Agencja Bezpieczeństwa Wewnętrznego

Raport kwartalny CERT.GOV.PL
styczeń – marzec 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

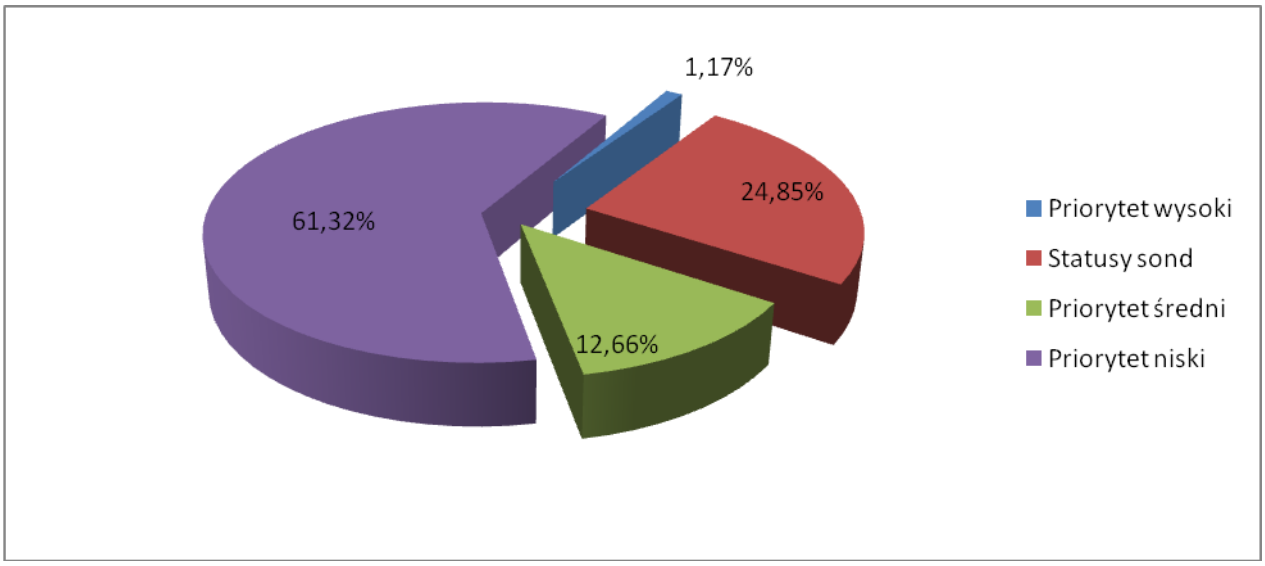
Dane kontaktowe:

- 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]

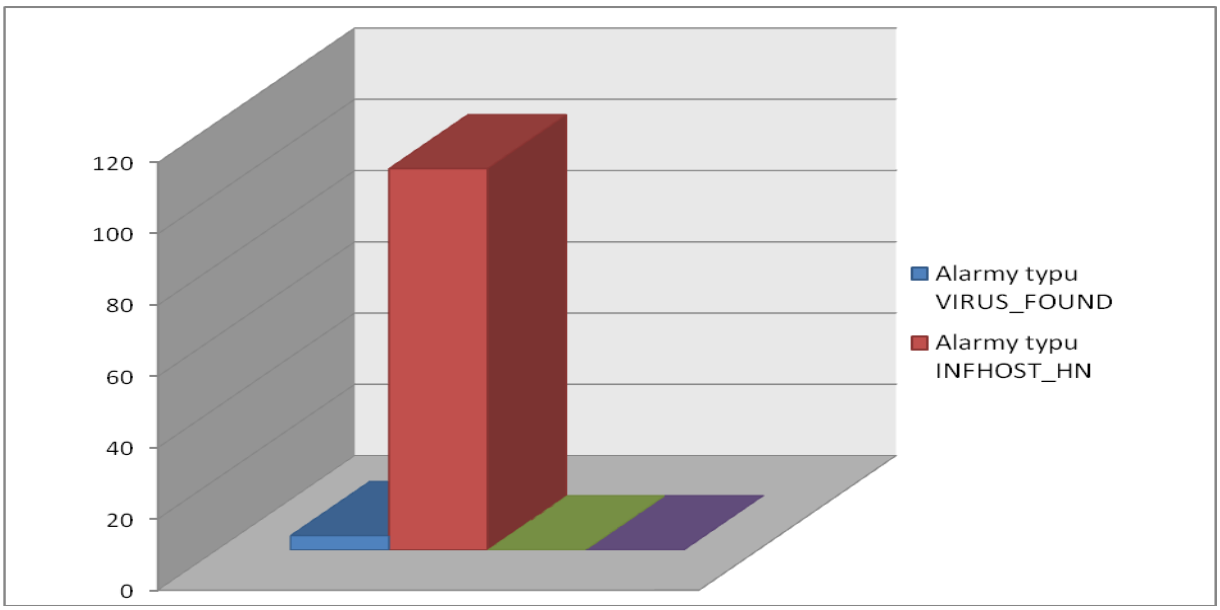
Pierwszy kwartał 2010 roku to zdecydowana większość alarmów informacyjnych, które stanowiły przeszło 61 procent wszystkich zarejestrowanych przez system ARAKIS-GOV. Alarmy o priorytecie średnim stanowiły 12,66%, natomiast diagnostyczne 24,85%. System zgłosił 111 alarmów o priorytecie wysokim, co stanowiło 1,17% wszystkich alarmów.



Rysunek 1 – Procentowy rozkład ważności alarmów.

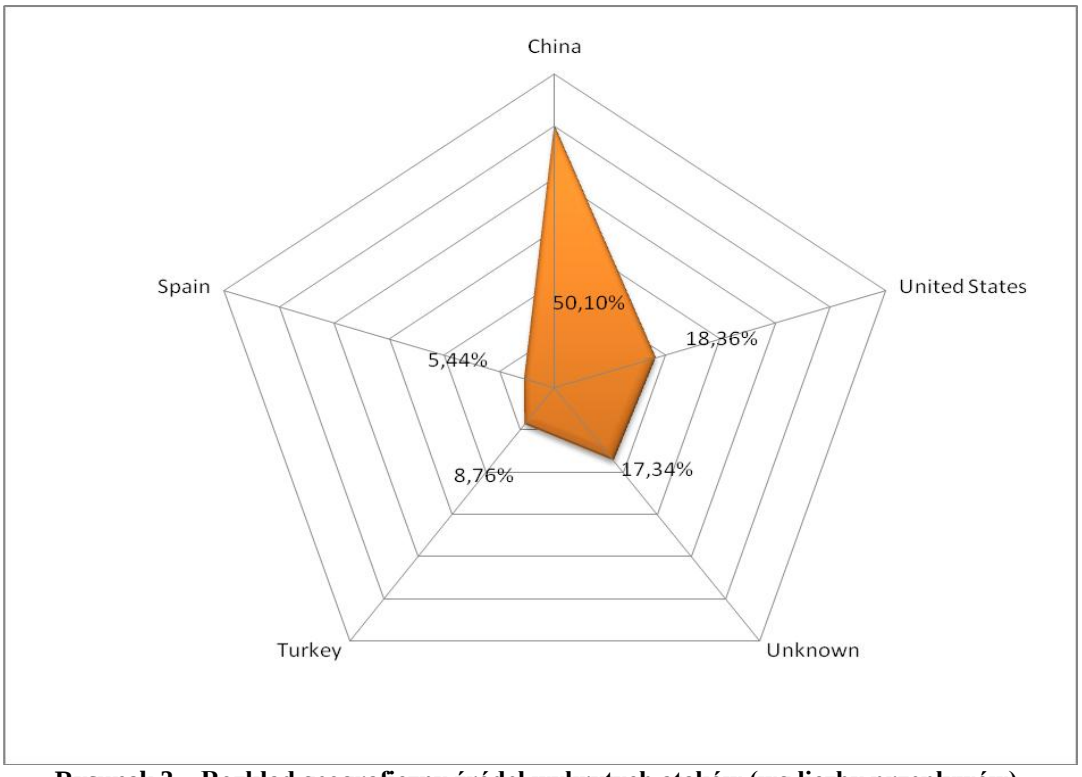
Wśród alarmów o priorytecie wysokim zaobserwowano 107 typu INFHOST_HN[2] oraz 4 typu VIRUS_FOUND[3]. Nie stwierdzono alarmów typu INFHOST_FW[4], a także NWORM[5].

