Agencja Bezpieczeństwa Wewnętrznego

Raport kwartalny CERT.GOV.PL
październik – grudzień 2009

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:

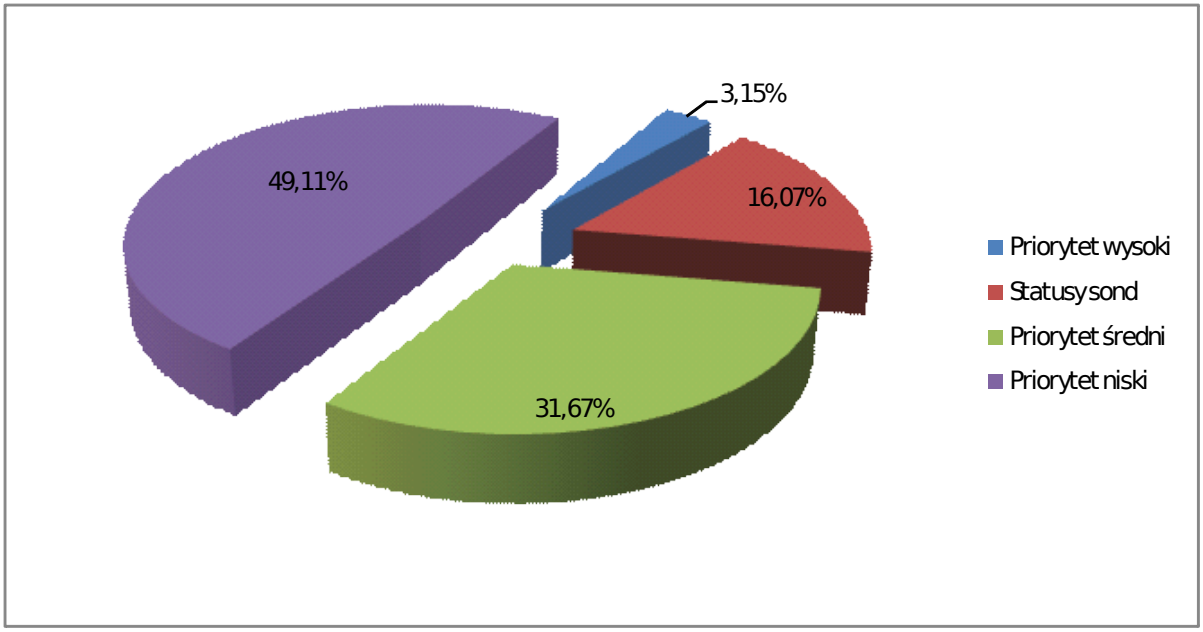
- E-mail: cert@cert.gov.pl
- Telefon: +48 22 58 58 844
- Fax: +48 22 58 56 099

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

2. Statystyki systemu ARAKIS-GOV[1]

W ostatnim kwartale 2009 roku, system ARAKIS-GOV zgłosił 1904 alarmy. Zdecydowaną większość stanowiły alarmy o priorytecie niskim − 935. Alarmy o priorytecie średnim wystąpiły 603 razy, natomiast alarmy diagnostyczne 306. System zgłosił najmniej alarmów o priorytecie wysokim – 60.

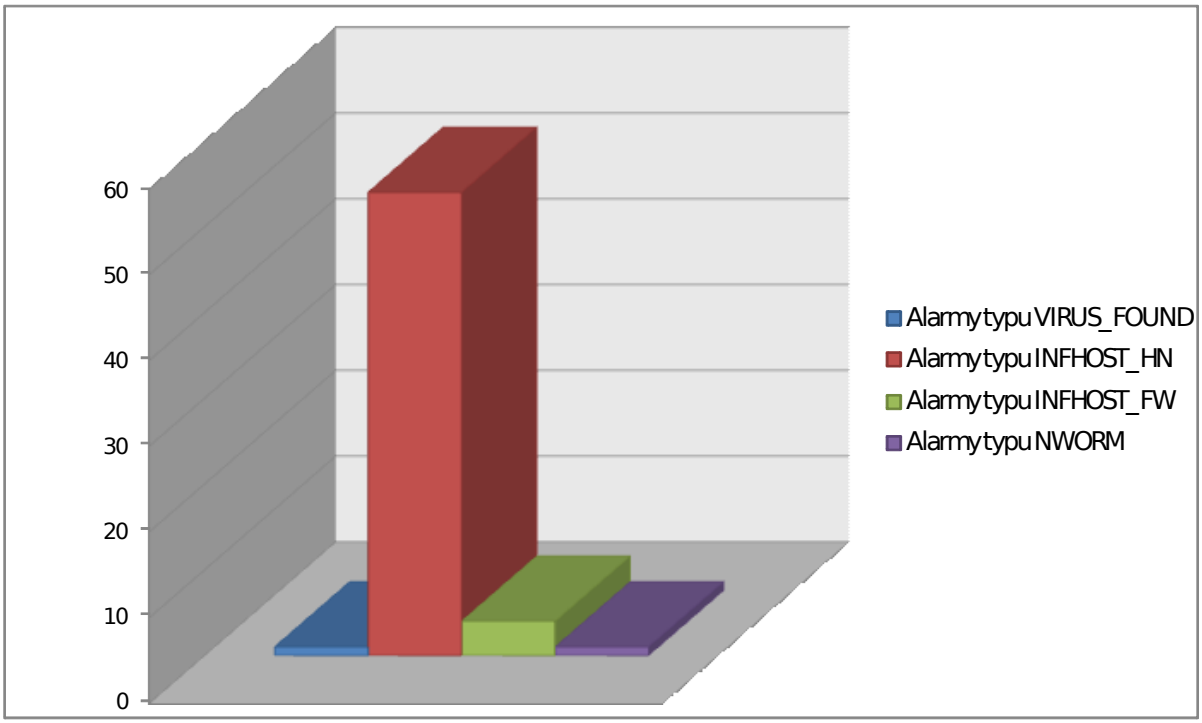
W porównaniu do poprzedniego kwartału procentowy udział poszczególnych typów zgłoszeń pozostał w przybliżeniu taki sam, przy prawie 25% wzroście liczby wszystkich alarmów.



Rysunek 1 - Procentowy rozkład ważności alarmów

[1] ARAKIS-GOV jest pasywnym systemem wczesnego ostrzegania o zagrożeniach w sieci Internet. W chwili obecnej został wdrożony w ponad 50 instytucjach państwowych.

Wśród alarmów o priorytecie wysokim zaobserwowano 54 alarmy typu INFHOST_HN[2], 4 alarmy VIRUS_FOUND[3], a także po jednym alarmie typu INFHOST_FW[4] oraz NWORM[5].



