# Raport kwartalny CERT.GOV.PL
# lipiec – wrzesień 2010


1. Informacje dotyczące zespołu CERT.GOV.PL ..... 2
2. Statystyki systemu ARAKIS-GOV ..... 3
3. Statystyki incydentów ..... 5
4. Istotne podatności, zagrożenia i biuletyny zabezpieczeń ..... 8
5. Testy bezpieczeństwa witryn WWW instytucji państwowych ..... 11
6. Informacje z systemów zewnętrznych ..... 12
7. Inne działania CERT.GOV.PL ..... 15

## 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:

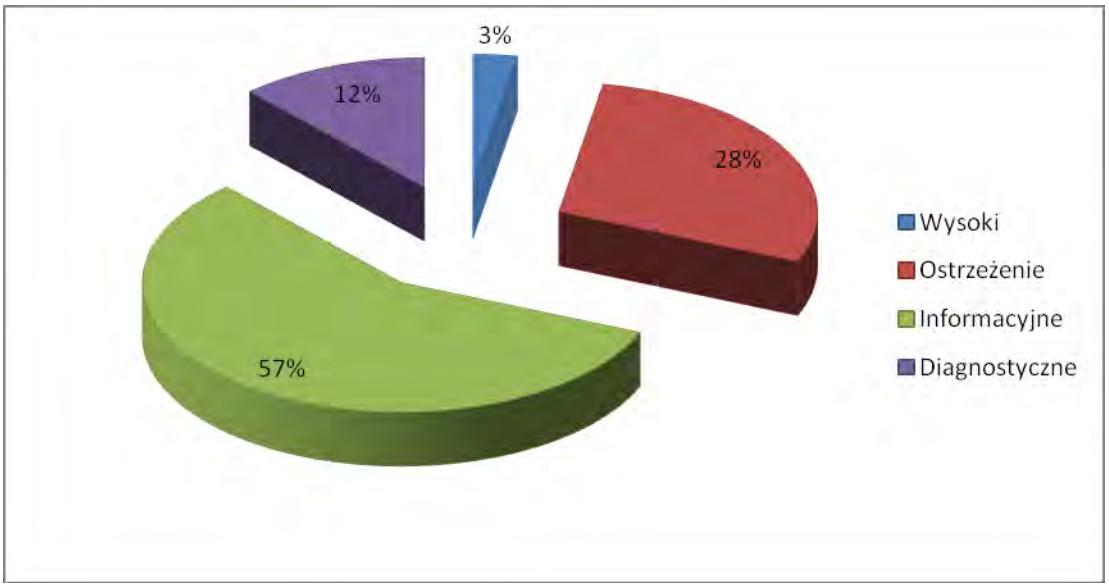
- E-mail: cert@cert.gov.pl
- Telefon: +48 22 58 58 844
- Fax: +48 22 58 56 099

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

## *2.* Statystyki systemu ARAKIS-GOV[1]

Trzeci kwartał 2010 roku to zdecydowana większość alarmów informacyjnych. Stanowiły one 57 procent wszystkich zarejestrowanych przez system ARAKIS-GOV. Alarmy o priorytecie średnim stanowiły 28%, natomiast alarmy diagnostyczne 12%. System zgłosił najmniej alarmów o priorytecie wysokim – 55, co stanowiło 3% wszystkich alarmów.

Jak można zauważyć, liczba alarmów jest mniejsza niż w poprzednich kwartałach 2010 roku.




**Rysunek 1 – Procentowy rozkład ważności alarmów.**

Wśród alarmów o priorytecie wysokim zaobserwowano 55 alarmów typu INFHOST_HN[2], 1 alarm typu VIRUS_FOUND[3], a także 2 alarmy typu NWORM[4]. Nie zarejestrowano żadnego alarmu typu INFHOST_FW[5].

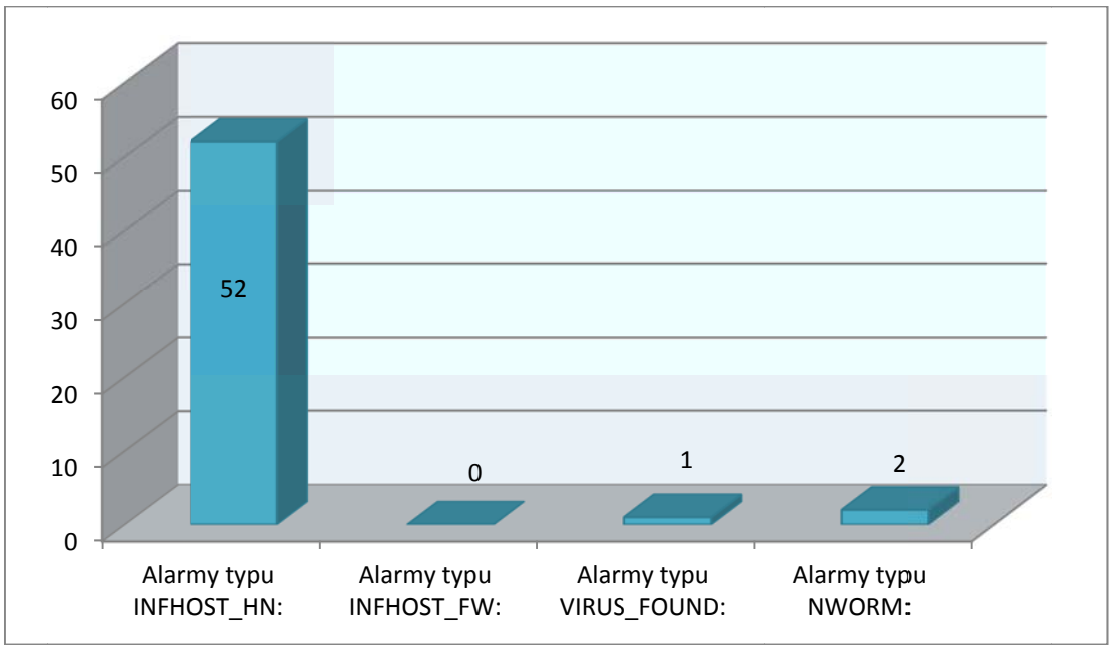
[1] ARAKIS-GOV jest pasywnym systemem wczesnego ostrzegania o zagrożeniach w sieci Internet. W chwili obecnej został wdrożony w 70 instytucjach państwowych.