[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)



Rysunek 2 – Statystyki alarmów o wysokim priorytecie.

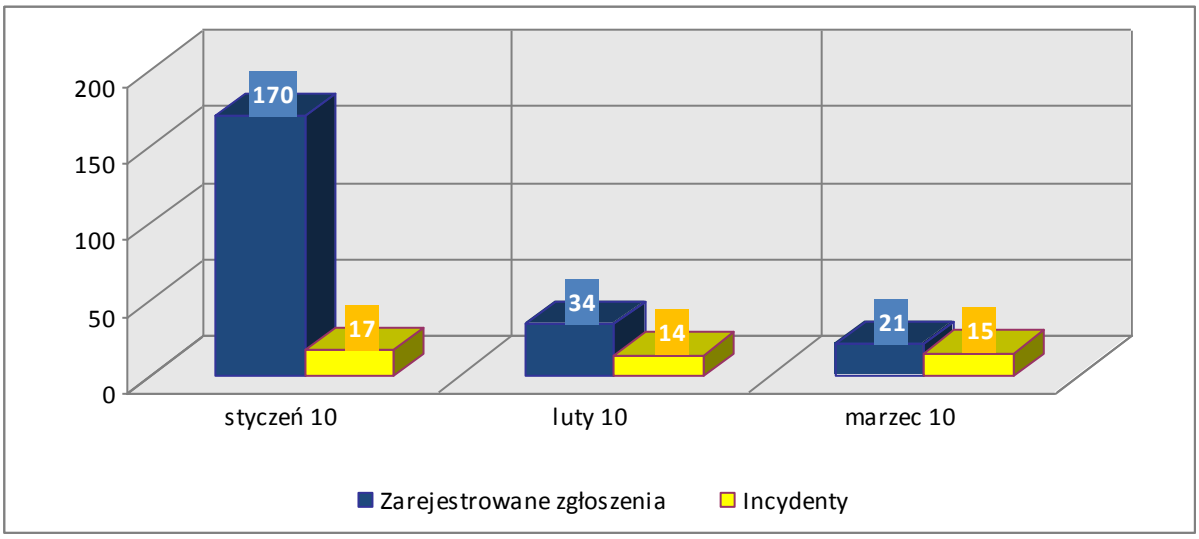
W wyniku analizy zarejestrowanych połączeń stwierdzono, iż w większości źródłem ataku były sieci komputerowe przypisane do Chin, Stanów Zjednoczonych, Turcji oraz Hiszpanii. Jednakże mając na uwadze specyfikę protokołu TCP/IP, nie można bezpośrednio łączyć źródła pochodzenia pakietów z faktyczną lokalizacją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



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

3. Statystyki incydentów

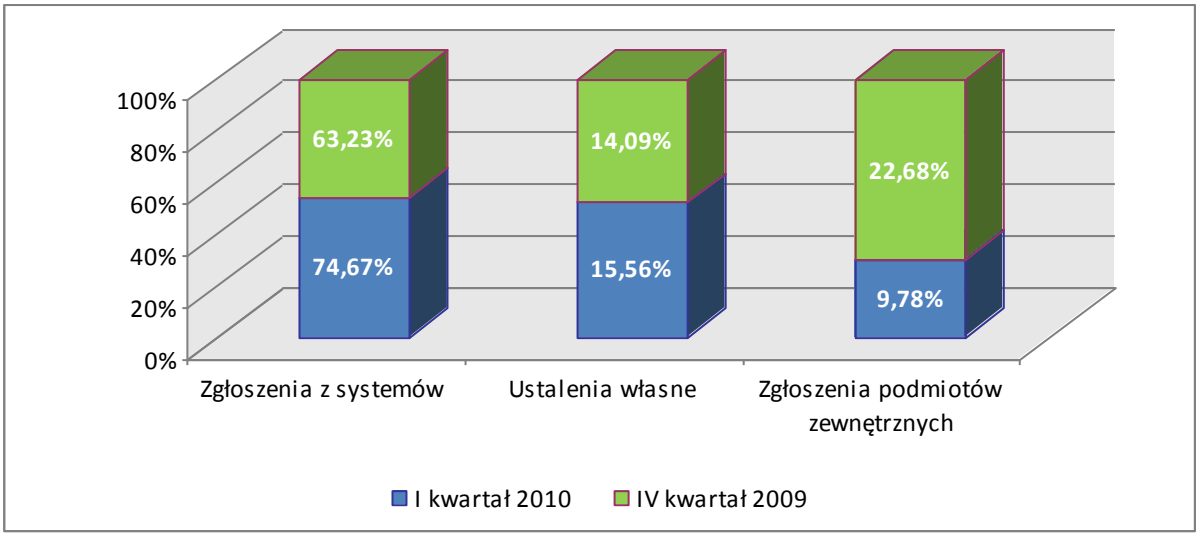
W pierwszym kwartale 2010 roku do zespołu CERT.GOV.PL wpłynęło 225 zgłoszeń, przy czym tylko 46 z nich zostały zakwalifikowane jako faktyczne incydenty.



