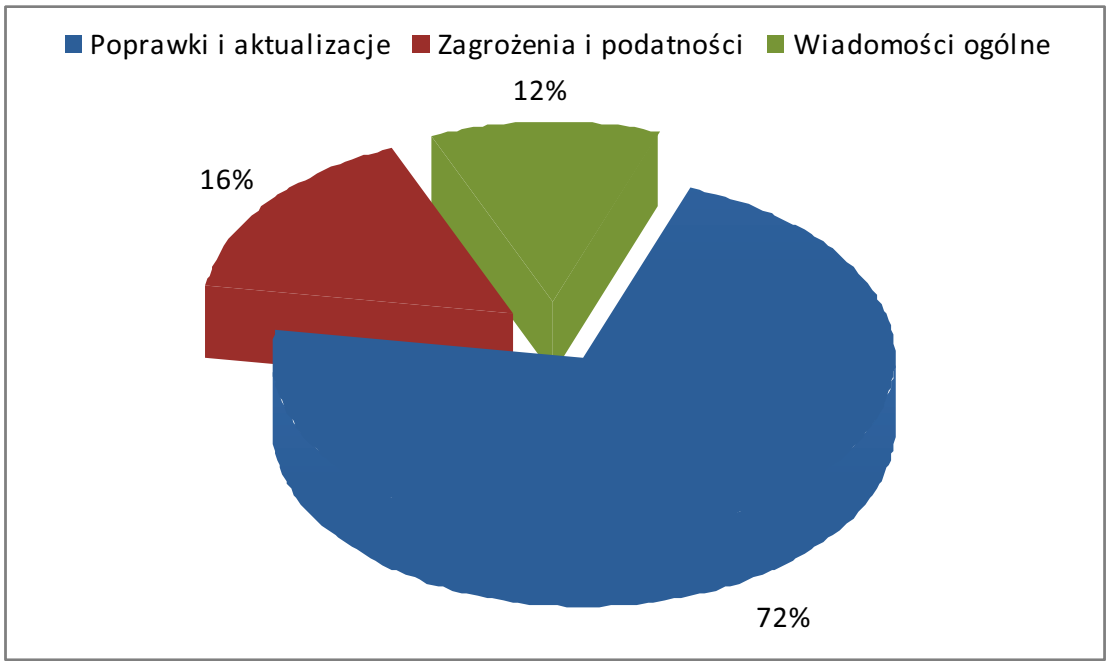
- W drugim kwartale 2010 roku Rządowy Zespół Reagowania na Incydenty Komputerowe CERT.GOV.PL odnotował ataki ukierunkowane na pracowników jednej z agend rządowych. Polegały one na wysyłaniu wiadomości e-mail z załącznikami, zainfekowanymi złośliwym oprogramowaniem rozpoznawanym tylko przez niektóre silniki antywirusowe. Treść wiadomości e-mail nawiązując do tragedii w Smoleńsku nakłaniała do otwarcia załącznika.
- W kwietniu uzyskano informację, iż na jednej ze witryn znajdujących się w domenie .edu.pl, umieszczono stronę phishingową podszywającą się pod instytucję finansową VISA. Strona została usunięta.
- W czerwcu dokonano podmiany zawartości dwunastu witryn znajdujących się w domenie mil.pl. Obsługą incydentu przekazana została do Wojskowego Biura Bezpieczeństwa Łączności i Informatyki MON.
- W maju, w dniu egzaminu maturalnego z matematyki, dokonano włamania, wraz ze zmianą zawartości witryny Centralnej Komisji Egzaminacyjnej cke.edu.pl.

4. Istotne podatności, zagrożenia i biuletyny zabezpieczeń

Witryna http://www.cert.gov.pl jest źródłem specjalistycznych informacji związanych z bezpieczeństwem teleinformatycznym. Publikowane są tam między innymi aktualne informacje dotyczące istotnych zagrożeń, nowych podatności w popularnych systemach i aplikacjach, najpopularniejszych formach ataków sieciowych oraz sposobach ochrony przed zagrożeniami. Dodatkowo na powyższej witrynie umieszczane są biuletyny bezpieczeństwa udostępnione przez producentów sprzętu i oprogramowania.

W drugim kwartale 2010 roku na witrynie www.cert.gov.pl dodano:

- 23 publikacje w kategorii „Poprawki i aktualizacje”,
- 5 publikacji w kategorii „Zagrożenia i podatności”,
- 4 publikacje w kategorii „Wiadomości ogólne”.