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

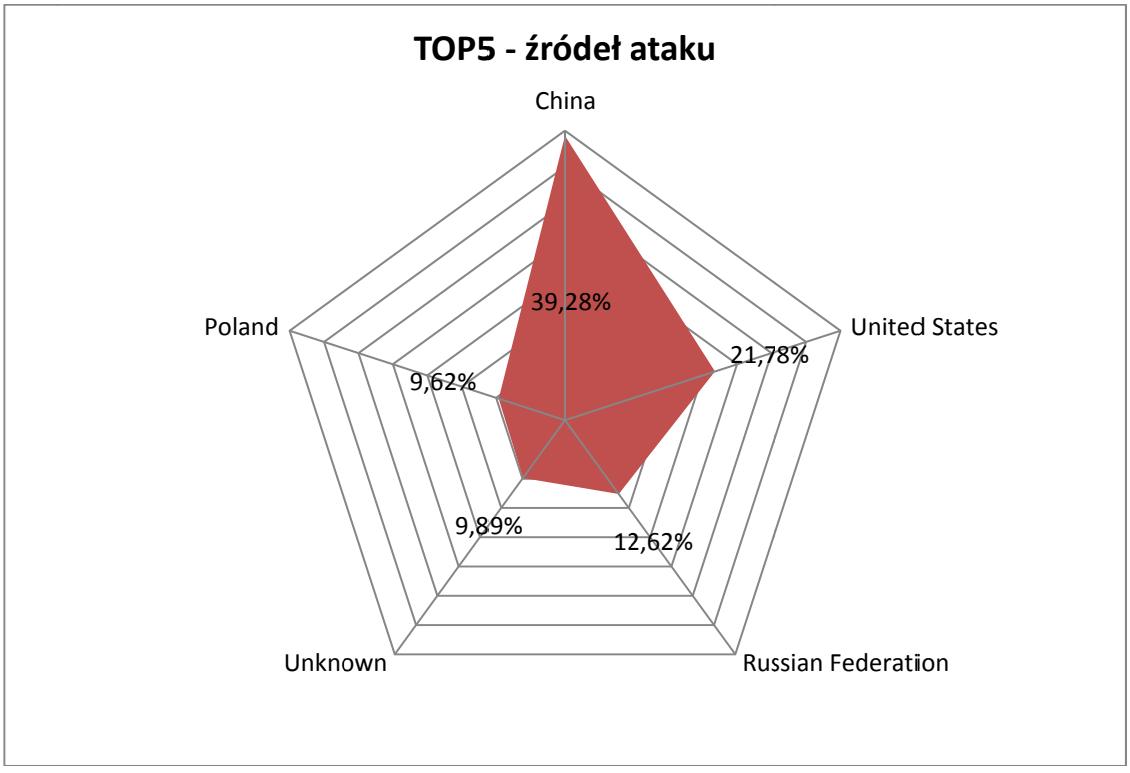
[5] Alarm INFHOST_FW oznacza potencjalne wykrycie zainfekowanego hosta w sieci wewnętrznej instytucji chronionej systemem ARAKIS-GOV. Alarm ten generowany jest na podstawie analizy logów systemów zaporowych.




**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, oraz Federacji Rosyjskiej. Na uwagę zasługuje fakt pojawienia się w statystyce Polski z przeszło 9 procentowym wynikiem.

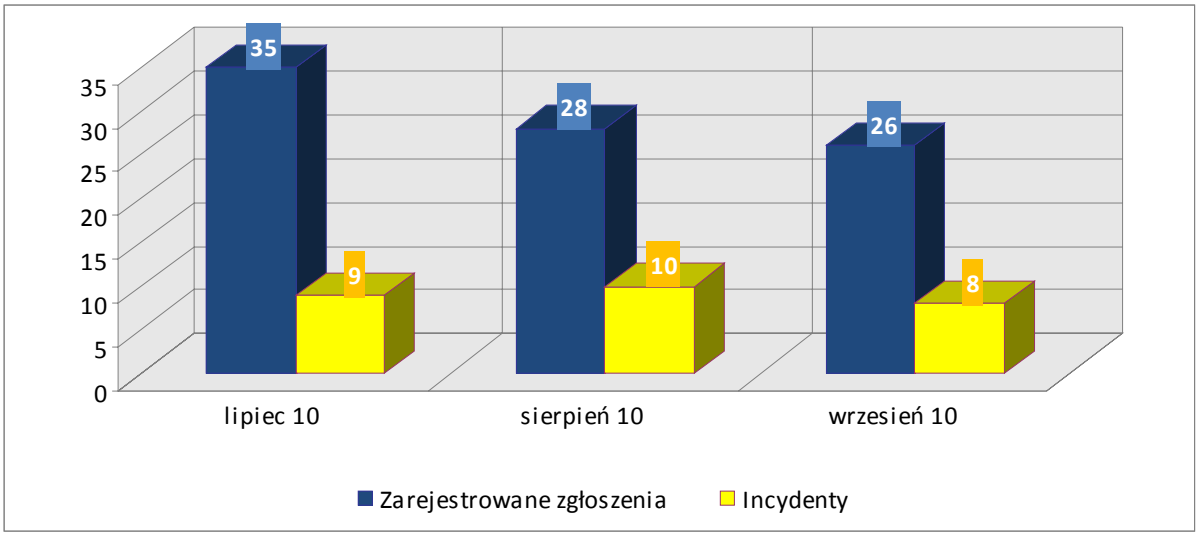
Jednakże mając na uwadze specyfikę protokołu TCP/IP, nie można bezpośrednio łączyć zarejestrowanego źródła pochodzenia pakietów z faktyczną lokalizacją wykonawcy ataku. Wynika to z faktu, iż w celu ukrycia swej tożsamości i fizycznej lokalizacji atakujący wykorzystują serwery pośredniczące (proxy) lub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