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

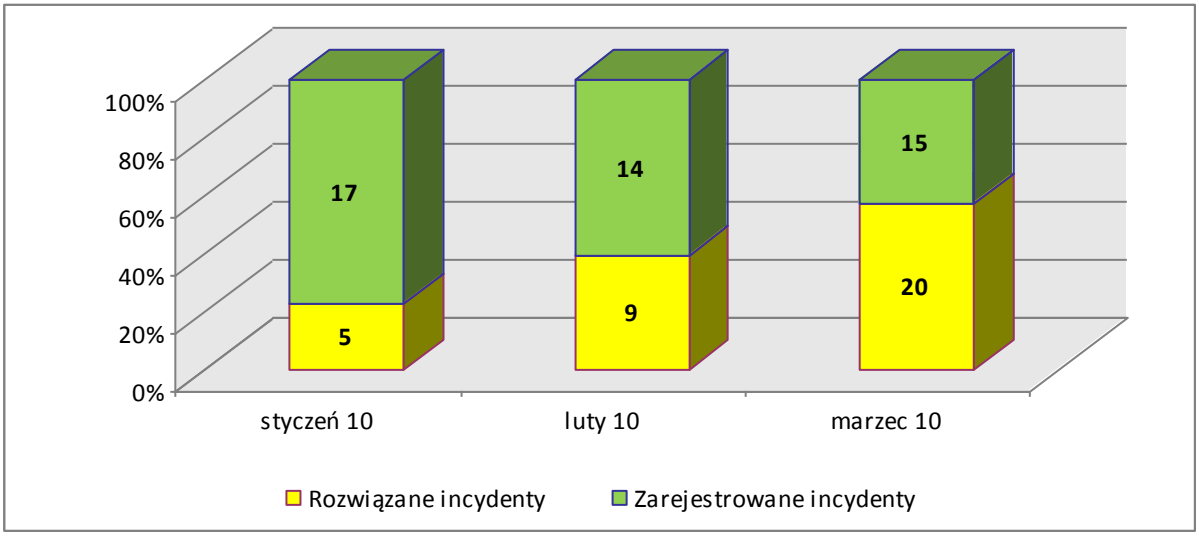
W miesiącu styczniu odnotowano znaczną ilość zgłoszeń. Powyższa sytuacja wynikała z błędnej konfiguracji urządzeń brzegowych w jednej z instytucji biorącej udział w projekcie ARAKIS-GOV. Ponadto różnica w liczbie zgłoszeń w stosunku do liczby faktycznych incydentów wynika z faktu, iż część z nich stanowią tzw. „false-positives", czyli przypadki błędnej interpretacji, przez zgłaszającego, legalnego ruchu sieciowego. Należy również podkreślić, iż większość zgłoszeń pochodzi z systemów automatyczne raportujących zdarzenia, które muszą dopiero zostać poddane weryfikacji.

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



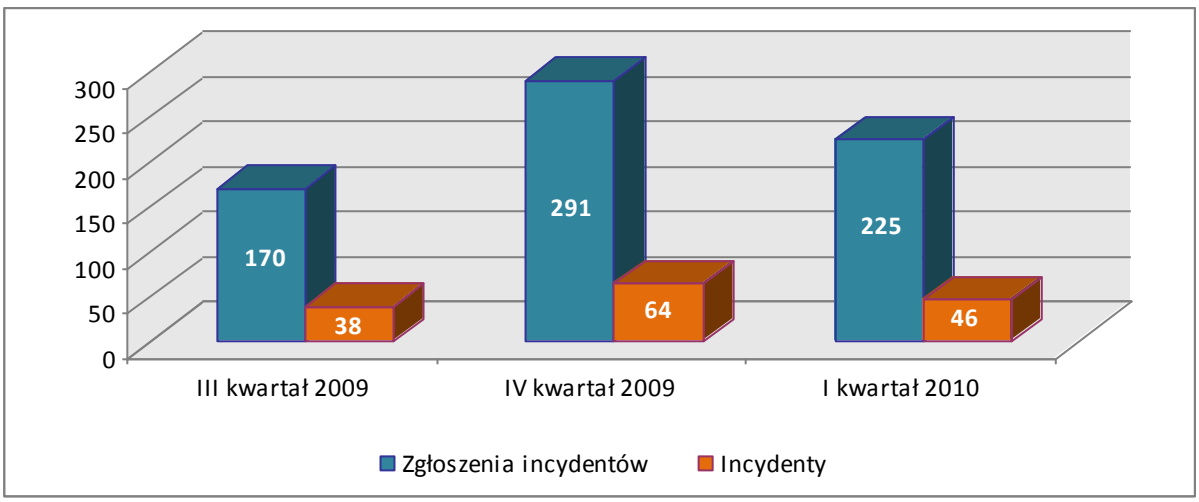
Rysunek 2 - Źródła zgłoszeń incydentów

Rozkład miesięczny incydentów zarejestrowanych i incydentów, które zostały rozwiązane, przedstawia się następująco: w styczniu 2010 zarejestrowano 161 incydentów, z czego rozwiązano 5, w lutym 2010 odnotowano 10 incydentów, z czego 9 zostało rozwiązanych, natomiast w marcu 2010 przyjęto do realizacji 20 incydentów z czego 20 jeszcze w tym samym miesiącu zostało zakończonych. Pozostałe incydenty są w trakcie dalszej analizy.



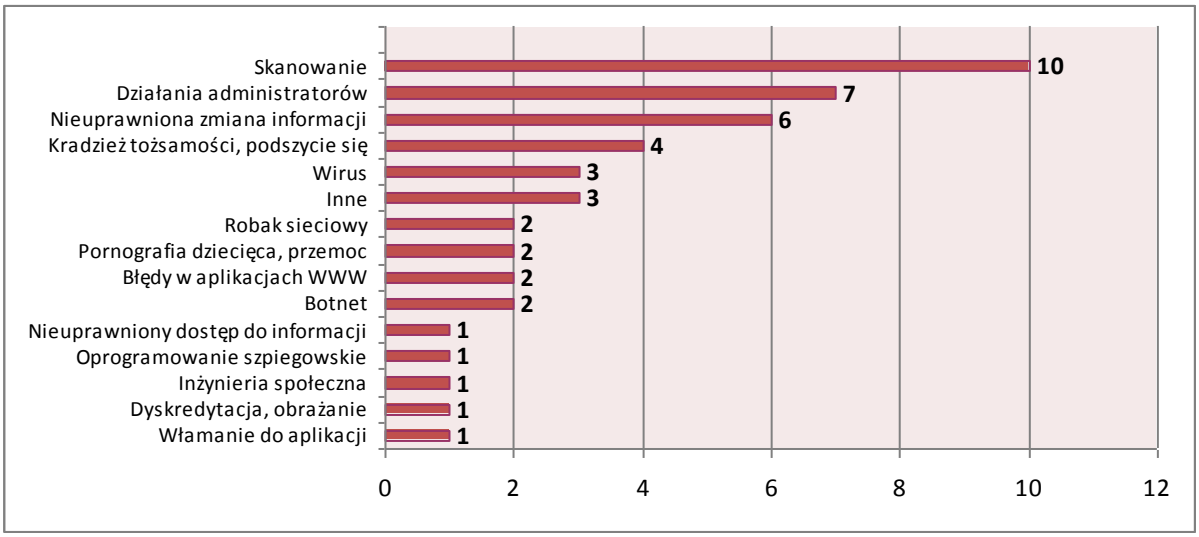
Rysunek 3 - Porównanie liczby incydentów otwartych i zamkniętych w poszczególnych miesiącach pierwszego kwartału

Poniższy wykres obrazuje spadek ilości zgłoszeń oraz incydentów w pierwszym kwartale 2010 r. w stosunku do IV kwartału 2009 r. Jednoczenie zauważono wzrost ilości zgłoszeń i incydentów w stosunku do kwartału III 2009r.