Rysunek 6 - Procentowy rozkład publikacji na witrynie www.cert.gov.pl

Najbardziej istotne publikacje dotyczące zagrożeń w drugim kwartale 2010 roku dotyczyły:

- **Comiesięcznych biuletynów bezpieczeństwa firmy Microsoft**

Kwietniowy Biuletyn Bezpieczeństwa:

Kwietniowy Biuletyn Bezpieczeństwa informował o wykryciu oraz usunięciu jedenastu poważnych błędów. Pięć otrzymało status „krytyczny”, kolejne pięć zakwalifikowano jako „ważne”, ostatni jeden określono mianem „umiarkowany”. Luki o statusie „krytyczny” pozwalały na zdalne wykonanie kodu.

1. MS10-019 – biuletyn dotyczący błędów w zabezpieczeniach systemu Windows Authenticode Verification - krytyczny
2. MS10-020 – biuletyn dotyczący podatności protokołu SMB (Server Message Block) – krytyczny

3. MS10-025 – biuletyn dotyczący podatności komponentu Windows Media Services w systemie Microsoft Windows 2000 Server - krytyczny
4. MS10-026 – biuletyn dotyczący błędów kodeków audio Microsoft MPEG Layer-3 - krytyczny
5. MS10-027 – biuletyn dotyczący luki w oprogramowaniu Windows Media Player - krytyczny
6. MS10-021 – biuletyn dotyczący błędów w jądrze systemu Windows - ważny
7. MS10-022 – biuletyn dotyczący usterki w VBScript (Visual Basic Scripting Edition) - ważny
8. MS10-023 – biuletyn dotyczący błędów oprogramowania Microsoft Office Publisher - ważny
9. MS10-024 – biuletyn dotyczący luki w Windows Microsoft Exchange i SMTP Service - ważny
10. MS10-028 – biuletyn dotyczący podatności oprogramowania Microsoft Office Visio - ważny
11. MS10-029 – biuletyn dotyczący błędów w jądrze systemu Windows – umiarkowany

Majowy Biuletyn Bezpieczeństwa:

Majowy Biuletyn Bezpieczeństwa informował o wykryciu oraz usunięciu dwóch poważnych błędów. Wszystkie otrzymały status „krytyczny”.

1. MS10-030 – biuletyn dotyczący podatności aplikacji Outlook Express, Windows Mail oraz Windows Live Mail - krytyczny
2. MS10-031 – biuletyn dotyczący luki w zabezpieczeniach programu Microsoft Visual Basic for Applications – krytyczny

Czerwcowy Biuletyn Bezpieczeństwa:

Czerwcowy biuletyn bezpieczeństwa informował o wykryciu oraz usunięciu dziesięciu biuletynów bezpieczeństwa. Trzy otrzymały status „krytyczny”, pozostałe siedem zostały sklasyfikowane jako „ważne”.

1. MS10-033 – biuletyn dotyczący błędów w jądrze systemu Windows - krytyczny
2. MS10-034 – biuletyn dotyczący błędów w jądrze systemu Windows - krytyczny
3. MS10-035 – zbiorcza aktualizacja zabezpieczeń dla programu Internet Explorer – krytyczny
4. MS10-032 – biuletyn dotyczący usterek w trybie jądra sterowników systemu Microsoft Windows - ważny
5. MS10-036 – biuletyn dotyczący podatności pakietu oprogramowania Microsoft Office - ważny
6. MS10-037 – biuletyn dotyczący błędów w sterowniku Windows OpenType Compact Font Format (CFF) - ważny
7. MS10-038 – zbiorcza aktualizacja zabezpieczeń dla pakietu Microsoft Office - ważny
8. MS10-039 – biuletyn dotyczący podatności programu Microsoft SharePoint - ważny
9. MS10-040 – biuletyn dotyczący błędów w usłudze IIS (Internet Information Services) - ważny
10. MS10-041 – biuletyn dotyczący podatności Microsoft .NET Framework – ważny

- **Biuletynów bezpieczeństwa dla produktów Adobe**

Rządowy Zespół Reagowania na Incydenty Komputerowe informował o:

1. Błędach w oprogramowaniu Adobe Reader i Adobe Acrobat, mogących doprowadzić do przejęcia kontroli nad zaatakowanym komputerem.
2. Biuletynie bezpieczeństwa Adobe APSA 10-01 dotyczącym likwidacji wykrytych podatności programów Adobe Flash Player, Reader oraz Acrobat. Wykorzystanie tych luk umożliwiło zdalne wykonanie kodu oraz w rezultacie przejęcie kontroli nad zaatakowanym systemem.