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

## *3.* Statystyki incydentów

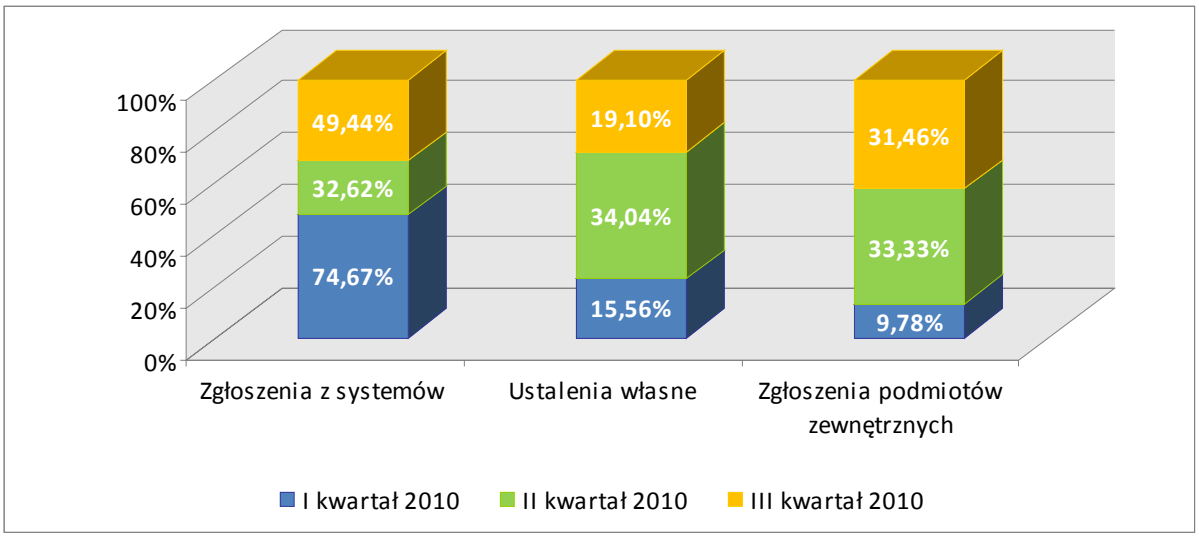
W trzecim kwartale 2010 roku do zespołu CERT.GOV.PL wpłynęło 89 zgłoszeń, przy czym tylko 27 z nich zostały zakwalifikowane jako faktyczne incydenty.




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

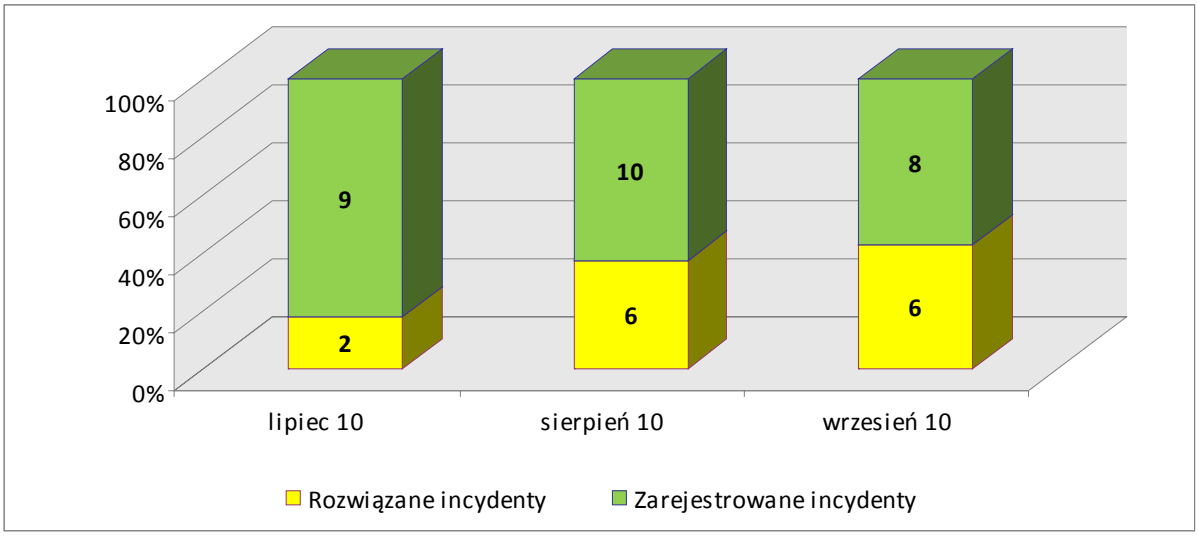
W stosunku do poprzedniego kwartału zmalała ilość faktycznych zgłoszeń, przy czym dotyczy to również zgłoszeń typu tzw. „false-positive". Okres spadkowy pokrywa się z okresem urlopowym w instytucjach państwowych.

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



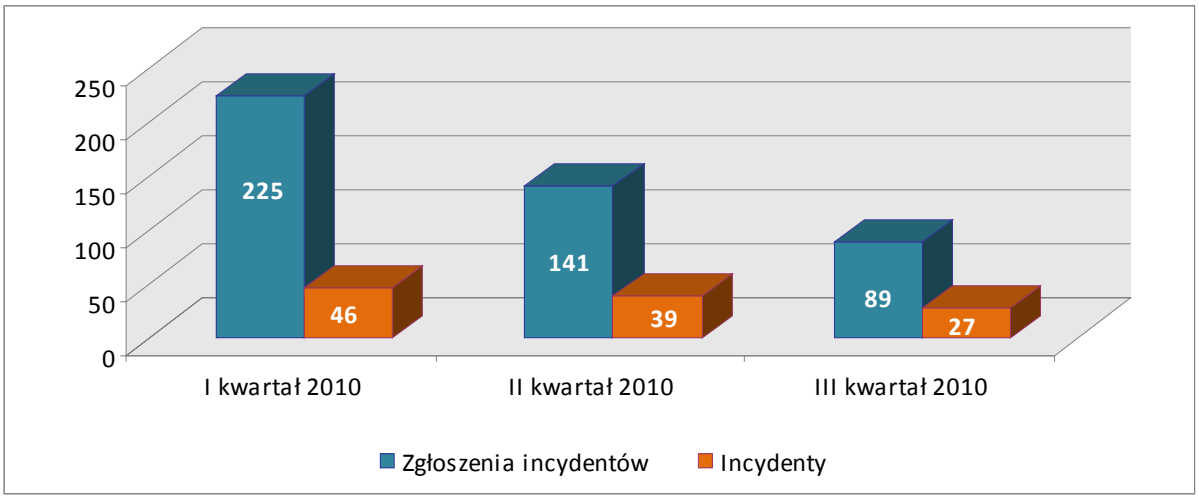

**Rysunek 2 - Źródła zgłoszeń incydentów**

Rozkład miesięczny incydentów zarejestrowanych i incydentów, które zostały rozwiązane, przedstawia się następująco: w lipcu 2010 zarejestrowano 9 incydentów, z czego rozwiązano 2, w sierpniu 2010 odnotowano 10 incydentów, z czego 6 zostało rozwiązanych, natomiast we wrześniu 2010 przyjęto do realizacji 8 incydentów z czego 6 jeszcze w tym samym miesiącu zostało zakończonych. Pozostałe incydenty są w trakcie dalszej analizy.