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

Podział zarejestrowanych incydentów na kategorie przedstawia się następująco:



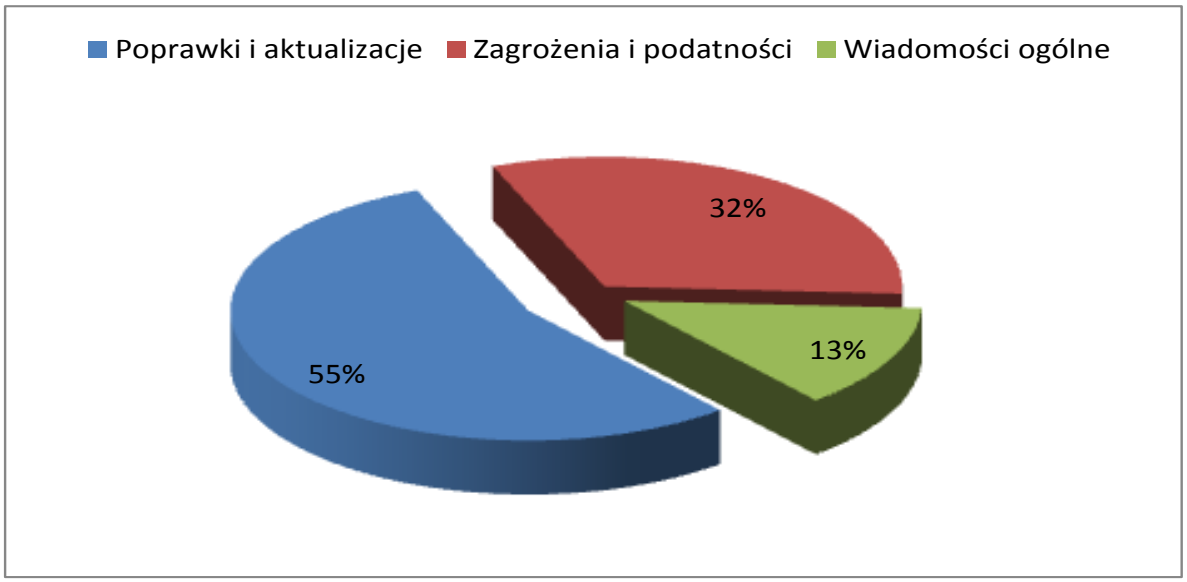
Rysunek 5 - Statystyka incydentów z podziałem na kategorie

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, najczęstszych form ataków sieciowych oraz sposobów ochrony przed zagrożeniami. Dodatkowo na powyższej witrynie umieszczane są informacje o biuletynach bezpieczeństwa udostępniane przez producentów sprzętu i oprogramowania.

W pierwszym kwartale 2010 roku na witrynie www.cert.gov.pl umieszczono:

- 25 publikacji w kategorii „Poprawki i aktualizacje”,
- 15 publikacji w kategorii „Zagrożenie i podatności”,
- 6 publikacji w kategorii „Wiadomości ogólne”.



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

Najbardziej istotne publikacje w pierwszym kwartale 2010 roku dotyczyły podatności w produktach Adobe, Apple, CISCO, Microsoft oraz Oracle.

Adobe

Poinformowano o następujących publikacjach:

1. Biuletynie Bezpieczeństwa Adobe APSB10-02 dotyczącym likwidacji krytycznych błędów w Adobe Reader oraz w Adobe Acrobat. Wykorzystanie podatności mogło spowodować awarię aplikacji i w konsekwencji pozwolenie atakującemu na przejęcie kontroli nad zaatakowanym systemem.
2. Biuletynie Bezpieczeństwa Adobe APSB10-06 dotyczącym likwidacji krytycznych błędów w Adobe Reader, Adobe Acrobat oraz Adobe Flash Player. Biuletyn opisuje dwa błędy, pierwszy umożliwia przemycenie do systemu i uruchomienie szkodliwego kodu z wykorzystaniem specjalnie spreparowanej strony WWW. Drugi umożliwia przeprowadzenie ataku typu cross-site-scripting (XSS).

Apple

Poinformowano o wydaniu:

1. Poprawek bezpieczeństwa Security Update 2010-001, likwidujących podatności, za pomocą których możliwe było przepełnienie bufora i ataku typu Denial of Service.
2. Poprawek bezpieczeństwa Security Update 2010-002, likwidujących luki pozwalające atakującemu na wykonanie dowolnego kodu, uzyskania poufnych informacji, przeprowadzenie ataku typu DoS (Denial-of-Service), ominięcie zabezpieczeń lub pracę z podwyższonymi uprawnieniami.

CISCO

Opublikowano informacje o:

1. Możliwości przepełnienia bufora w produkcie CiscoWorks Internetwork Performance Monitor (IPM). Rezultat udanego wykorzystania powyższej luki pozwalał na wykonanie kodu z uprawnieniami użytkownika „SYSTEM" na podatnych systemach z rodziny Windows. Podatność dotyczyła produktów CiscoWorks IPM w wersji 2.6 i wcześniejszych dla platformy Windows.
2. Podatności w implementacji serwera SSH w CISCO IOS XR. Odpowiednio spreparowany pakiet protokołu SSH w wersji 2 mógł doprowadzić do destabilizacji działania urządzenia poprzez wysycenie dostępnych zasobów systemowych (pamięci). Wykorzystanie luki doprowadzić mogło do udanego ataku DoS. Podatność dotyczyła systemów CISCO IOS XR z włączonym serwerem SSH.
3. Wydaniu poradnika bezpieczeństwa dotyczący wielu podatności w narzędziu wykorzystywanym do wideokonferencji - Unified MeetingPlace.
4. Podatnościach w produkcie firmy Cisco IronPort. Błędy zezwalały na wyjawienie wrażliwych informacji lub skompromitowanie podatnego systemu.
5. Podatnościach urządzeń z serii Adaptive Security Appliance ASA 5500, w których to załatano siedem luk bezpieczeństwa pozwalających między innymi na wykonanie ataku DoS przy pomocy odpowiednio spreparowanego pakietu TCP, SCCP, IKE lub SIP.
6. Usunięciu błędów modułu Cisco Firewall Services Module (FWSM) dla routerów Cisco Catalyst 6500 Series i switchy Cisco 7600 Series. Problem dotyczył mechanizmu przetwarzania wiadomości Skinny Client Control Protocol (SCCP).
7. Załataniu luk w oprogramowaniu zarządzającym Cisco Security Agent, pozwalającym na możliwość zmiany danych dotyczących ustawień konfiguracyjnych trzymanych w bazie bez uwierzytelnienia oraz odczytanie i ściągniecie dowolnych plików trzymanych na serwerze Management Center.