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

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

1. Cisco Secure Desktop – błędy komponentów ActiveX, które pozwalały osobie atakującej na wykonanie dowolnego kodu.
2. Cisco PGW 2200 Softswitch – odnotowano wiele usterek, które mogły zostać wykorzystane do przeprowadzenia ataku typu Dos (Denial of Sernice).

- **Wykrytych podatnościach w produktach VMware**

Opublikowano informacje na temat błędów w VMware ESX oraz vCENTER, podatnych na przeprowadzenie ataku DoS (Denial of Service).
Na stronie www.cert.gov.pl opublikowano również informację o usunięciu poważnego błędu w oprogramowaniu ESX 3.5 COS (Console Operating System), którego skutkiem mogło być przeprowadzenie ataku typu DoS.

- **Critical Patch Update dla produktów Oracle**

Opublikowany został biuletyn bezpieczeństwa łatająca 47 istotnych luk w produktach Oracle. Poprawki usuwały błędy w niżej wymienionych programach:

1. Oracle Database Server – 7 poprawek bezpieczeństwa
2. Oracle Fusion Middleware – 5 poprawek bezpieczeństwa
3. Oracle Collaboration Suite – 1 poprawka bezpieczeństwa
4. Oracle Application Suite – 8 poprawek bezpieczeństwa
5. PeopleSoft i JD Edwards Suite – 4 poprawki bezpieczeństwa
6. Oracle Industry Applications – 6 poprawek bezpieczeństwa
7. Oracle Solaris Products Suite – 16 poprawek bezpieczeństwa

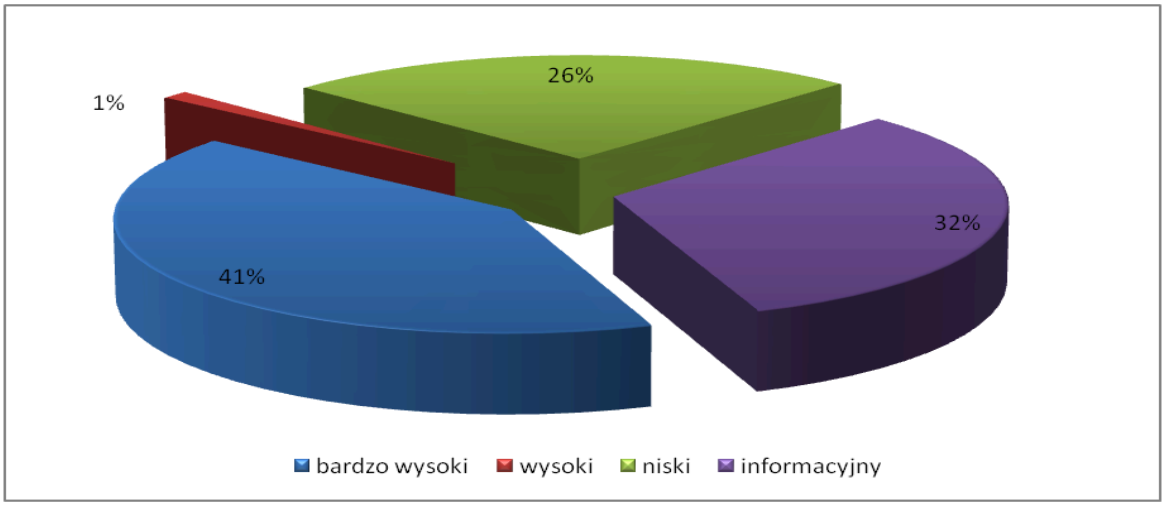
- **Podatności i poprawki dla użytkowników systemu Mac OS**

1. Zespół CERT.GOV.PL zamieścił na stronie szczegółowe informacje na temat pakietu aktualizacyjnego dla systemu operacyjnego Mac OS X.