Rysunek 2 - Statystyki alarmów o wysokim priorytecie

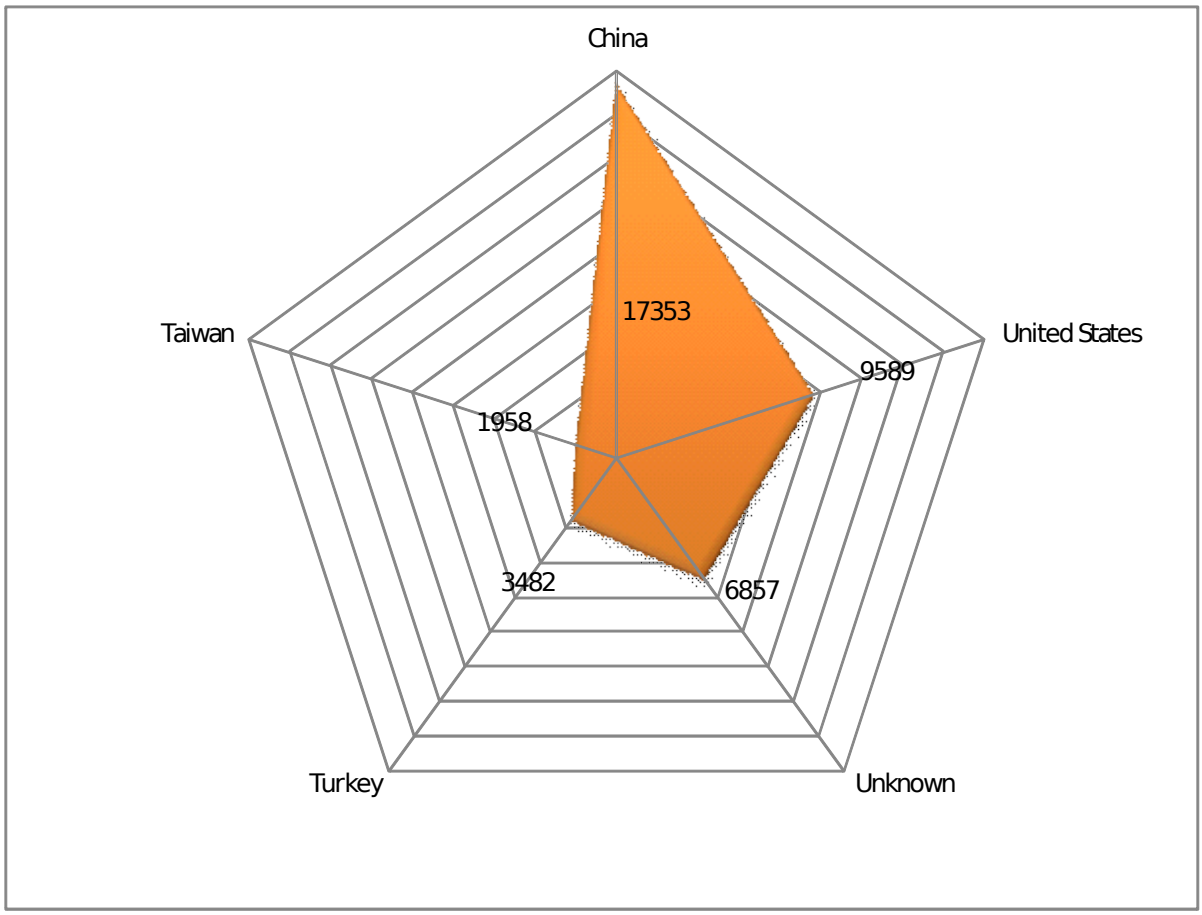
[2] Alarm INFHOST_HN oznacza potencjalne wykrycie zainfekowanego hosta w sieci wewnętrznej instytucji chronionej systemem ARAKIS-GOV. Alarm ten generowany jest na podstawie analizy danych z systemów typu honeypot.

[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)

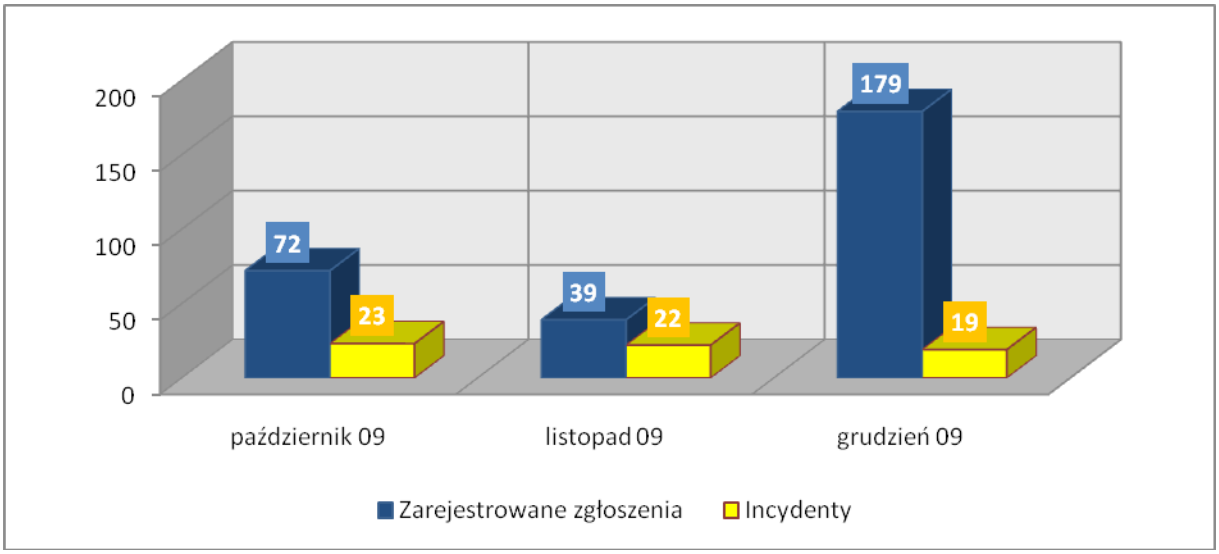
Na podstawie analizy adresu IP nadawcy pakietu stwierdzono, iż źródła ataków zaobserwowanych przez ARAKIS-GOV pochodziły najczęściej z sieci komputerowych Chin, Stanów Zjednoczonych, nieznanego nadawcy, Turcji oraz Tajwanu. Jednakże ze względu na specyfikę protokołu TCP/IP nie można bezpośrednio łączyć źródła pochodzenia pakietów z rzeczywistą 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 przejmują kontrolę.