Microsoft

Opublikowano informacje o wydaniu następujących biuletynów:

1. MS10-001 – dotyczącym usterki w Embedded OpenType Font Engine – krytyczny
2. MS10-002 – dotyczącym krytycznej luki w przeglądarce Internet Explorer – krytyczny
3. MS10-003 - dotyczącym podatności w pakiecie Microsoft Office - ważny
4. MS10-004 - dotyczącym podatności w programie PowerPoint z pakietu Microsoft Office – ważny
5. MS10-005 - dotyczącym podatności w Microsoft Paint – umiarkowany
6. MS10-006 - dotyczącym podatności w kliencie SMB – krytyczny
7. MS10-007 - dotyczącym podatności w Windows Shell Handler – krytyczny
8. MS10-008 - dotyczącym podatności w ActiveX – krytyczny
9. MS10-009 - dotyczącym podatności w protokole Windows TCP/IP – krytyczny
10. MS10-010 - dotyczącym podatności w Hyper-V w Windows Server 2008 – ważny
11. MS10-011 - dotyczącym podatności w Windows Client/Server Run-time Subsystem (CSRSS) – ważny
12. MS10-012 - dotyczącym podatności w SMB Server – ważny
13. MS10-013 - dotyczącym podatności w Microsoft DirectShow – krytyczny
14. MS10-014 - dotyczącym podatności w Kerberosie – ważny
15. MS10-015 - dotyczącym podatności w Windows Kernel – ważny
16. MS10-016 – dotyczącym podatności w Windows Movie Maker i Microsoft Producer 2003 – ważny
17. MS10-017 - dotyczącym podatności w Microsoft Office Excel – ważny
18. MS10-018 - dotyczącym podatności w programie Internet Explorer - krytyczny

Oracle

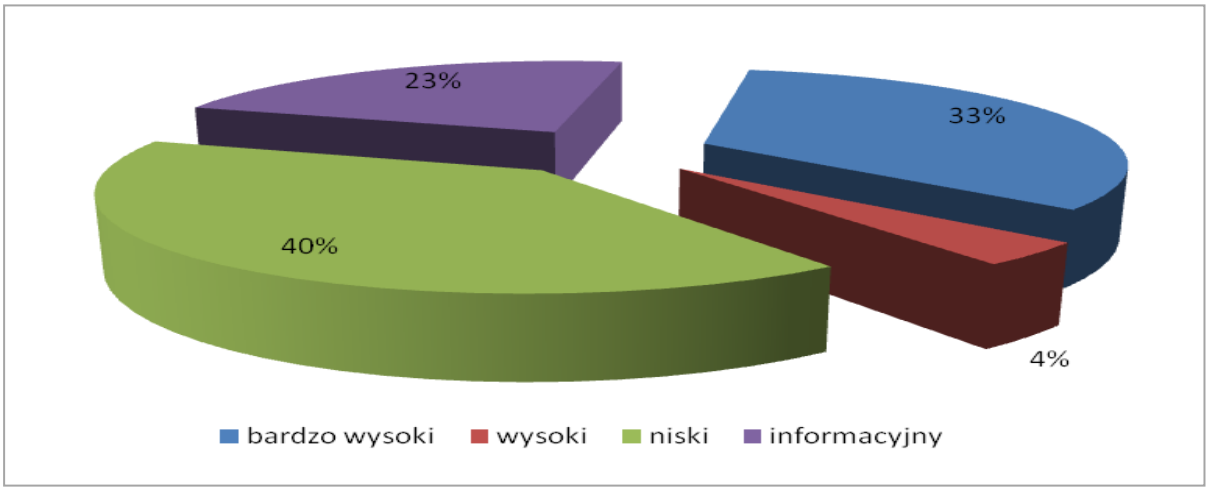
Opublikowano informacje o wydaniu:

1. Zbioru poprawek Oracle Critical Patch Update Advisory - January 2010, który likwidował błędy w produktach Oracle.
2. Zbioru poprawek Oracle Java SE and Java for Business Critical Patch Update Advisory - March 2010, który łatał 27 podatności w Java SE i Java for Business. Aktualizacja została sklasyfikowana jako „krytyczna”.

5. Testy bezpieczeństwa witryn WWW instytucji państwowych

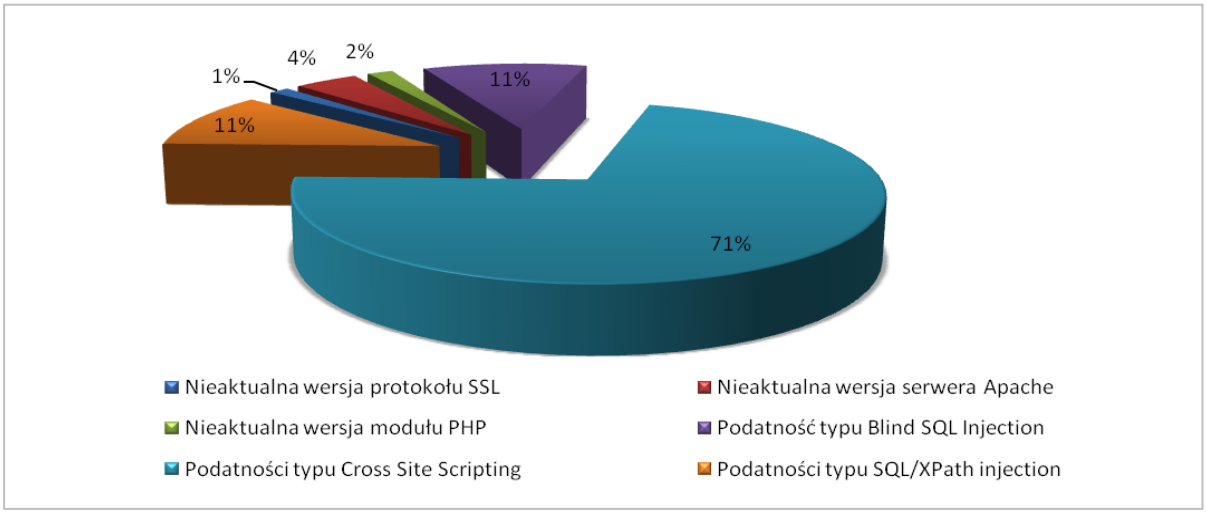
Zespół CERT.GOV.PL kontynuował testy bezpieczeństwa witryn WWW należących do instytucji państwowych.

W I kwartale 2010 roku przebadano 29 witryn należących do 23 instytucji państwowych. Stwierdzono ogółem 369 błędów w tym: 124 błędy o bardzo wysokim poziomie zagrożenia, 14 błędów o wysokim poziomie zagrożenia, 147 błędów o niskim poziomie zagrożenia i 84 błędy 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