5. Testy bezpieczeństwa witryn WWW instytucji państwowych

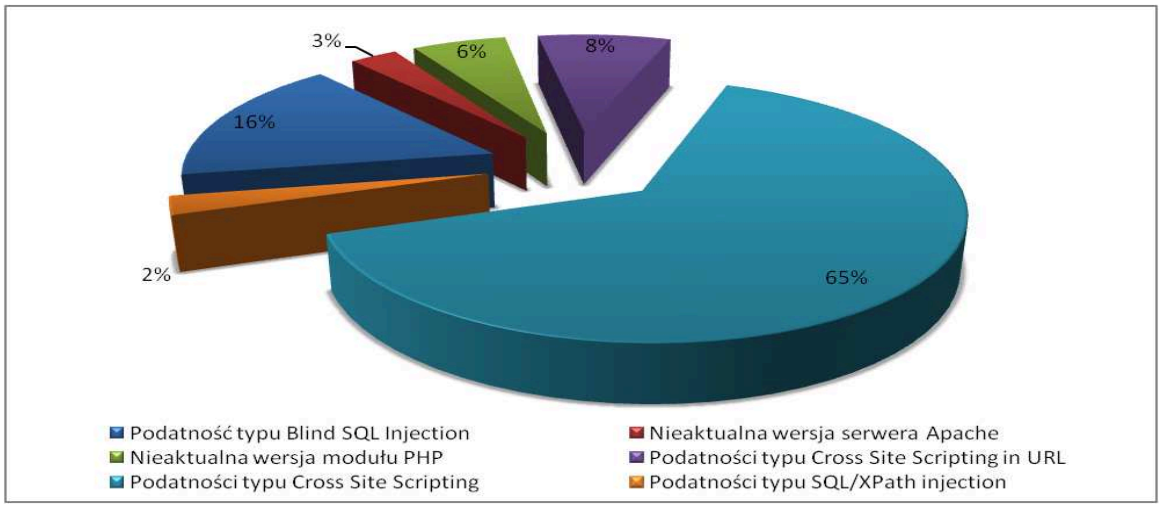
Zespół CERT.GOV.PL kontynuował testy bezpieczeństwa witryn WWW należących do instytucji państwowych.

W II kwartale 2010 roku przebadano 18 witryn należących do 10 instytucji państwowych. Stwierdzono ogółem 515 błędów w tym: 212 błędów o bardzo wysokim poziomie zagrożenia, 6 błędów o wysokim poziomie zagrożenia, 132 błędy o niskim poziomie zagrożenia i 165 błędów oznaczonych jako informacyjne.



Rysunek 7 - 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/XPath Injection. Istotnym problemem jest również wykorzystywanie w serwerach produkcyjnych nieaktualnych wersji oprogramowania.



Rysunek 8 - Procentowy rozkład najpoważniejszych błędów

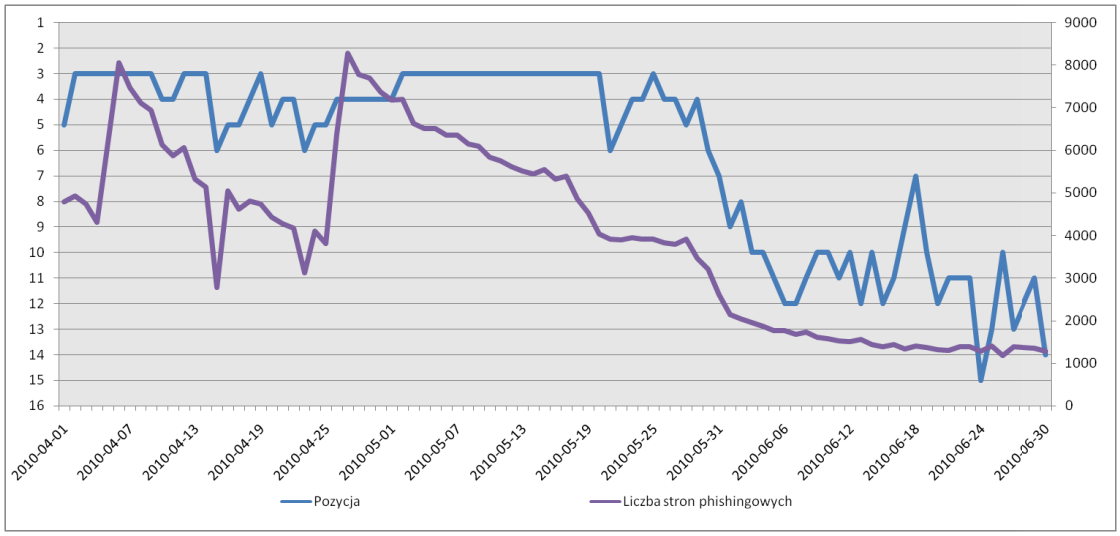
Należy zwrócić uwagę, iż podatności krytyczne najczęściej znajdują się w warstwie usługowej systemu (np. serwerze http czy frontendzie do bazy danych), a nie w warstwie systemu operacyjnego. Jak widać, obecnie największe zagrożenie dla bezpieczeństwa stanowią błędy w aplikacjach, które są budowane, konfigurowane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