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

3. Statystyki incydentów

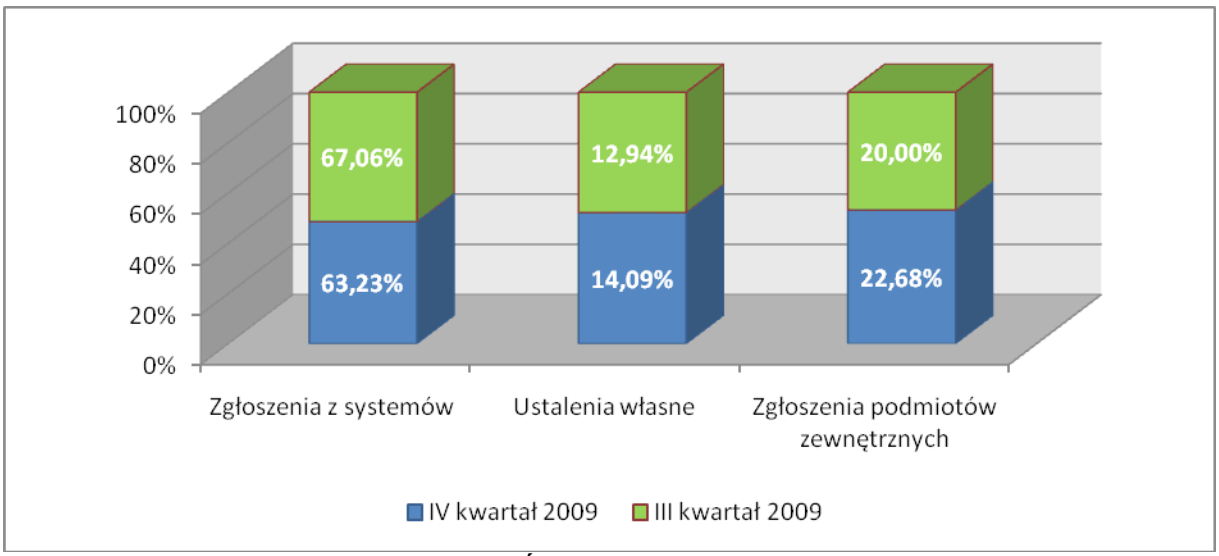
W czwartym kwartale 2009 roku do zespołu CERT.GOV.PL wpłynęło 290 zgłoszeń, przy czym tylko 64 z nich zostały zakwalifikowane jako faktyczne incydenty.



Rysunek 4 - Liczba zgłoszeń oraz faktycznych incydentów w poszczególnych miesiącach czwartego kwartału 2009

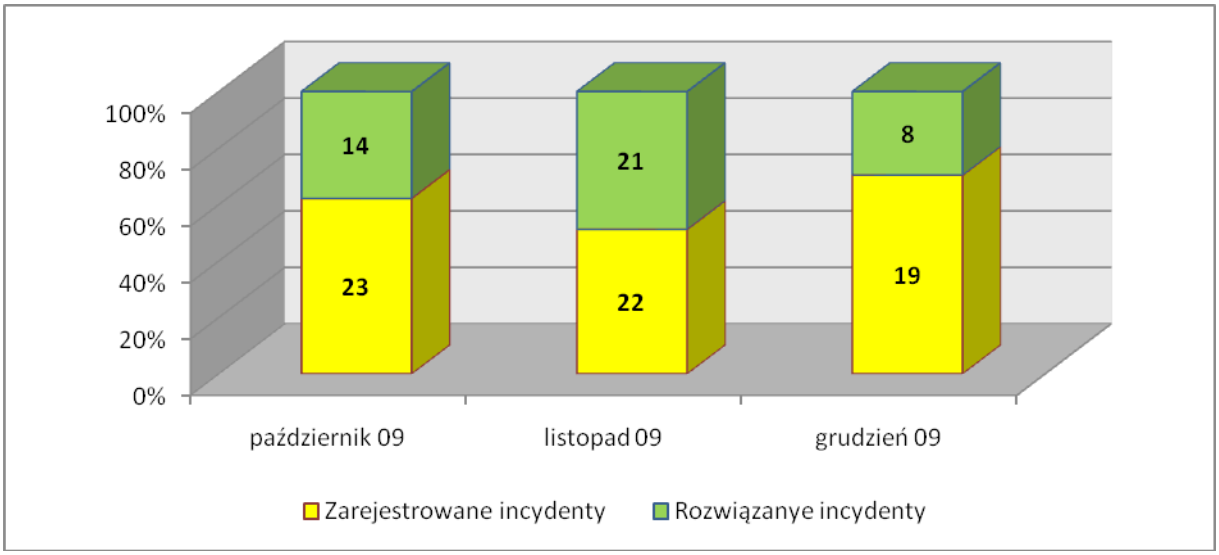
Duża liczba zgłoszeń w stosunku do liczby faktycznych incydentów wynika z faktu, iż część z nich stanowią tzw. „false-positives", czyli przypadki błędnej interpretacji, przez zgłaszającego, legalnego ruchu sieciowego. Ponadto większość zgłoszeń pochodzi z systemów automatyczne raportujących zdarzenia, które muszą dopiero zostać poddane ocenie człowieka.

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



Rysunek 5 - Źródła zgłoszeń incydentów

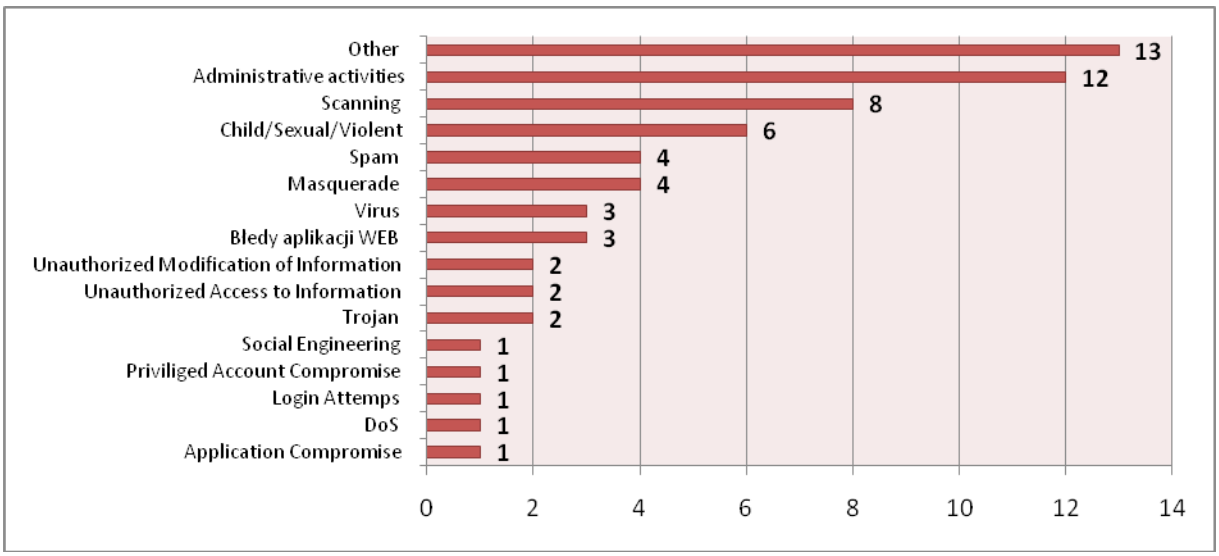
Rozkład miesięczny incydentów zarejestrowanych i incydentów, które zostały rozwiązane, przedstawia się następująco: w październiku 2009 zarejestrowano 23 incydenty, z czego rozwiązano 14, w listopadzie 2009 odnotowano 22 incydenty, z czego 21 zostało rozwiązanych, natomiast w grudniu 2009 przyjęto do realizacji 19 incydentów z czego 8 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 czwartego kwartału