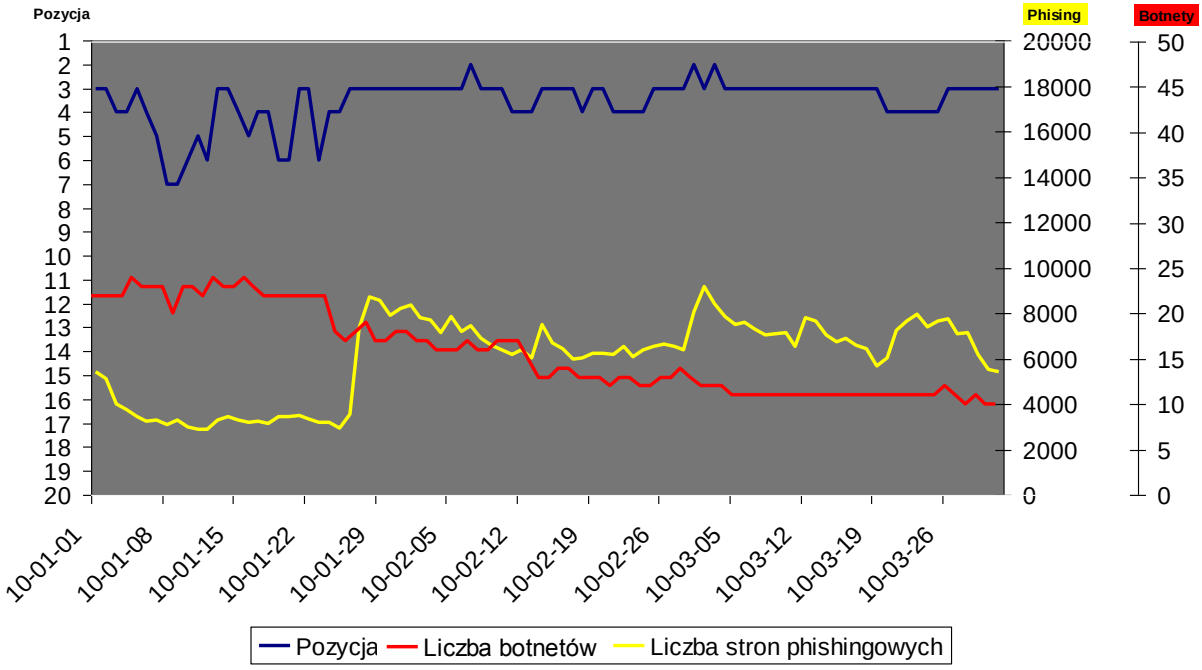
Należy zwrócić uwagę, iż podatności krytyczne najczęściej znajdują się w warstwie usługowej systemu (np. serwerze http czy frontendzie do bazy danych), a nie w warstwie systemu operacyjnego. Jak widać, obecnie największe zagrożenie dla bezpieczeństwa stanowią błędy w aplikacjach, do których ma dostęp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

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.

Podobnie jak w poprzednim okresie, również w I kwartale 2010 roku pozycja Polski, pod względem zagrożenia dla bezpieczeństwa Internetu, nadal jest bardzo wysoka – utrzymuje się w okolicach 3-go miejsca. Należy odnotować ciągły spadek ilości botnetów w Polsce – w okresie 3 miesięcy ilość serwerów C&C[7] spadła o połowę. Z niepokojem należy przyjąć wyraźny wzrost liczby stron służących do wyłudzania danych. Wyraźny skok widoczny w końcu stycznia spowodowany był najprawdopodobniej opublikowaniem serii exploitów[8] na platformę Joomla.



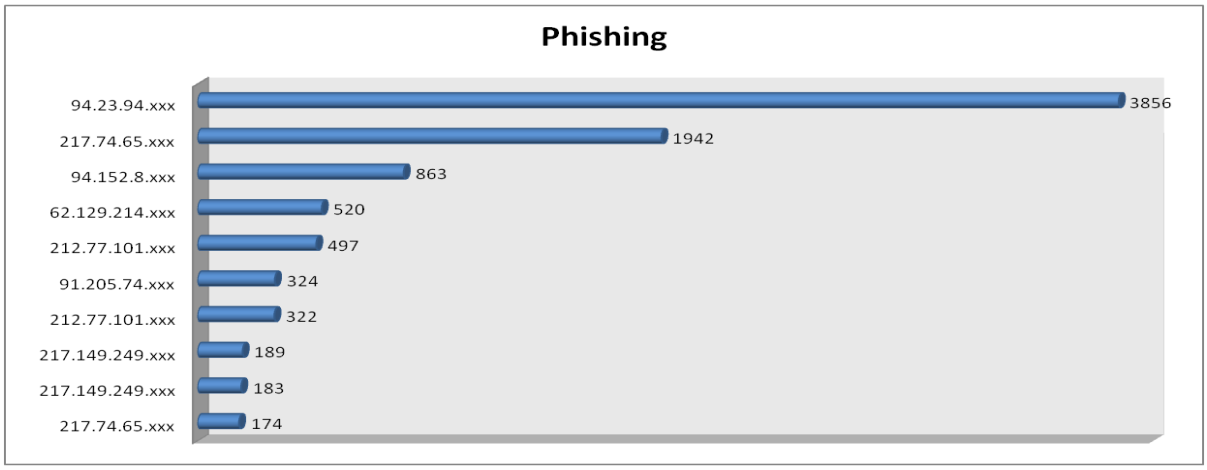
Rysunek 9 - Pozycja Polski w rankingu ATLAS i jej związek z phishingiem

Na powyższym wykresie widać wyraźną korelację pomiędzy zajmowaną pozycją a liczbą stron phishingowych i botnetów. Pomimo malejącej ilości systemów C&C, Polska nadal jest traktowana jako wyraźne zagrożenie dla bezpieczeństwa Internetu

[6] http://atlas.arbor.net
[7] Serwer zarządzający siecią komputerów wchodzących w skład botnetu.
[8] Exploit – program, wykorzystujący błędy w oprogramowaniu w celu przejęcia kontroli nad działającym procesem systemowym i wykonania odpowiednio spreparowanej sekwencji bajtów.

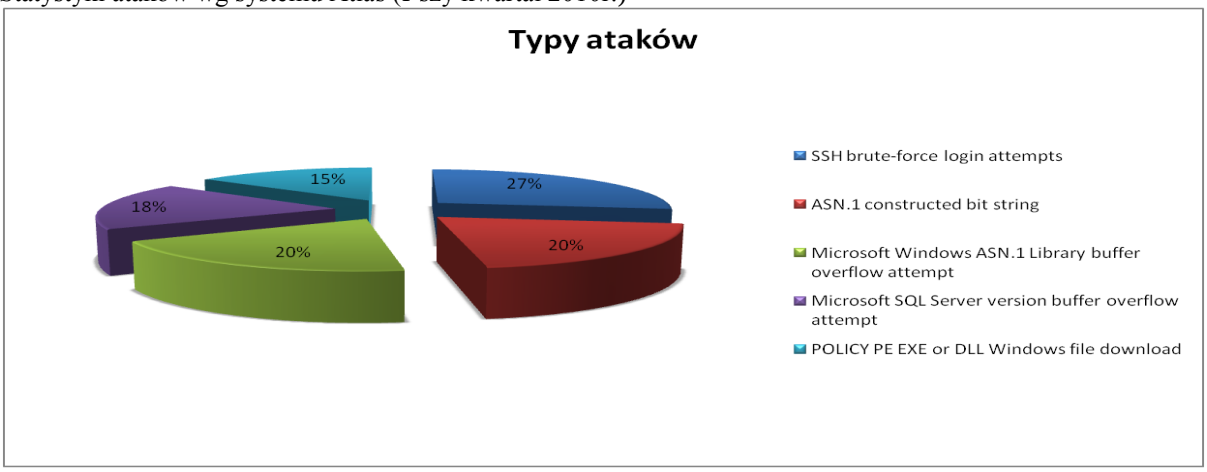
Korelacja publikacji exploitów ze skokiem ilości hostowanych na polskich serwerach stron phishingowych potwierdza opinię Zespołu CERT.GOV.PL, iż duża liczba stron phishingowych w polskiej przestrzeni adresowej wynika jedynie z dużej liczby słabo zabezpieczonych witryn WWW, na których po przełamaniu zabezpieczeń włamywacze umieszczają nieautoryzowane treści a nie z działalności w Polsce firm oferujących tzw. kuloodporny hosting[9].

W większości przypadków strony służące do wyłudzania informacji znajdują się 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.