6. Informacje z systemów zewnętrznych

6.1. System ATLAS

System ATLAS[6] gromadzi informacje na temat zagrożeń teleinformatycznych w Internecie 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 należy odnotować wyraźny spadek pozycji Polski w niechlubnym rankingu krajów stwarzających zagrożenie dla bezpieczeństwa Internetu. Na koniec okresu raportowania, Polska znajduje się poza pierwszą dziesiątką. Działania zespołów bezpieczeństwa pozwoliły na wyraźne zmniejszenie ilości stron służących do wyłudzania danych, co w bezpośredni sposób przełożyło się na pozycję Polski w rankingu ATLAS.



Rysunek 9 - Pozycja Polski w rankingu ATLAS i jej związek z phishingiem

Liczba systemów C&C (nieujęta na powyższym wykresie) utrzymuje się niestety na stałym poziomie.

Po raz kolejny, korelacja publikacji exploitów na jeden z systemów zarządzania treścią ze skokiem ilości hostowanych na polskich serwerach stron phishingowych 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[7].

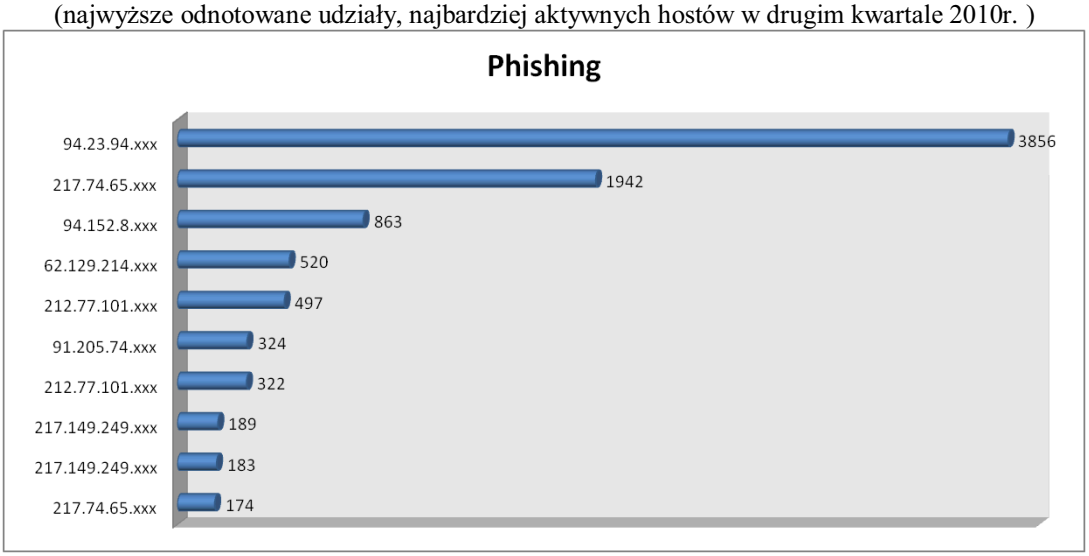
W większości przypadków strony służące do wyłudzania informacji znajdują się w prywatnych zasobach WWW. Zazwyczaj ich właściciele nie wiedzą o włamaniu, ponieważ