Obserwowany w grudniu spadek liczby zakończonych incydentów ma niewątpliwie związek z okresem świątecznym, w czasie którego wydłuża się okres reakcji podmiotów zewnętrznych na zgłaszane problemy.

Podział zarejestrowanych incydentów na kategorie przedstawia się następująco:



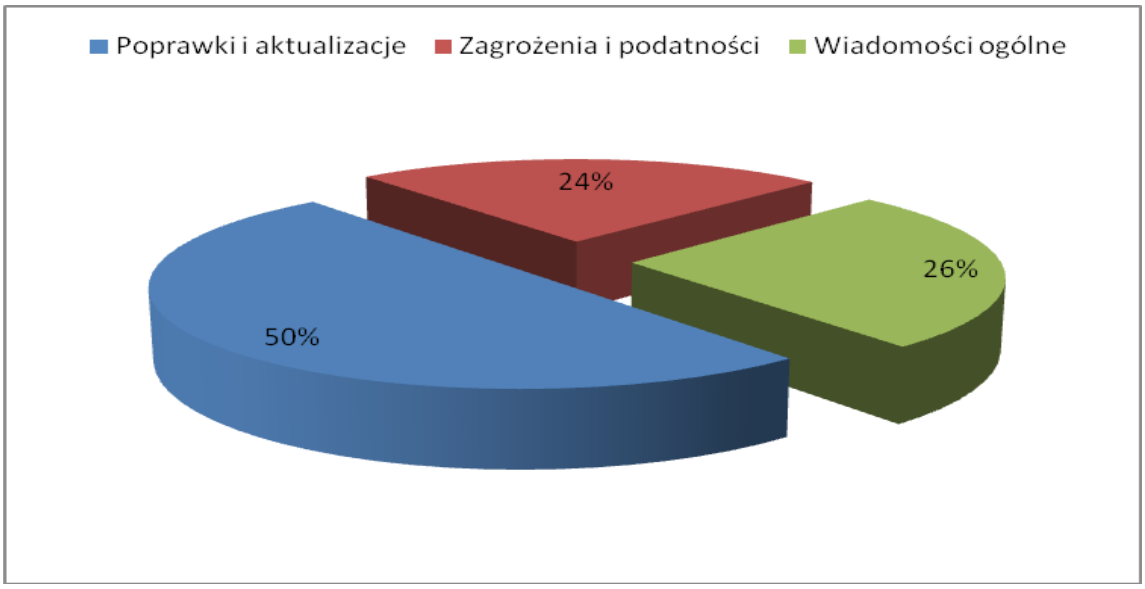
Rysunek 7 - Statystyka incydentów z podziałem na kategorie

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 biuletyny bezpieczeństwa udostępniane przez producentów sprzętu i oprogramowania.

W czwartym kwartale 2009 roku na witrynie www.cert.gov.pl umieszczono:

- 21 publikacji w kategorii „Poprawki i aktualizacje”,
- 10 publikacji w kategorii „Zagrożenie i podatności”,
- 11 publikacji w kategorii „Wiadomości ogólne”.



Rysunek 8 - Procentowy rozkład publikacji na witrynie www.cert.gov.pl

Najbardziej istotne publikacje dotyczące zagrożeń w czwartym kwartale 2009 roku dotyczyły:

- **Nowej fali ataków phishingowych ukierunkowanych na klientów usługi Outlook Web Access.**

Opublikowano informacje na temat nowej fali ataków phishingowych, których celem są klienci usługi Outlook Web Access. Do użytkowników rozsyłane są wiadomości, pochodzące rzekomo od administratora systemu, z prośbą o modyfikację ustawień OWA w związku z aktualizacją systemu. Do wiadomości e-mail dołączany jest link prowadzący do fałszywej strony OWA. Po wejściu na sfałszowaną stronę i zastosowaniu się do prośby o aktualizację ustawień w systemie, instalowany jest koń trojański Zeus/Zbot, którego głównym zadaniem jest zbieranie wykorzystywanych przez użytkownika identyfikatorów i haseł.

- **Podatności w produktach CISCO**

1. Błędy w Cisco Unified Presence:
   - Błąd w procesie TimesTenD może zostać wykorzystany do zerwania połączeń TCP na portach 16200 lub 22794.
   - Błąd w firewallu może zostać wykorzystany do wypełnienia tablicy połączeń co uniemożliwi zestawienie nowych połączeń TCP.

- **Biuletynów Bezpieczeństwa dla produktów firmy Adobe**

Rządowy Zespół Reagowanie na Incydenty Komputerowe informował o:

1. Biuletynie Bezpieczeństwa Adobe APSB09-15 dotyczącym likwidacji krytycznych podatności w Adobe Reader oraz w Adobe Acrobat. Wykorzystanie podatności umożliwiało zdalne wykonanie kodu na komputerze ofiary, zwiększenie lokalnych uprawnień oraz atak typu DoS (Denial-of-Service).
2. Biuletynie Bezpieczeństwa Adobe APSB09-16, który wskazywał podatności w Adobe Shockwave Player. Wykorzystanie luk bezpieczeństwa mogło doprowadzić do zdalnego wykonania kodu.
3. Istnieniu krytycznego błędu w produktach Adobe Reader i Adobe Acrobat w wersji 9.2 i wcześniejszych. Wykorzystanie podatności może prowadzić do przejęcia kontroli nad komputerem użytkownika, który otworzy specjalnie spreparowany plik pdf.
4. Biuletynie bezpieczeństwa Adobe APSB09-18 dla aplikacji Flash Media Server, który wskazywał podatnościa, umożliwiające przeprowadzenie ataku typu DoS (Denial of Service) lub skompromitowanie systemu użytkownika.
5. Biuletynie Bezpieczeństwa Adobe APSB09-19 dla aplikacji Adobe Flash Player i Adobe AIR. Wykryte nieprawidłowości umożliwiają przejęcie kontroli nad systemem operacyjnym ofiary.