Rysunek 10 - Statystyki phishingu wg systemu Atlas (najwyższe odnotowane udziały, najbardziej aktywnych hostów w I-szym kwartale 2010r.)

Statystyki ataków wg systemu Atlas (I-szy kwartał 2010r.)

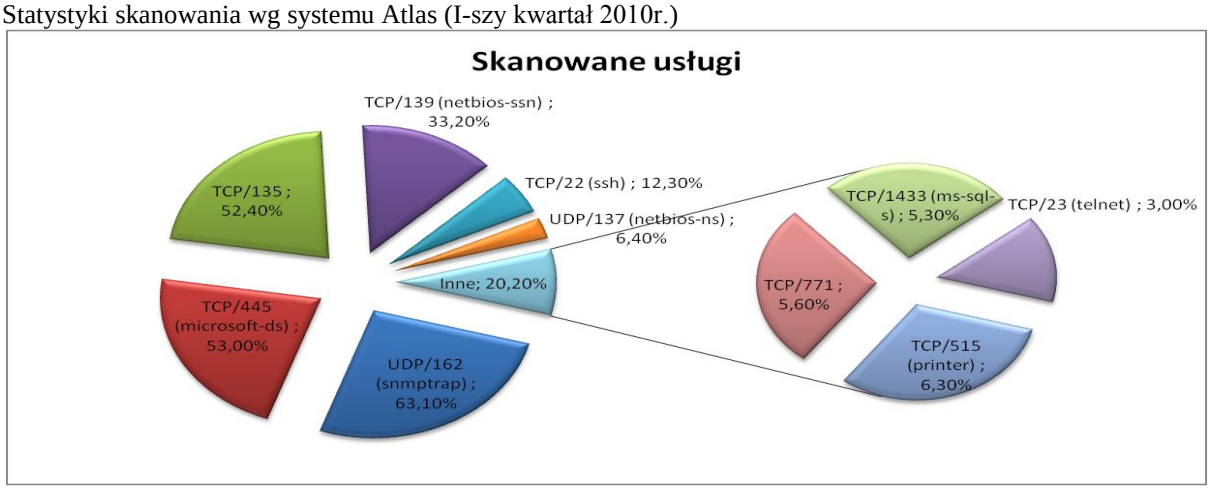


Rysunek 11 - Pięć najczęściej występujących typów ataków wg systemu ATLAS – w I-szym kwartale 2010r. (udział procentowy liczony tylko dla tych usług)

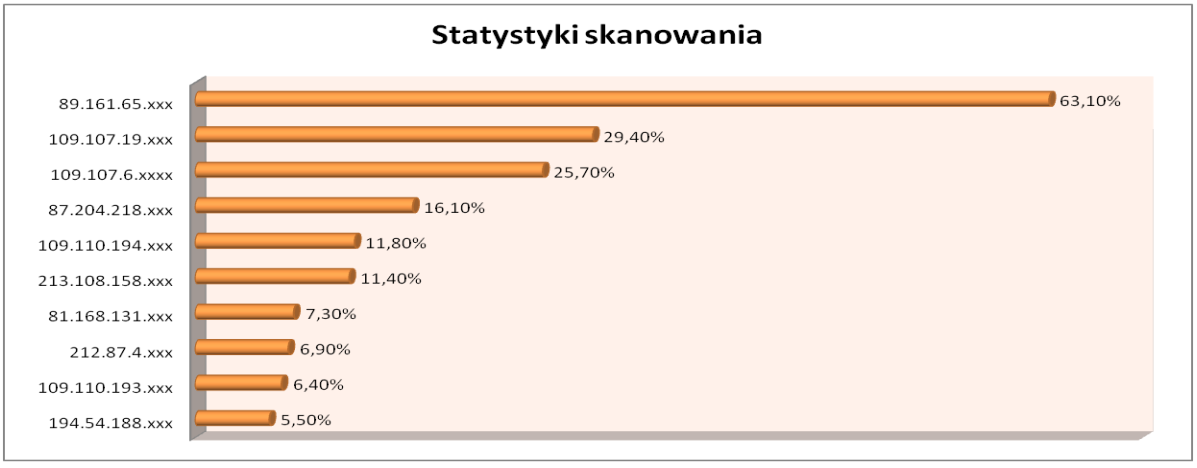
[9] ang. *bulletproof hosting* – usługa hostingowi polegająca na udostępnieniu przestrzeni dyskowej i łącza bez ograniczeń co do publikowanych przez usługobiorcę treści. Bardzo często tego typu hosting wykorzystywany jest przy phishingu, działaniach spamerskich lub publikacji pornografii. W przypadku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

Rysunek 12 - Najbardziej aktywne hosty w Polsce wg systemu ATLAS – w I-szym kwartale 2010r. (najwyższe odnotowane udziały procentowe w stosunku do pozostałych)

Statystyki skanowania wg systemu Atlas (I-szy kwartał 2010r.)



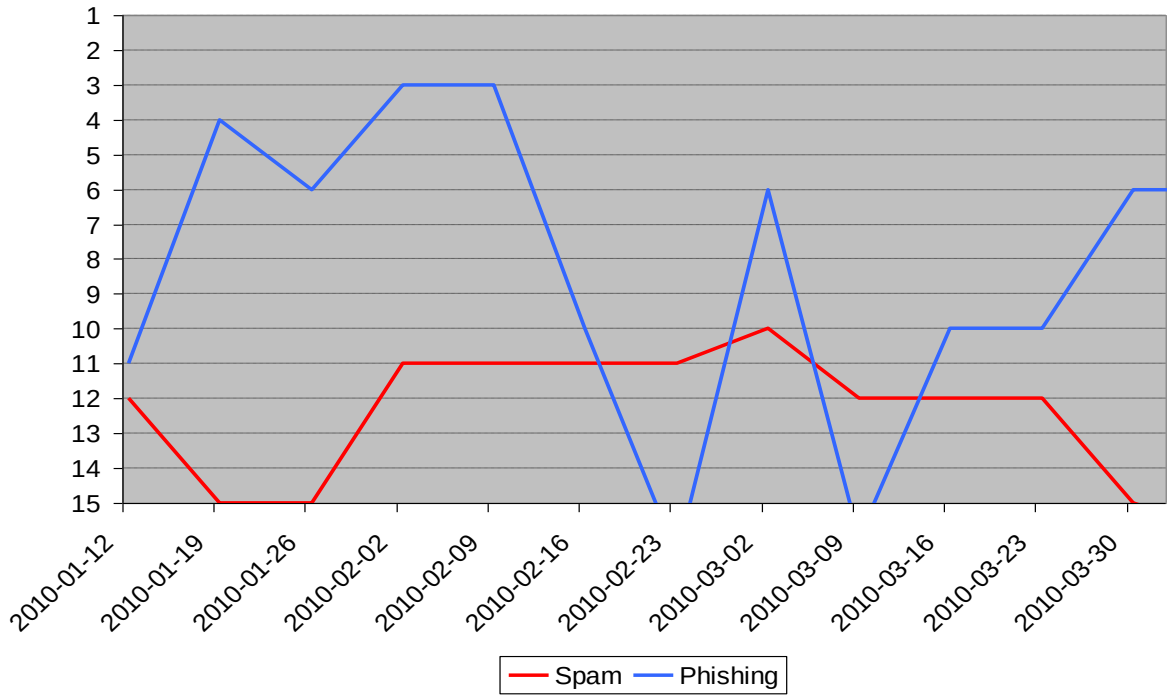
Rysunek 13 - Najczęściej skanowane porty/usługi wg systemu ATLAS – w I-szym kwartale 2010r.