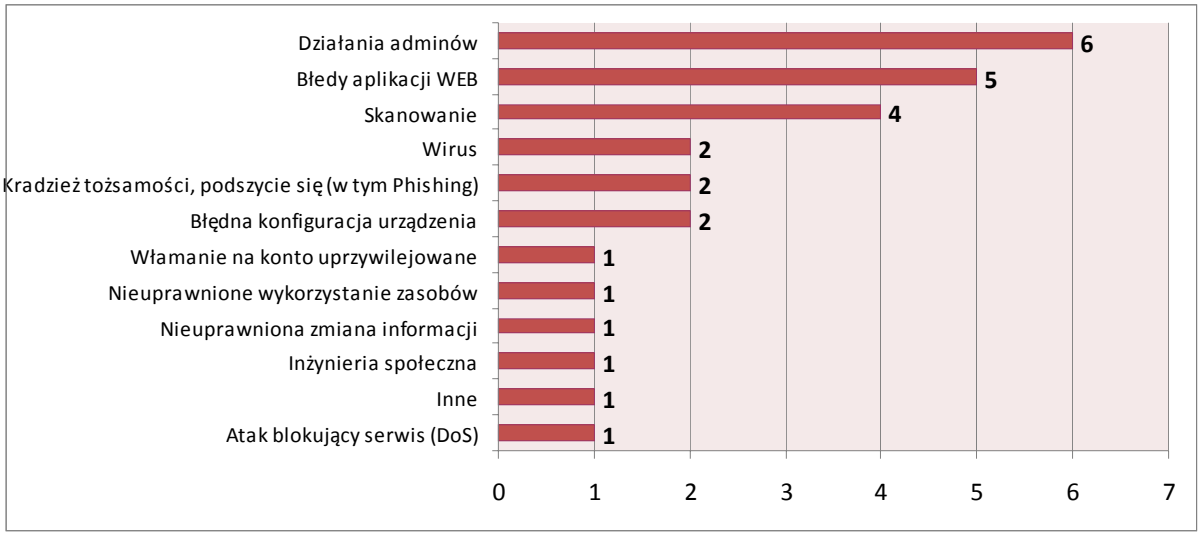

**Rysunek 3 - Porównanie liczby incydentów otwartych i zamkniętych w poszczególnych miesiącach trzeciego kwartału**

Poniższy wykres obrazuje aktualnie utrzymującą się tendencję spadkową ilości zgłoszeń oraz faktycznych incydentów od I kwartału 2010 roku do III 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**

Istotne ataki odnotowane przez Rządowy Zespół Reagowania na Incydenty Komputerowe CERT.GOV.PL w III kwartale 2010 r.:

- Do zespołu CERT.GOV.PL wpłynęło zawiadomienie o kradzieży impulsów telefonicznych w jednej z jednostek administracji terenowej. Kradzież impulsów odbyła się poprzez przełamanie zabezpieczeń (słabe hasło) konta uprzywilejowanego w systemie telefonii IP, pozwalającego na wykonywanie połączeń wychodzących. W wyniku powyższego, instytucja poniosła straty na kwotę około 50000 PLN. Wykonane połączenia kierowane były do krajów afrykańskich i ich łączny czas przekroczył 8.5 doby.
- Na przełomie sierpnia 2010 r., miał miejsce atak typu DoS (Denial-of-Service) skierowany przeciwko jednej z instytucji administracji państwowej. Atak pochodził z adresu IP, którego dostawca zlokalizowany jest w Niemczech i miał na celu zablokowanie serwera WWW przedmiotowej instytucji. Systemy detekcji intruzów zidentyfikowały powyższy atak jako „Teardrop attack".
- Kolejny incydent dotyczył włamania na stronę WWW instytucji państwowej. Atakujący uzyskał dostęp do loginów i haseł użytkowników systemu zarządzania treścią (CMS). Dane te zostały uzyskane przy wykorzystaniu błędu w aplikacji WWW (SQL-Injection).
- We wrześniu 2010 r. uzyskano informację o stronie phishingowej dotyczącej czołowego wystawcy kart kredytowych we Włoszech CartaSi, zlokalizowanej w przestrzeni adresowej instytucji administracji państwowej RP. Analiza przypadku wykazała, iż w strukturze katalogów strony znajdowało się oprogramowanie tzw. „php shell", przy pomocy którego dokonano umieszczenia strony phishingowej na serwerze WWW. Powyższy skrypt został umieszczony prawdopodobnie w wyniku przechwycenia hasła użytkownika do serwera FTP na którym utrzymywana była strona podmiotu.
- Kolejnym przykładem ataku na serwer WWW instytucji administracji państwowej była podmiana strony głównej departamentu informatyki w tej instytucji. Podmiany dokonano w wyniku błędu w aplikacji CMS pozwalającego na zdalne zresetowanie hasła użytkownika „admin", posiadającego uprawnienia administracyjne. Do włamania wykorzystano błąd w nieaktualnej wersji aplikacji systemu zarządzania treścią (CMS).

## 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 trzecim kwartale 2010 roku na witrynie http://www.cert.gov.pl dodano:

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


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

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

- **Comiesięcznych biuletynów bezpieczeństwa firmy Microsoft**

Lipcowy Biuletyn Bezpieczeństwa:

Lipcowy Biuletyn Bezpieczeństwa informował o wykryciu oraz usunięciu czterech poważnych błędów. Trzy otrzymały status „krytyczny”, a czwarty zakwalifikowano jako „ważny”. Luki o statusie „krytyczny” pozwalały na zdalne wykonanie kodu.

1. MS10-042 – biuletyn dotyczący błędów w zabezpieczeniach funkcji Centrum pomocy i obsługi technicznej systemu Windows - krytyczny
2. MS10-043 – biuletyn dotyczący błędów w zabezpieczeniach kanonicznego sterownika ekranu (cdd.dll) – krytyczny
3. MS10-044 – biuletyn dotyczący błędów w zabezpieczeniach formantów ActiveX programu Microsoft Office Access - krytyczny
4. MS10-045 – biuletyn dotyczący błędów w zabezpieczeniach programu Microsoft Office Outlook - ważny

Sierpniowy Biuletyn Bezpieczeństwa:

Sierpniowy Biuletyn Bezpieczeństwa informował o wykryciu oraz usunięciu piętnastu błędów. Dziewięć otrzymało status „krytyczny", a sześć zakwalifikowano jako „ważne".