- **Comiesięcznych biuletynów bezpieczeństwa firmy Microsoft**

Październikowy Biuletyn Bezpieczeństwa:

Październikowy Biuletyn Bezpieczeństwa informował o wykryciu oraz usunięciu dwunastu poważnych błędów. Siedem otrzymało status „krytyczny", pozostałe pięć zakwalifikowano jako „ważne". Luki o statusie „krytyczny" pozwalały na zdalne wykonanie kodu.

1. MS09-050 - biuletyn dotyczący usterek w Server Message Block Version 2 (SMBv2) - krytyczny
2. MS09-051 - biuletyn dotyczący błędów w programie Windows Media Runtime - krytyczny
3. MS09-052 - biuletyn dotyczący oprogramowania Windows Media Player - krytyczny
4. MS09-054 - biuletyn dotyczący zbiorczej aktualizacji zabezpieczeń dla programu Internet Explorer - krytyczny
5. MS09-055 - biuletyn dotyczący aktualizacji zabezpieczeń formatów ActiveX - krytyczny
6. MS09-061 - biuletyn dotyczący usterki w Microsoft. NET Framework oraz Microsoft Silverlight – krytyczny
7. MS09-062 - biuletyn dotyczący usterek interfejsu GDI + – krytyczny
8. MS09-053 - biuletyn dotyczący błędów w usłudze FTP dla Internet Information Services – ważny

9. MS09-056 - biuletyn dotyczący błędów składnika Windows CryptoAPI – ważny
10. MS09-057 - biuletyn dotyczący podatności w usłudze indeksowania – ważny
11. MS09-058 - biuletyn dotyczący błędów w jądrze systemu Windows – ważny
12. MS09-059 - biuletyn dotyczący błędów w zabezpieczeniach usługi LSASS – ważny

Listopadowy biuletyn bezpieczeństwa:

Listopadowy Biuletyn Bezpieczeństwa informował o wykryciu oraz usunięciu sześciu poważnych błędów. Trzy otrzymały status „krytyczny", pozostałe trzy „ważny". Luki o statusie „krytyczny" pozwalały na zdalne wykonanie kodu.

1. MS09-063 - biuletyn dotyczący usterki w zabezpieczeniach interfejsu WSDAPI - krytyczny
2. MS09-064 – biuletyn dotyczący luki w zabezpieczeniach serwera rejestrowania licencji (LLS) - krytyczny
3. MS09-065 – biuletyn dotyczący błędów w zabezpieczeniach sterowników trybu jądra systemu Windows - krytyczny
4. MS09-066 – biuletyn dotyczący błędów w zabezpieczeniach usługi Active Directory - ważny
5. MS09-067 – biuletyn dotyczący podatności programu Microsoft Office Excel - ważny
6. MS09-068 - biuletyn dotyczący podatności programu Microsoft Office Word - ważny

Grudniowy Biuletyn Bezpieczeństwa:

Grudniowy Biuletyn Bezpieczeństwa informował o wykryciu oraz usunięciu sześciu poważnych błędów. Trzy aktualizacje otrzymały status „krytyczne", pozostałe trzy zostały zakwalifikowane jako „ważne". Luki o statusie „krytyczny" pozwalały na zdalne wykonanie kodu.

1. MS09-071 – biuletyn dotyczący podatności w usłudze Internet Authentication Service (IAS) - krytyczny
2. MS09-072 – biuletyn dotyczący podatności w przeglądarce internetowej Internet Explorer - krytyczny
3. MS09-074 – biuletyn dotyczący biuletyn dotyczy podatności w oprogramowaniu Microsoft Office Project - krytyczny
4. MS09-069 – biuletyn dotyczący błędu usługi LSASS (Local Security Authority Subsystem Service) - ważny
5. MS09-070 – biuletyn dotyczący luki w zabezpieczeniach usługi Active Directory Federation Services – ważny
6. MS09-073 – biuletyn dotyczący podatności w aplikacji Microsoft WordPad i konwerterów tekstowych w pakiecie Microsoft Office - ważny

- **Podatność w jądrze systemu Linux RTL8169 NIC na atak typu DoS**

Opublikowano informacje na temat błędów sterownika karty sieciowej, opartej na chipsecie Realtek w jądrze Linuksa, podatnego na atak typu zdalne zatrzymanie usługi (Remote DoS). Wykorzystanie tej podatności może doprowadzić do zatrzymania systemu.

- **Poradnik bezpiecznej konfiguracji Red Hat Enterprise Linux5**

Na stronie www.cert.gov.pl opublikowane zostały najnowsze zalecenia National Security Agency (NSA) dotyczące bezpieczeństwa systemu Red Hat Enterprise Linux.

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

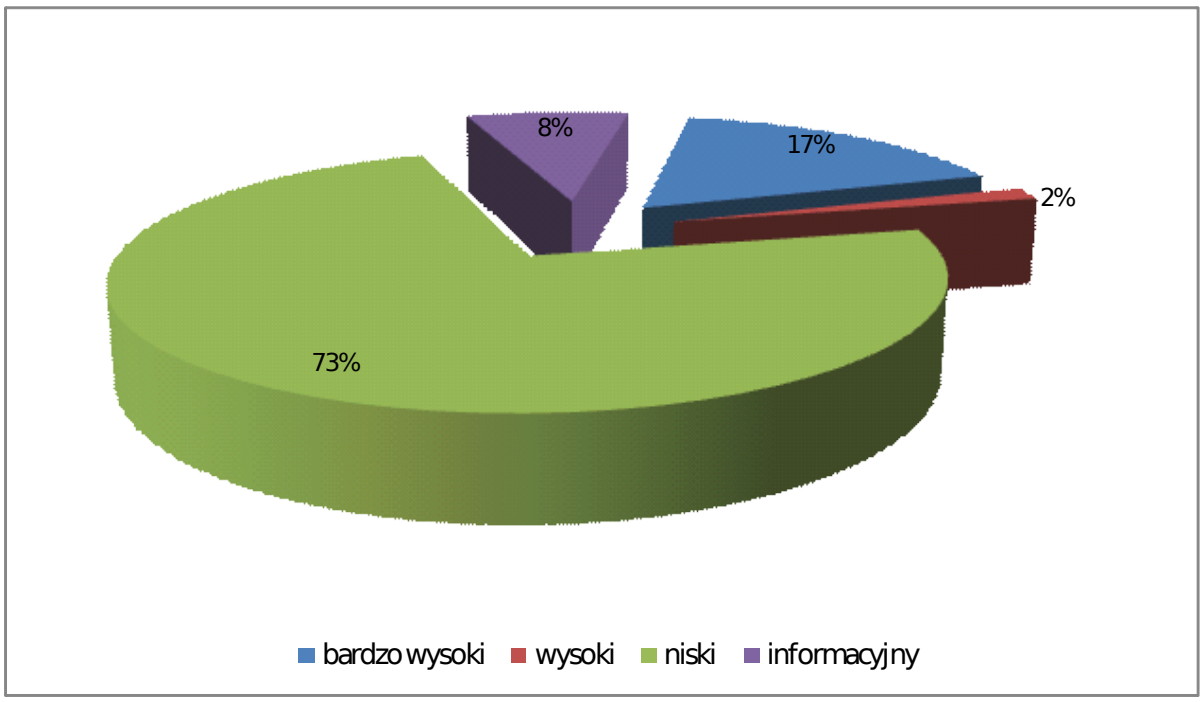
Zespół CERT.GOV.PL zamieścił na stronie informacje na temat:

- Uaktualnienia Security Update 2009-006/Mac OS X v10.6.2 firmy Apple. Aktualizacja usuwa błędy, które pozwalają atakującemu na zdalne wykonanie kodu, przeprowadzenie ataku typu DoS (Denial of Service), przeprowadzenie ataku typu man-in-the-middle, wyjawienie poufnych danych czy zwiększenie praw administracyjnych.
- Podatności w Apple Safari, które pozwalały atakującemu na obejście zabezpieczeń, wyjawienie poufnych danych lub uszkodzenie systemu użytkownika.

5. Testy bezpieczeństwa witryn WWW instytucji państwowych

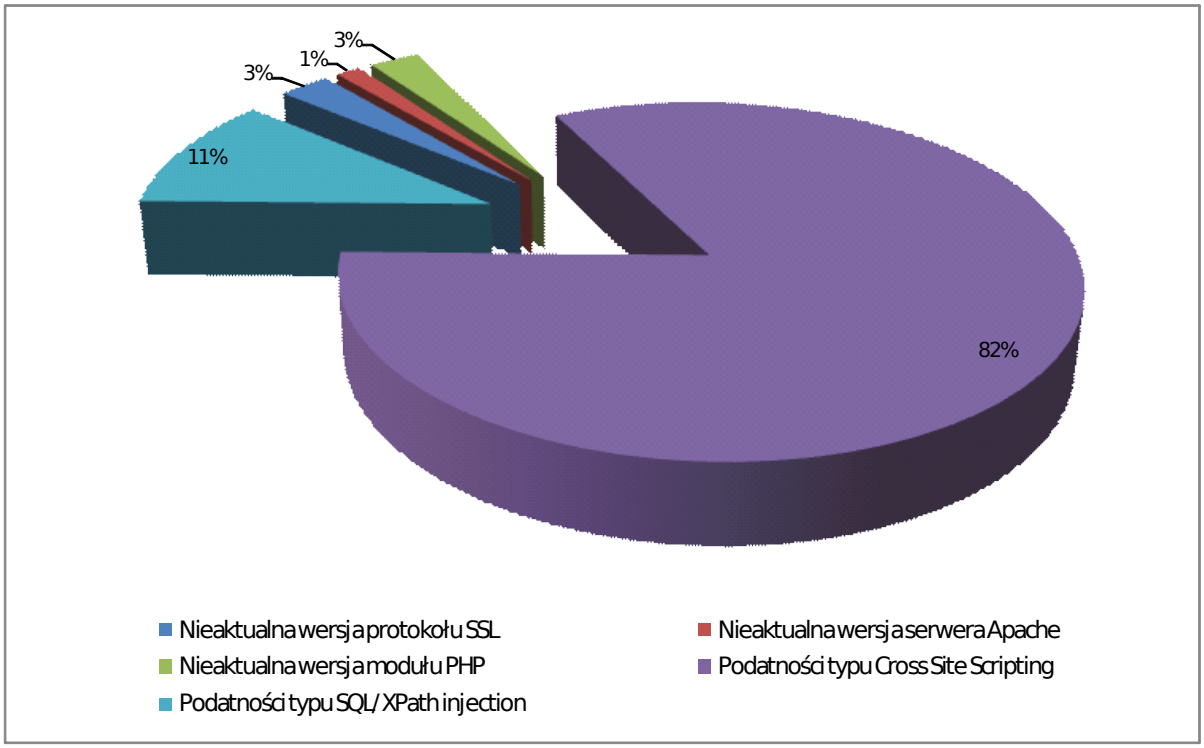
W IV kwartale 2009 roku zespół CERT.GOV.PL kontynuował testy bezpieczeństwa witryn należących do instytucji państwowych.

W okresie tym przebadano 16 witryn należących do 5 instytucji państwowych.
Stwierdzono ogółem 431 błędów w tym: 74 błędy o bardzo wysokim poziomie zagrożenia, 7 błędów o wysokim poziomie zagrożenia, 315 błędów o niskim poziomie zagrożenia i 35 błędów oznaczonych jako informacyjne.



Rysunek 9 - 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 oraz SQL/XPath Injection. Istotnym problemem jest również wykorzystywanie w serwerach produkcyjnych nieaktualnych wersji oprogramowania.