Rysunek 14 - Najbardziej aktywne hosty w Polsce wg systemu ATLAS – w I-szym 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[10]



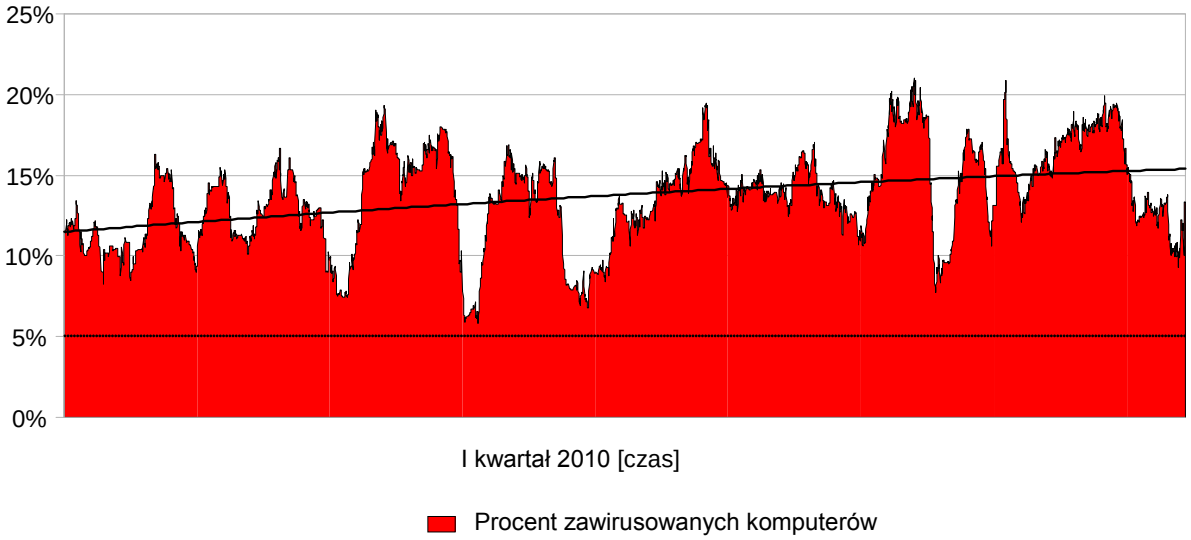
Rysunek 15 – Ranking Polski pod względem wysyłanych e-maili typu „spam" oraz phishingowych (pozycje poniżej miejsca 15-go nie są raportowane)

Należy zauważyć, iż wysoka pozycja Polski pod względem ilości wysyłanych z jej obszaru przesyłek phishingowych potwierdza wyniki z systemu ATLAS, czyli wskazanie na stwarzanie wysoki zagrożenia dla Internetu. Biorąc pod uwagę pozycję pod względem ogólnej wysyłki niezamówionych przesyłek poczty elektronicznej Polska znajduje się praktycznie poza pierwszą 10-tką). Analiza ta będzie prowadzona w dalszych okresach.

W uzupełnieniu do analizy niezamówionych przesyłek e-mailowych, rozpoczęto szacowanie[11] poziomu zainfekowanych komputerów znajdujących się w obszarze polskiej cyberprzestrzeni. Komputer zainfekowanyrozumiany jest jako pojedyncza maszyna na której znajduje się przynajmniej jeden program należący do jednego z poniższych typów:

- Trojan[12];
- Worm[13];
- Wirus[14];
- Backdoor[15];
- Adware[16].

[10] Informacje zbierane na podstawie tygodniowych raportów dostarczanych przez firmę M86 Security (http://www.m86security.com)
[11] Na podstawie informacji publikowanych przez firmę Panda Security (http://www.pandasecurity.com)
[12] Oprogramowanie złośliwe, udające swoim działaniem program nieszkodliwy
[13] Samoreplikujące się oprogramowanie niepotrzebujące do swego działania innego pliku
[14] Samoreplikujące się oprogramowanie propagujące się poprzez dystrybucję pliku do którego jest przyłączone
[15] Umyślnie stworzona luka w zabezpieczeniach systemu pozwalająca na zdalny dostęp osoby niepowołanej



Rysunek 10 – Procentowy poziom zawirusowanych komputerów w okresie I-szego kwartału 2010r.

Zauważalny jest trend rosnący w średniej ilości zarażonych komputerów. Ze względów technicznych, statystyka obejmuje jedynie komputery pracujące pod kontrolą systemu operacyjnego Windows. Jednocześnie, nawet w najlepszym okresie, poziom ilości zawirusowanych komputerów nie spadł poniżej 5%. Należy pamiętać, że statystyka odnosi się wyłącznie do komputerów włączonych, a dane zbierane są co 15 minut.

Na podstawie informacji zebranych z niezależnych od siebie źródeł, należy przyjąć, iż pod względem stanowienia potencjalnego zagrożenia dla użytkowników Internetu, Polska zajmuje wysokie miejsca. Zwrócić należy jednak uwagę na fakt, iż są to zagrożenia typu pasywnego (strony phisingowe, przesyłki e-mailowe). Pod względem zagrożeń aktywnych (ataki, rozsyłanie wirusów, skanowania, próby wywołania odmowy dostępu /DDoS/) Polska praktycznie znajduje się poza przedziałem klasyfikowanym.

[16] Oprogramowanie, które bez zgody odbiorcy, w sposób utrudniający użytkowanie komputera, wyświetla reklamy i/lub posiadające moduły szpiegujące użytkownika.

7. Inne działania CERT.GOV.PL

W trakcie XIV spotkania ABUSE-FORUM (grupa zrzeszająca przedstawicieli zespołów reagujących na incydenty bezpieczeństwa komputerowego, zespołów bezpieczeństwa operatorów telekomunikacyjnych oraz dostawców treści internetowych), którego członkiem jest między innymi Rządowy Zespół Reagowania na Incydenty Komputerowe CERT.GOV.PL, wypracowano wspólne stanowisko dotyczące dalszego wykorzystywania przeglądarki Internet Explorer 6. W zgodnej opinii uczestników, Internet Explorer w wersji 6.x jest niebezpieczną aplikacją i nie powinien być narzędziem z którego korzysta się przy dostępie do treści internetowych. Korzystanie z tej przeglądarki związane jest z dużym ryzykiem zainfekowania komputera złośliwym oprogramowaniem. Rządowy Zespół Reagowania na Incydenty Komputerowe CERT.GOV.PL, jako członek ABUSE-FORUM rekomenduje zaprzestanie używania tej przeglądarki i jako alternatywne rozwiązanie proponuje zainstalowanie nowszej wersji przeglądarki firmy Microsoft lub przeglądarek innych producentów, np.:

- Microsoft IE 7.x oraz 8.x
- Firefox 3.x
- Google Chrome 4.x
- Opera 10

Pełna treść stanowiska ABUSE-FORUM znajduje się na stronie www.cert.gov.pl.