1. MS10-046 - biuletyn dotyczący podatności w Windows Shell – krytyczny
2. MS10-047 - biuletyn dotyczy podatności jądra systemu Windows – ważny
3. MS10-048 - biuletyn dotyczy podatności w trybie jądra sterowników - ważny
4. MS10-049 - biuletyn dotyczy podatności w Secure Channel (SChannel) – krytyczny
5. MS10-050 - biuletyn dotyczy podatności programu Windows Movie Maker – ważny
6. MS10-051 - biuletyn dotyczy podatności w Microsoft XML Core Services – krytyczny
7. MS10-052 - biuletyn dotyczy podatności kodeka audio MPEG Layer-3 - krytyczny
8. MS10-053 - biuletyn dotyczy podatności programu Internet Explorer - krytyczny
9. MS10-054 - biuletyn dotyczy podatności w zabezpieczeniach protokołu SMB Server - krytyczny
10. MS10-055 - biuletyn dotyczy podatności w Cinepak Codec - krytyczny
11. MS10-056 - biuletyn dotyczy podatności pakietu Microsoft Office – krytyczny
12. MS10-057 - biuletyn dotyczy podatności pakietu Microsoft Office – ważny
13. MS10-058 - biuletyn dotyczy podatności protokołu sieciowego TCP/IP – ważny
14. MS10-059 - biuletyn dotyczy błędów w zabezpieczeniach funkcji śledzenia usługi – ważny
15. MS10-060 - biuletyn dotyczy luk w zabezpieczeniach programów Microsoft .NET Framework oraz Microsoft Silverlight - krytyczny

Wrześniowy Biuletyn Bezpieczeństwa:

Wrześniowy biuletyn bezpieczeństwa informował o wykryciu oraz usunięciu dziewięciu biuletynów bezpieczeństwa. Cztery otrzymały status „krytyczny", pozostałe pięć zostało sklasyfikowanych jako „ważne".

1. MS10-061 - biuletyn dotyczy podatności w usłudze Print Spooler – krytyczny
2. MS10-062 - biuletyn dotyczy podatności w kodeku MPEG-4 – krytyczny
3. MS10-063 - biuletyn dotyczy podatności w Unicode Scripts Processor – krytyczny
4. MS10-064 - biuletyn dotyczy podatności w aplikacji Microsoft Outlook – krytyczny
5. MS10-065 - biuletyn dotyczy trzech podatności w Internet Information Services (IIS) – ważny
6. MS10-066 - biuletyn dotyczy podatności w usłudze RPC – ważny
7. MS10-067 - biuletyn dotyczy podatności w aplikacji WordPad – ważny
8. MS10-068 - biuletyn dotyczy podatności w Active Directory, Active Directory Application Mode (ADAM) oraz Active Directory Lightweight Directory Service (AD LDS) – ważny
9. MS10-069 – biuletyn dotyczy podatności w Windows Client/Server Runtime Subsystem – ważny

- **Biuletynów bezpieczeństwa dla produktów Adobe**

Rządowy Zespół Reagowania na Incydenty Komputerowe informował o:

1. Wykryciu szeregu podatności w oprogramowaniu Shockwave Player, mogących doprowadzić do wykonania dowolnego kodu przez atakującego przy wykorzystaniu tzw. „memory corruption" lub przeprowadzenie ataku DoS (denial of service).

2. Opublikowaniu aktualizacji dla programu Acrobat Reader oraz dla Adobe Acrobat (APSB10-17). Wykryte w niej podatności mogą pozwolić atakującemu na przeprowadzenie ataku typu DoS (Denial of Service) oraz na zdalne wykonanie kodu.
3. Biuletynie bezpieczeństwa Adobe APSB10-16 oraz APSB10-19 dotyczącym likwidacji wykrytych błędów w programach Adobe Flash Player, Adobe AIR oraz Adobe Flash Media Server. Wykryte błędy mogą spowodować awarię aplikacji, co w konsekwencji może umożliwić osobie atakującej 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 Industrial Ethernet 3000 Switch (IE 3000) działających w oparciu o system operacyjny Cisco IOS ver. 12.2(52)SE lub 12.2(52)SE1 – Wykorzystanie wykrytej podatności daje możliwość pozyskania odpowiednich danych generowanych w trakcie połączenia SNMP pomiędzy zarządcą a agentem, co w konsekwencji prowadzi do przejęcia kontroli nad zaatakowanym urządzeniem.
2. Cisco Firewall Services Module – wykorzystanie tych luk stwarza możliwość przeprowadzenia ataku typu DoS (Denial of Service).
3. Cisco IOS XR Software Border Gateway Protocol - wykorzystanie tej luki może prowadzić do ciągłego resetowania sesji BGP, co może spowodować odmowę dostępu (denial-of-service) dla atakowanych sieci.

- **Critical Patch Update dla produktów Oracle**

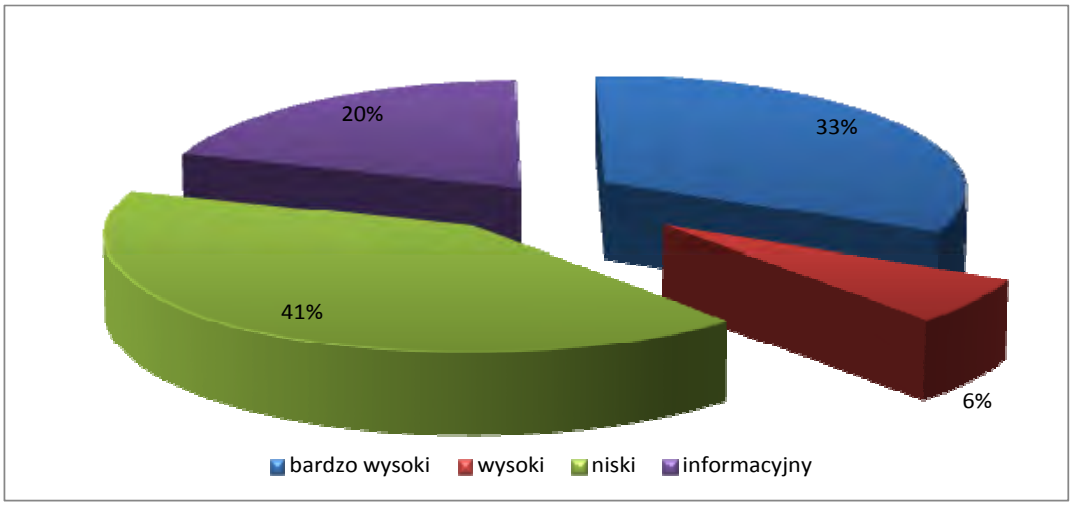
Opublikowany został biuletyn bezpieczeństwa, który likwiduje 59 podatności zarówno w bazie jak i innych produktach Oracle.
Poprawki usuwały błędy w niżej wymienionych programach:

1. Oracle Database (13 poprawek)
2. Oracle Fusion Middleware (7 poprawek)
3. Oracle Enterprise Manager (1 poprawka)
4. Oracle E-Business and Applications Suite (17 poprawek)
5. Oracle Solaris Products Suite (aż 21 nowych poprawek dla systemu Solaris)

## 5. Testy bezpieczeństwa witryn WWW instytucji państwowych

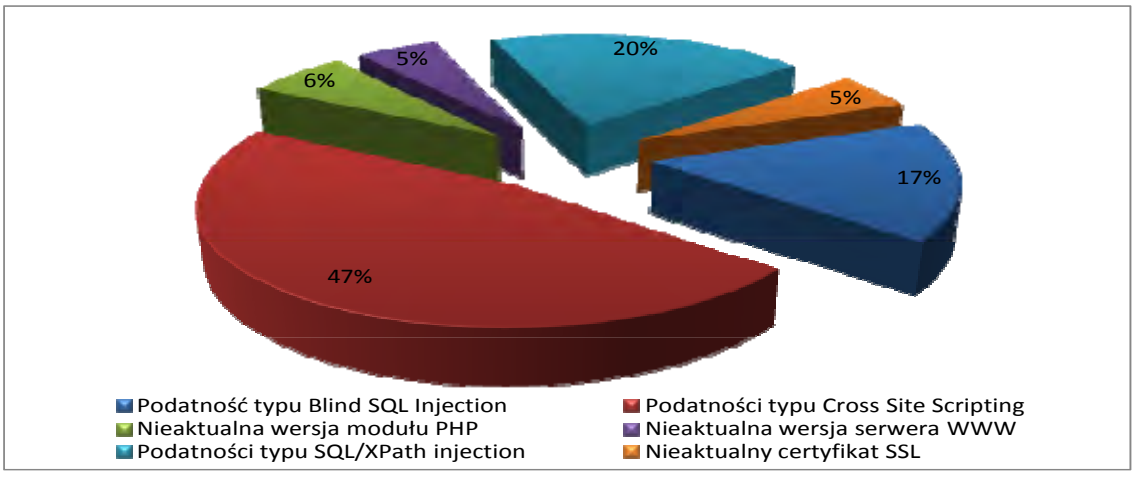
Zespół CERT.GOV.PL kontynuował testy bezpieczeństwa witryn WWW należących do instytucji państwowych.

W III kwartale 2010 roku przebadano 26 witryn należących do 18 instytucji państwowych. Stwierdzono ogółem 258 błędów w tym: 84 błędów o bardzo wysokim poziomie zagrożenia, 16 błędów o wysokim poziomie zagrożenia, 107 błędy o niskim poziomie zagrożenia i 51 błędów oznaczonych jako informacyjne.




**Rysunek 6 - 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. W dalszym ciągu istotnym problemem jest również wykorzystywanie w serwerach produkcyjnych nieaktualnych wersji oprogramowania.



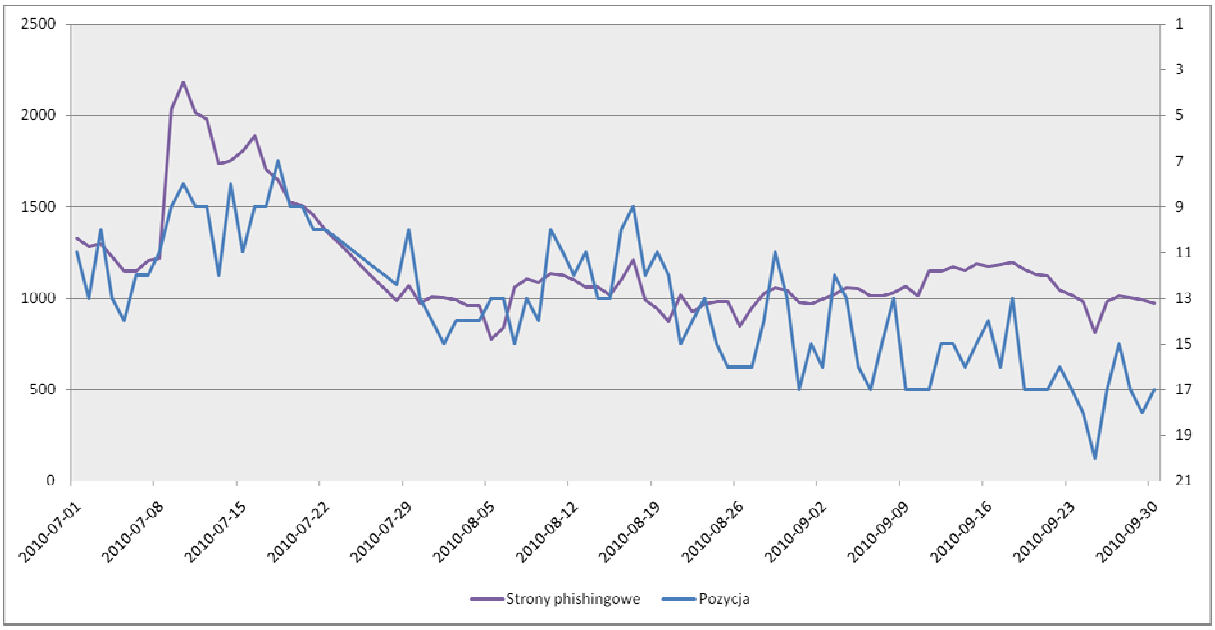

**Rysunek 7 - Procentowy rozkład najpoważniejszych błędów**

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

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.

Porównując kwartał III do kwartału II należy zauważyć ustabilizowanie się Polski na niskich pozycjach w niechlubnym rankingu krajów stwarzających zagrożenie dla bezpieczeństwa Internetu. Przez większość okresu raportowania Polska znajdowała się poza pierwszą dziesiątką. Działania zespołów bezpieczeństwa, które w poprzednim kwartale spowodowały spadek ilości stron służących do wyłudzania danych, pozwoliły na utrzymanie tego trendu. Bezpośrednio odzwierciedlone jest to w pozycji Polski w rankingu ATLAS.