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

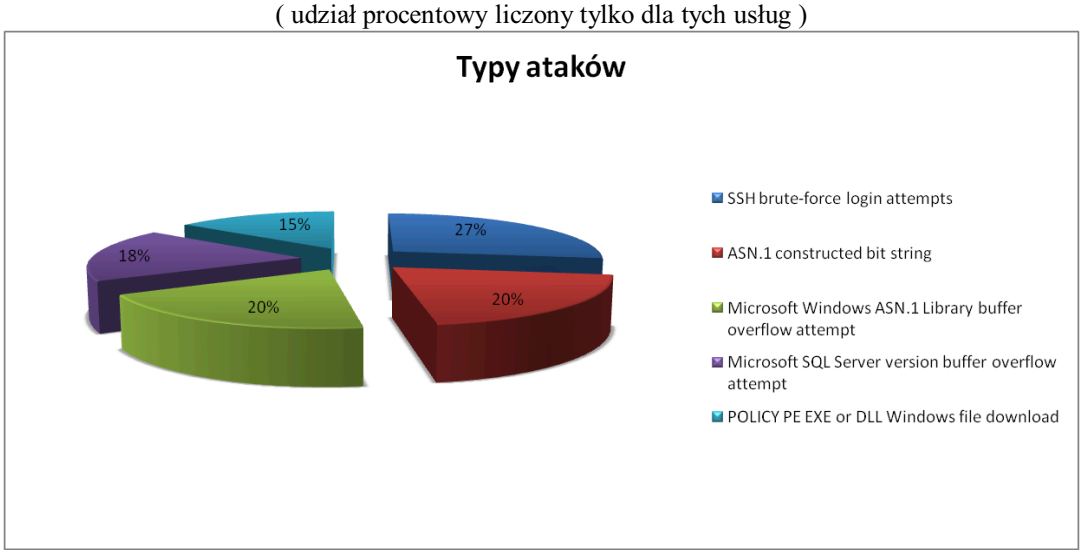
[7] ang. *bulletproof hosting* – usługa hostingowi polegająca na udostępnieniu przestrzeni dyskowej i łącza bez ograniczeń co do publikowanych przez usługobiorcę treści. Bardzo często tego typu hosting wykorzystywany jest przy phishingu, działaniach spamerskich lub publikacji pornografii. W przypadku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

treść phishingowa jest jedynie dodawana, bez zmiany dotychczasowej zawartości stron w danej witrynie, co pozwala ukryć przed właścicielem dodanie nielegalnych treści.

Statystyki phishingu wg systemu Atlas
(najwyższe odnotowane udziały, najbardziej aktywnych hostów w drugim kwartale 2010r.)



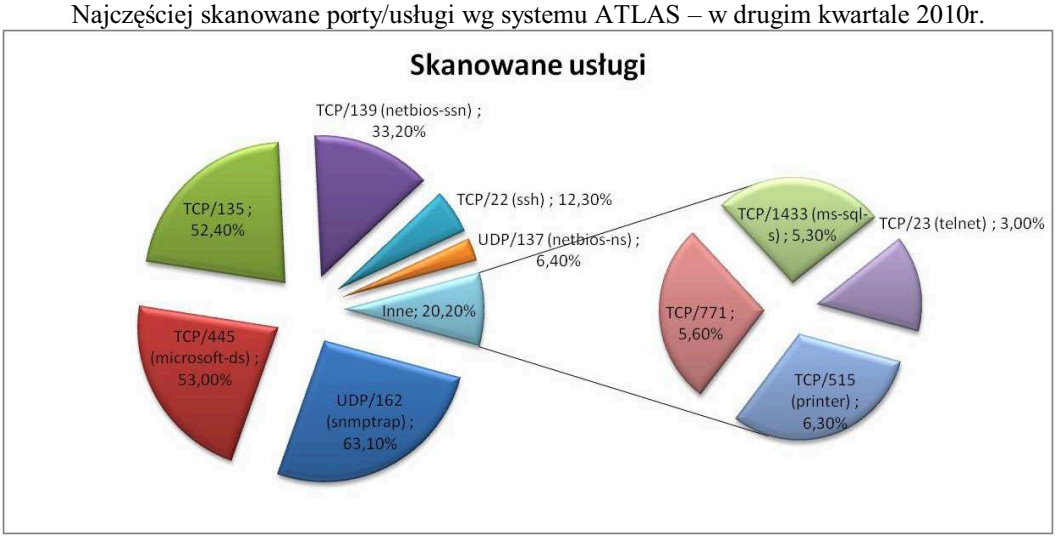
Statystyki ataków wg systemu Atlas (II kwartał 2010r.)
Pięć najczęściej występujących typów ataków wg systemu ATLAS – w drugim kwartale 2010r.
(udział procentowy liczony tylko dla tych usług)