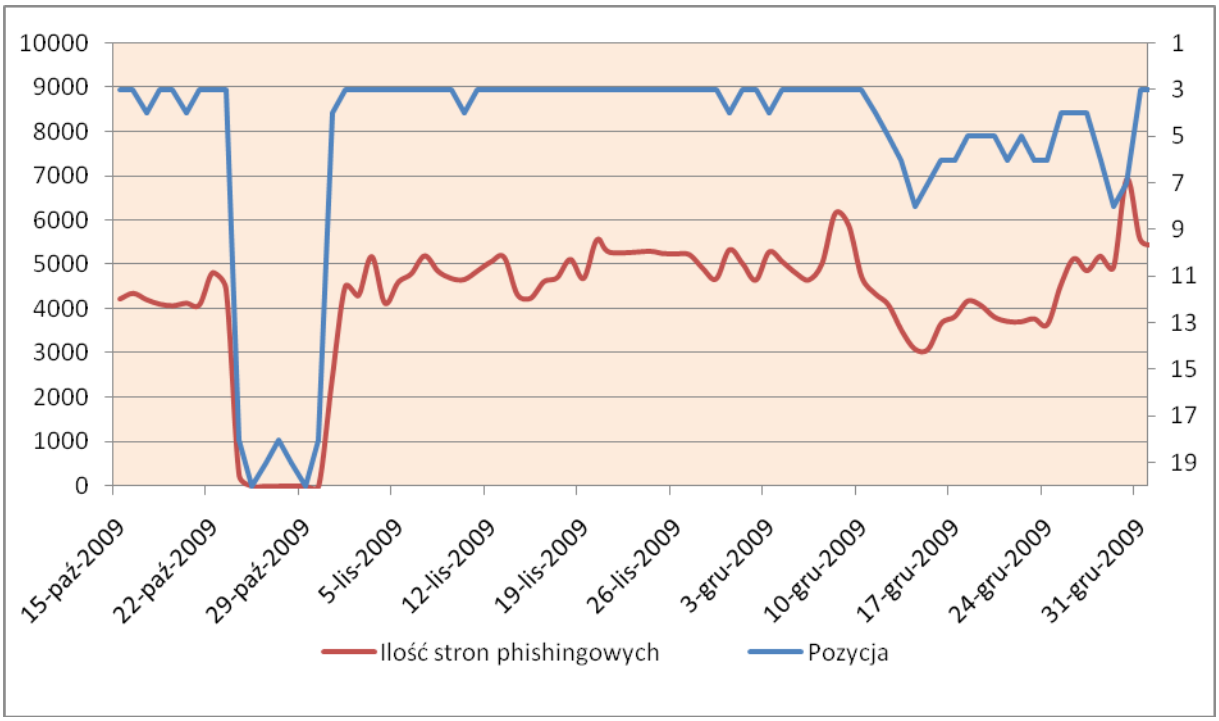
Rysunek 10 - Procentowy rozkład najpoważniejszych błędów

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 systemu ATLAS[6]

System ATLAS 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 IV kwartale 2009 roku pozycja Polski, pod względem zagrożenia dla bezpieczeństwa Internetu, nadal jest bardzo wysoka – utrzymuje się w okolicach 3-go miejsca. Tak jak poprzednio spowodowane jest to dużą liczbą witryn phishingowych umieszczonych w polskiej przestrzeni adresowej.



Rysunek 11 - Pozycja Polski w rankingu ATLAS i jej związek z phishingiem

Na powyższym wykresie widać wyraźną korelację pomiędzy zajmowaną pozycją a liczbą stron phishingowych. Szczególnie widoczne jest to w ostatnim tygodniu października, gdy na skutek awarii podsystemu zajmującego się analizą informacji o phishingu, Polska spadła natychmiast w okolice miejsca 19-go. W pozostałych kategoriach, (ataki, liczba botnetów itp) mających wpływ na miejsce w rankingu, udział Polski w ogólnej ilości zagrożeń jest bowiem stosunkowo niewielki.

W opinii Zespołu CERT.GOV.PL duża liczba stron phishingowych w polskiej przestrzeni adresowej nie wynika z działalności w Polsce firm oferujących tzw. kuloodporny hosting[7], lecz z dużej liczby słabo zabezpieczonych witryn WWW, na których po przełamaniu zabezpieczeń włamywacze umieszczają nieautoryzowane treści. W większości przypadków są

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

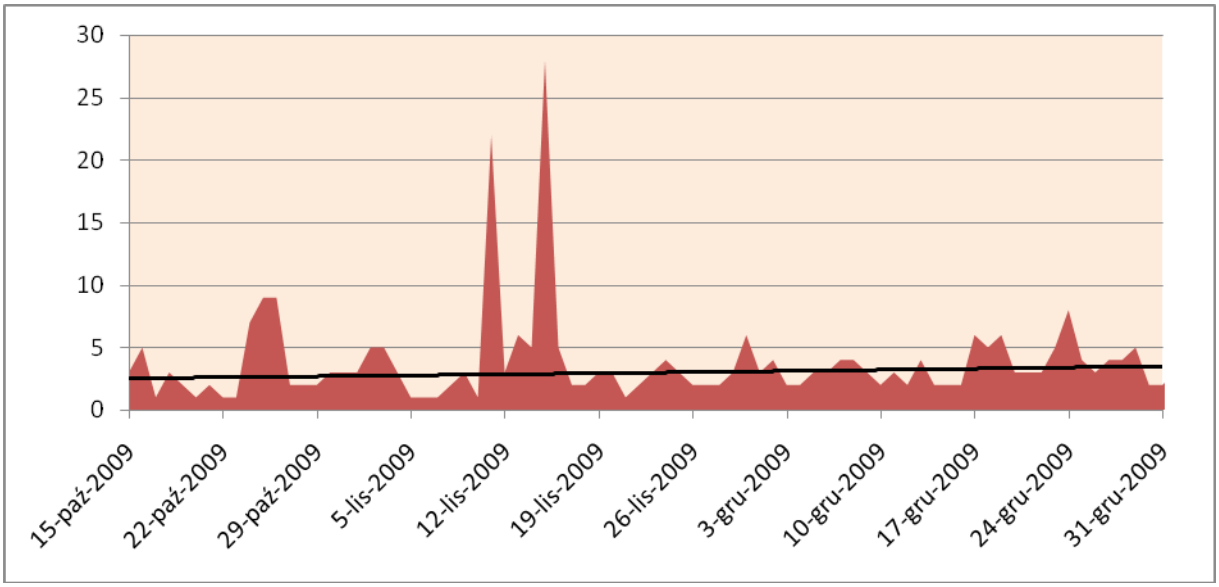
[7] ang. b*ulletproof hosting* – usługa hostingowi polegająca na udostępnieniu przestrzeni dyskowej i łącza bez ograniczeń co do publikowanych przez usługobiorcę treści. Bardzo często tego typu hosting wykorzystywany jest przy phishingu, działaniach spamerskich lub publikacji pornografii. W przypadku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

to prywatne strony WWW, których właściciele nie wiedzą o włamaniu, ponieważ zazwyczaj legalna treść nie jest zmieniana, a jedynie dodawane są dodatkowe podstrony, do których nie ma linków ze strony głównej, co pozwala ukryć przed właścicielem nielegalne treści na jego stronie.