**Rysunek 8 - Pozycja Polski w rankingu ATLAS i jej związek z phishingiem**

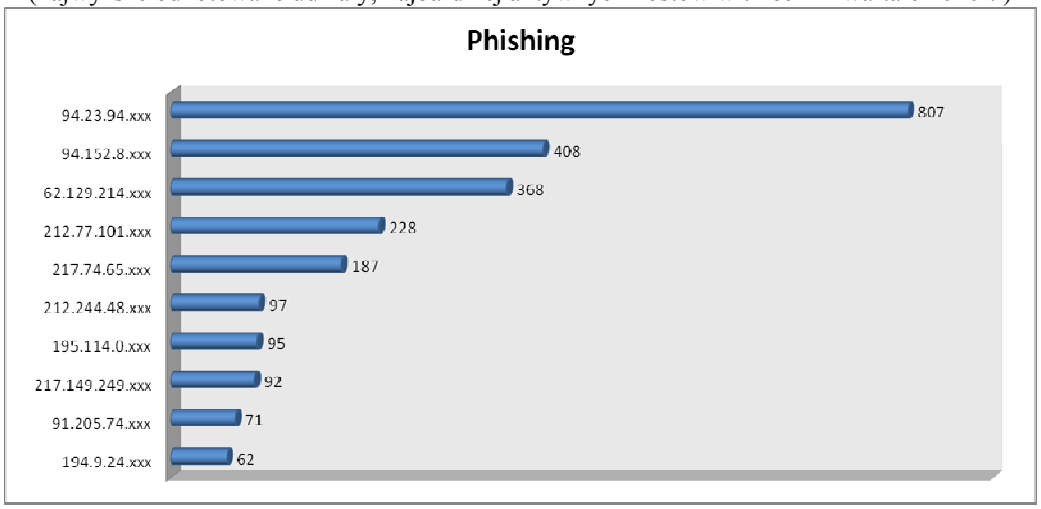
Brak nagłych skoków w ilości stron wyłudzających informacje nie pozwala na wyraźną korelację dat publikacji exploitów na systemy zarządzania treścią z ilością hostowanych stron phishingowych na polskich serwerach, co było możliwe w poprzednich okresach. Należy pamiętać, iż brak takiego przełożenia w obecnym okresie nie oznacza możliwości wystąpienia go w przyszłości. Zespół CERT.GOV.PL, nie stwierdził obecności działania 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 treść phishingowa jest jedynie dodawana, bez zmiany dotychczasowej zawartości stron w danej witrynie, co pozwala ukryć przed właścicielem dodanie nielegalnych treści.

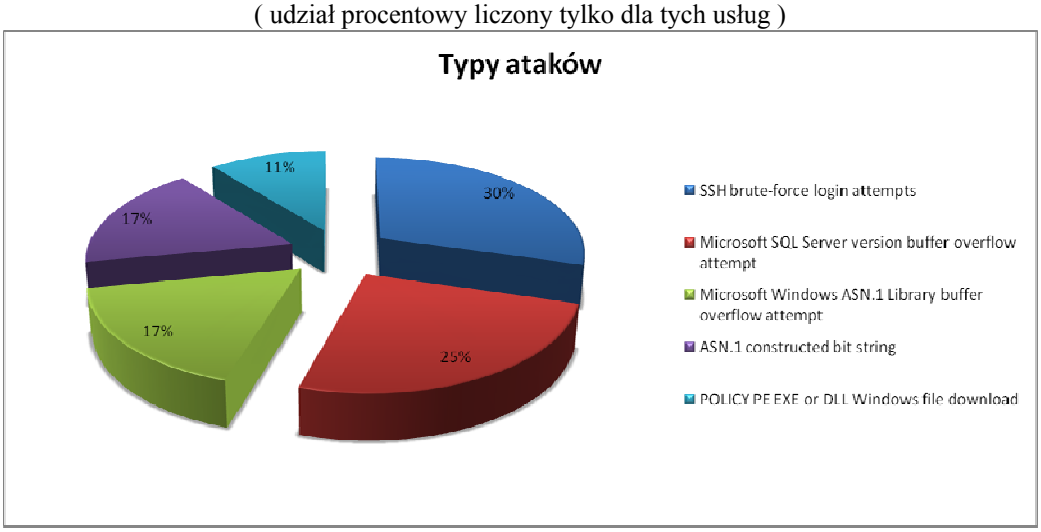
[6] http://atlas.arbor.net

[7] ang. b*ulletproof hosting* – usługa hostingowa 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.

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

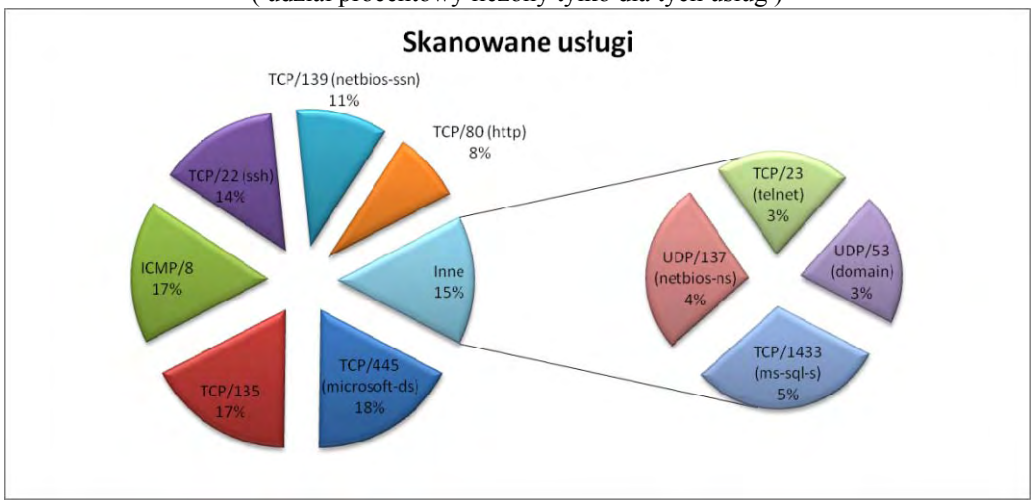



Statystyki ataków wg systemu Atlas (III kwartał 2010r.)
Pięć najczęściej występujących typów ataków wg systemu ATLAS – w trzecim kwartale 2010r.
( udział procentowy liczony tylko dla tych usług )