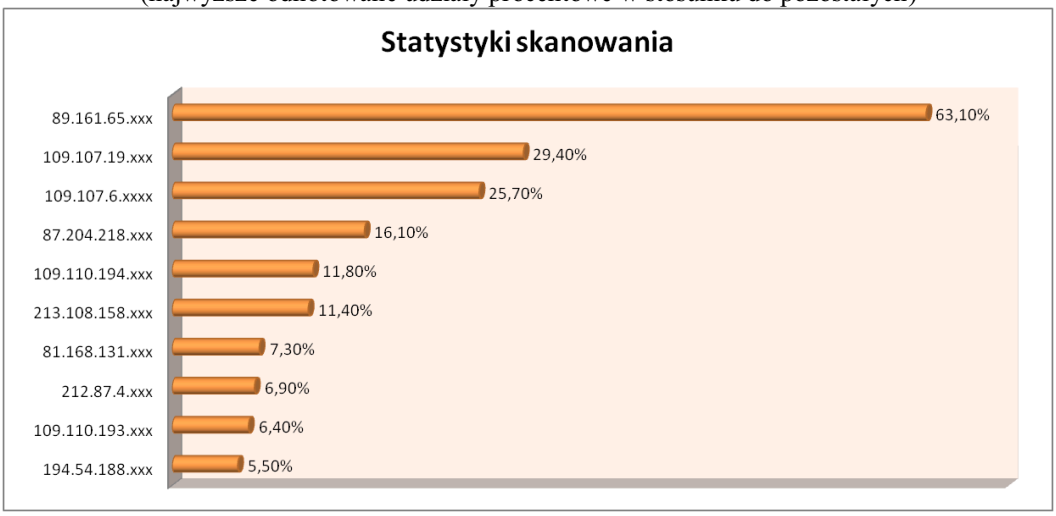
Najbardziej aktywne hosty w Polsce wg systemu ATLAS – w drugim kwartale 2010r.
(najwyższe odnotowane udziały procentowe w stosunku do pozostałych)

Statystyki skanowania wg systemu Atlas (II kwartał 2010r.)

Najczęściej skanowane porty/usługi wg systemu ATLAS – w drugim kwartale 2010r.

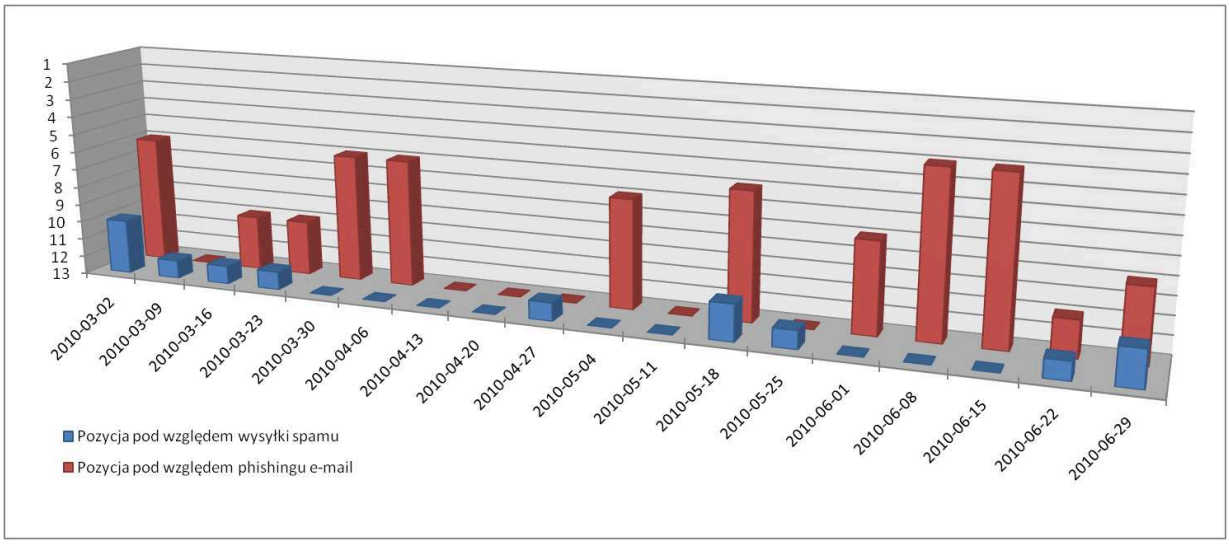


Najbardziej aktywne hosty w Polsce wg systemu ATLAS – w drugim kwartale 2010r.
(najwyższe odnotowane udziały procentowe w stosunku do pozostałych)