Należy zauważyć ciągłą tendencję wzrostową w liczbie tego typu stron w polskiej przestrzeni adresowej.
W porównaniu do minionego kwartału, zmienił się udział poszczególnych systemów autonomicznych AS:

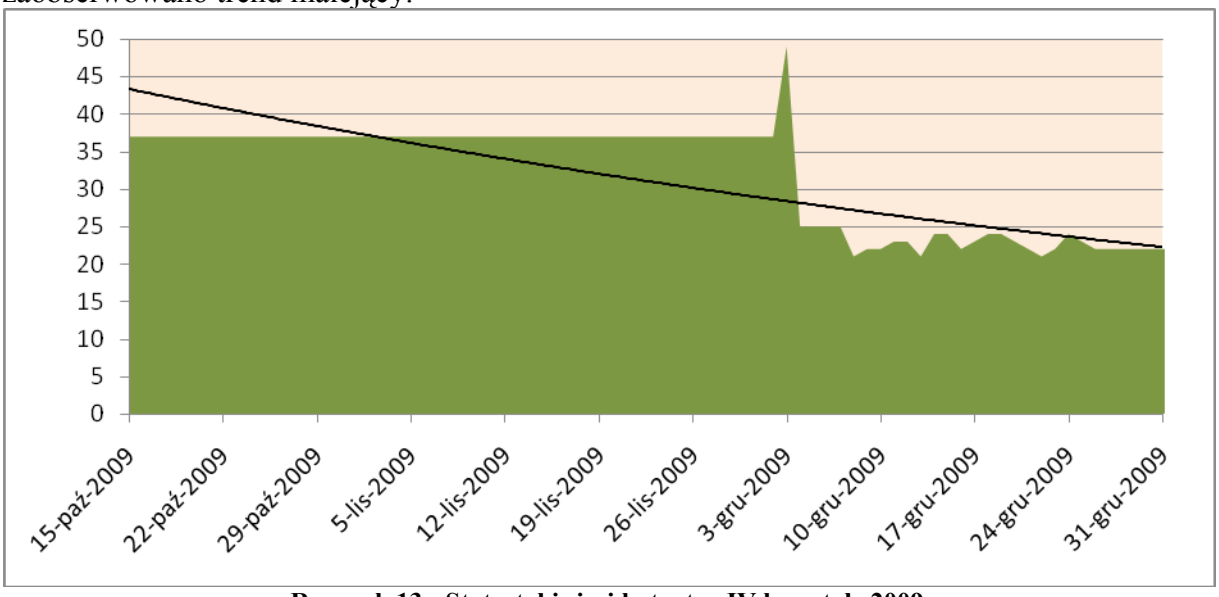
- dla AS16138 zmalał z 40% do 19%
- dla AS16276 zmalał z 35% do 10%
- dla AS29522 wzrósł do ponad 25%
- dla AS12826 wzrósł do ponad 17%

Podobnie jak w przypadku phishingu, trend ataków kierowanych z zakresów adresowych Polski w stronę pozostałych obszarów Internetu pozostaje w miarę stały z lekką tendencją wzrostową. Na tym tle wyraźnie widać próby ataków skierowanych najprawdopodobniej z botnetów przeciwko wybranym celom (11 i 15 XI). Przedstawia to poniższy wykres.



Rysunek 12 - Ataki pochodzące z polskiej przestrzeni adresowej

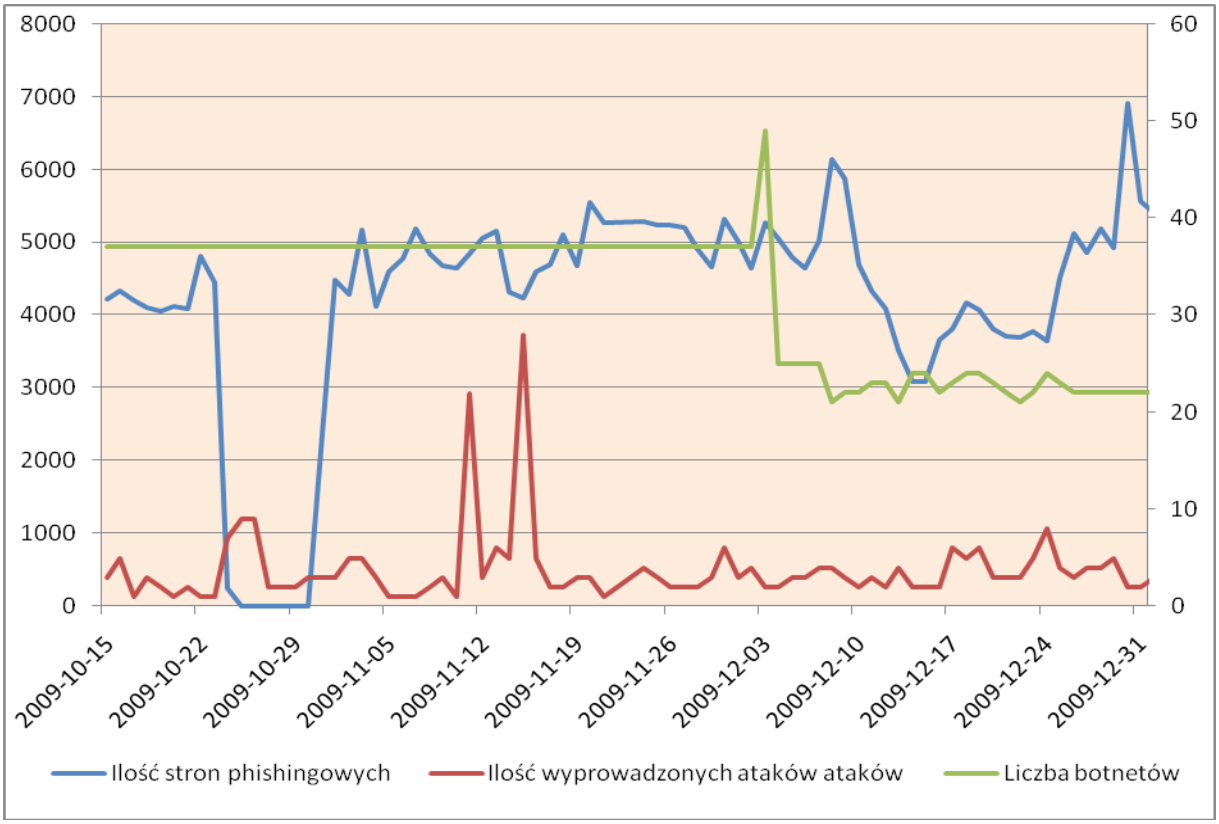
W przypadku liczby serwerów botnetów wykrytych w polskiej przestrzeni adresowej zaobserwowano trend malejący.



Rysunek 13 - Statystyki sieci botnet w IV kwartale 2009

Wyraźna zmiana w tym zakresie spowodowana jest zarówno zmianą metod wykrywania zarażonych komputerów, jak i działaniami, na całym świecie, skierowanymi przeciwko systemom kierującym grupami zarażonych komputerów zombie.

W drugiej połowie grudnia można zauważyć pewną korelację pomiędzy liczbą wykrytych bonetów a wyprowadzanych ataków. Kierunki i zależności tych przebiegów będą badane w kolejnych kwartałach po zebraniu odpowiedniej ilości danych.



Rysunek 14 - Wykres porównawczy ilości botnetów, stron phisingowych i ataków