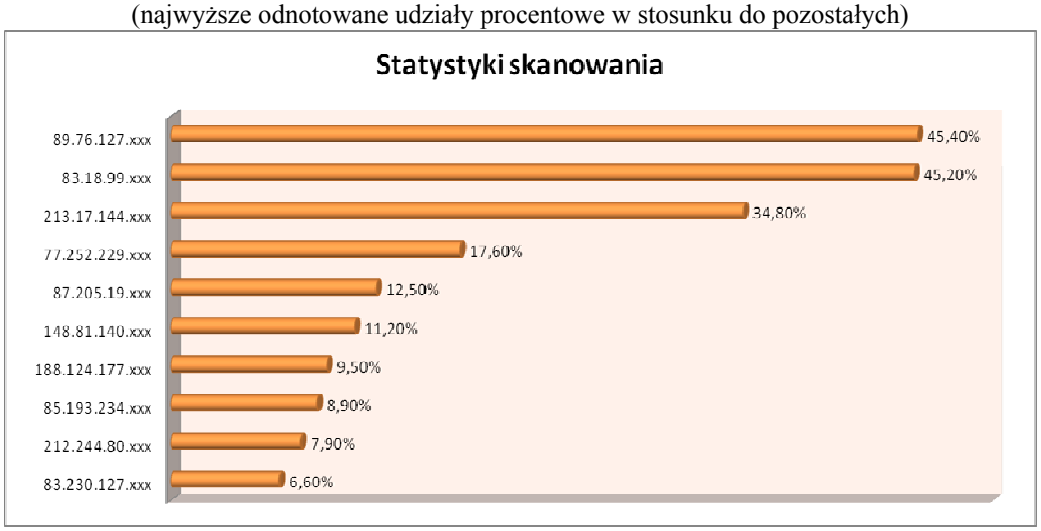



Najbardziej aktywne hosty w Polsce wg systemu ATLAS – w trzecim kwartale 2010r.
(najwyższe odnotowane udziały procentowe w stosunku do pozostałych)

Statystyki skanowania wg systemu Atlas (III kwartał 2010r.)
Najczęściej skanowane porty/usługi wg systemu ATLAS – w trzecim kwartale 2010r.
( udział procentowy liczony tylko dla tych usług )

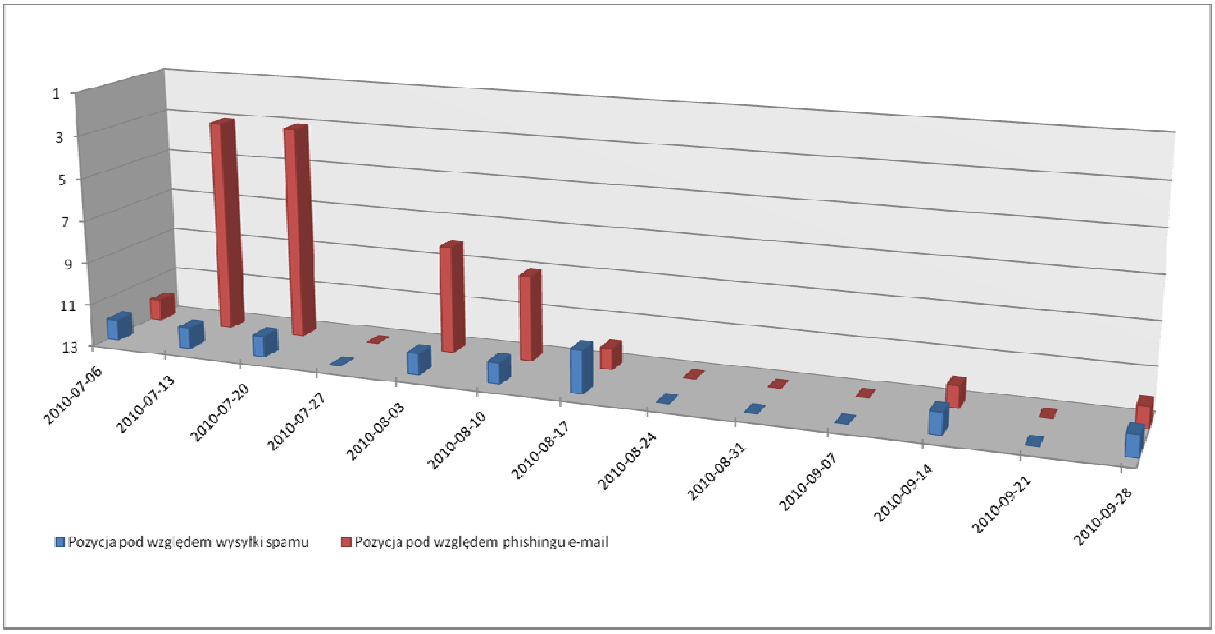



Najbardziej aktywne hosty w Polsce wg systemu ATLAS – w trzecim kwartale 2010r.
(najwyższe odnotowane udziały procentowe w stosunku do pozostałych)



### 6.1. Inne systemy zewnętrzne

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




**Rysunek 9 – 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, po raz kolejny plasuje się na wysokich miejscach. Biorąc pod uwagę ogólną ilość spamu wysyłanego z polskich podsieci sytuacja przedstawia się lepiej - Polska znajduje się praktycznie cały czas poza pierwszą 10-tką, a przez połowę okresu nie jest nawet klasyfikowana. Próby ograniczenia wysyłki niechcianych informacji zaczynają jednak przynosić efekty – widać wyraźny spadek ilości spamu w drugiej połowie kwartału..

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 10 – 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%, jednakże, nawet w szczytowych momentach nie przekroczył 18 %. Sytuacja jest zbliżona do statystyki z poprzedniego kwartału. Należy pamiętać, iż statystyka odnosi się do komputerów (pracujących pod kontrolą systemu operacyjnego Windows) włączonych w danym okresie. Dane zbierane są co 15 minut, a następnie uśredniane do postaci dziennej.

Analizując powyższe informacje można stwierdzić, iż pod względem potencjalnego zagrożenia dla użytkowników Internetu, Polska przestaje zajmować wysokie miejsca, w porównaniu do danych z poprzednich kwartałów. Aktualnie, obszarami budzącymi największe zaniepokojenie jest wysyłka spamu oraz poziom zawirusowania maszyn w polskiej cyberprzestrzeni. O ile spam jest (stosunkowo) najmniej szkodliwym działaniem to złośliwe oprogramowanie (zarażonych jest do 15% komputerów) stanowi duże zagrożenie dla bezpieczeństwa. Pod względem zagrożeń aktywnych (ataki, rozsyłanie wirusów drogą mailową, 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

W trzecim kwartale 2010r. pod auspicjami CERT.GOV.PL zorganizowano dwa szkolenia dla administratorów systemów teleinformatycznych instytucji sektora publicznego. Szkolenia obejmowały zagadnienia budowy systemów bezpieczeństwa sieci teleinformatycznych, ochrony przetwarzanych danych, analizę ryzyka, a także metodologię migracji pomiędzy poszczególnymi wersjami oprogramowania.