6.2. Inne systemy zewnętrzne

Od początku 2010 r. zbierane są informacje na temat udziału Polski pod względem zawartości niechcianych przesyłek e-mailowych[8]



Rysunek 10 – Ranking Polski pod względem wysyłanych e-maili typu „spam" oraz phishingowych (pozycje poniżej miejsca 12-go nie są raportowane)

Należy zwrócić uwagę, iż pod względem przesyłek phishingowych Polska w dalszym ciągu plasuje się na wysokich miejscach. Biorąc pod uwagę ogólną ilość spamu wysyłanego z polskich podsieci sytuacja przedstawia się lepiej - Polska znajduje się praktycznie poza pierwszą 10-tką, a przez połowę okresu nie jest nawet klasyfikowana. Próby ograniczenia wysyłki niechcianych informacji przynoszą jedynie chwilową poprawę sytuacji, albowiem cyberprzestępcy bardzo szybko przystosowują metody swoich działań do nowych warunków.

W dalszym ciągu prowadzona jest analiza (na podstawie informacji zewnętrznych) ilości komputerów zainfekowanych złośliwym oprogramowaniem znajdujących się w obszarze polskiej cyberprzestrzeni. Komputer zainfekowany rozumiany jest jako pojedyncza maszyna na której znajduje się przynajmniej jeden program należący do jednego z poniższych typów:

- Trojan;
- Worm;
- Wirus;
- Backdoor;
- Adware.

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

Rysunek 11 – Procentowy poziom zawirusowanych komputerów w okresie II-go kwartału 2010r.[9]

Wyraźnie widać wpływ pojawiania się nowych wersji wirusów i opóźnienie w instalowaniu szczepionek w programach antywirusowych – następuje wyraźny skok, a następnie spadek liczby zainfekowanych komputerów. W żadnym momencie poziom ilości zawirusowanych komputerów nie spadł poniżej 5%. Należy pamiętać, iż statystyka odnosi się do komputerów włączonych w danym okresie (dane zbierane są co 15 minut). Ze względów technicznych, statystyka obejmuje jedynie komputery pracujące pod kontrolą systemu operacyjnego Windows.

Analizując powyższe informacje można stwierdzić, iż pod względem stanowienia potencjalnego zagrożenia dla użytkowników Internetu, Polska przestaje zajmować wysokie miejsca. Aktualnie obszarem, w którym nadal jest wysoko klasyfikowana jest wysyłanie spamu. Zwrócić należy jednak uwagę na fakt, iż spam jest (stosunkowo) najmniej szkodliwym działaniem. Pod względem zagrożeń aktywnych (ataki, rozsyłanie wirusów, skanowania, próby wywołania odmowy dostępu /DDoS/) Polska praktycznie znajduje się poza przedziałem klasyfikowanym.

[9] Na podstawie informacji otrzymywanych od f-my Panda Security (http://www.pandasecurity.com)

7. Inne działania CERT.GOV.PL

Po raz kolejny funkcjonariusze Agencji Bezpieczeństwa Wewnętrznego z Rządowego Zespołu Reagowania na Incydenty Komputerowe CERT.GOV.PL oraz Laboratorium Elektronicznych Nośników Informacji godnie zaprezentowali stronę polską w międzynarodowych warsztatach International Cyber Demence Workshop (ICDW), zorganizowanych w dniach 21-25 czerwca 2010 roku przez Departament Obrony USA.

Celem ćwiczeń ICDW było podniesienie poziomu kompetencji rządowych i wojskowych służb odpowiedzialnych za cyberbezpieczeństwo w swoich krajach oraz wypracowanie metod współdziałania w przypadku zagrożeń pochodzących z sieci Internet. Poprzez analizę przypadków typowych incydentów oraz dyskusje ze specjalistami z całego świata, podnoszony jest poziom wiedzy i kompetencji zespołów odpowiedzialnych za cyberbezpieczeństwo, jak również doskonalenie technik obrony przed atakami i analizy powłamaniowej.

Zwyczajowo, na zakończenie warsztatów, odbyły się zawody krajowych zespołów bezpieczeństwa, w których – spośród 19 zespołów z całego świata – Agencja Bezpieczeństwa Wewnętrznego zdobyła największą liczbę punktów. Jest to kolejny sukces funkcjonariuszy ABW, którzy w poprzednich edycjach międzynarodowych warsztatów, w czerwcu i listopadzie 2009 roku, również zajęli pierwsze miejsce.