Agencja Bezpieczeństwa Wewnętrznego

Raport kwartalny CERT.GOV.PL

październik – grudzień 2011

1. Informacje dotyczące zespołu CERT.GOV.PL

Rządowy Zespół Reagowania na Incydenty Komputerowe CERT.GOV.PL został powołany w dniu 1 lutego 2008 roku. Podstawowym zadaniem zespołu jest zapewnianie i rozwijanie zdolności jednostek organizacyjnych administracji publicznej Rzeczypospolitej Polskiej do ochrony przed cyberzagrożeniami, ze szczególnym uwzględnieniem ataków ukierunkowanych na infrastrukturę obejmującą systemy i sieci teleinformatyczne, których zniszczenie lub zakłócenie może stanowić zagrożenie dla życia, zdrowia ludzi, dziedzictwa narodowego oraz środowiska w znacznych rozmiarach, albo spowodować poważne straty materialne, a także zakłócić funkcjonowanie państwa.

Do zakresu świadczonych przez CERT.GOV.PL usług należy:

- koordynacja reagowania na incydenty,
- publikacja alertów i ostrzeżeń,
- obsługa i analiza incydentów (w tym gromadzenie dowodów realizowane przez zespół biegłych sądowych),
- publikacja powiadomień (biuletynów zabezpieczeń),
- koordynacja reagowania na luki w zabezpieczeniach,
- obsługa zdarzeń w sieciach objętych ochroną przez system ARAKIS-GOV,
- przeprowadzanie testów bezpieczeństwa.

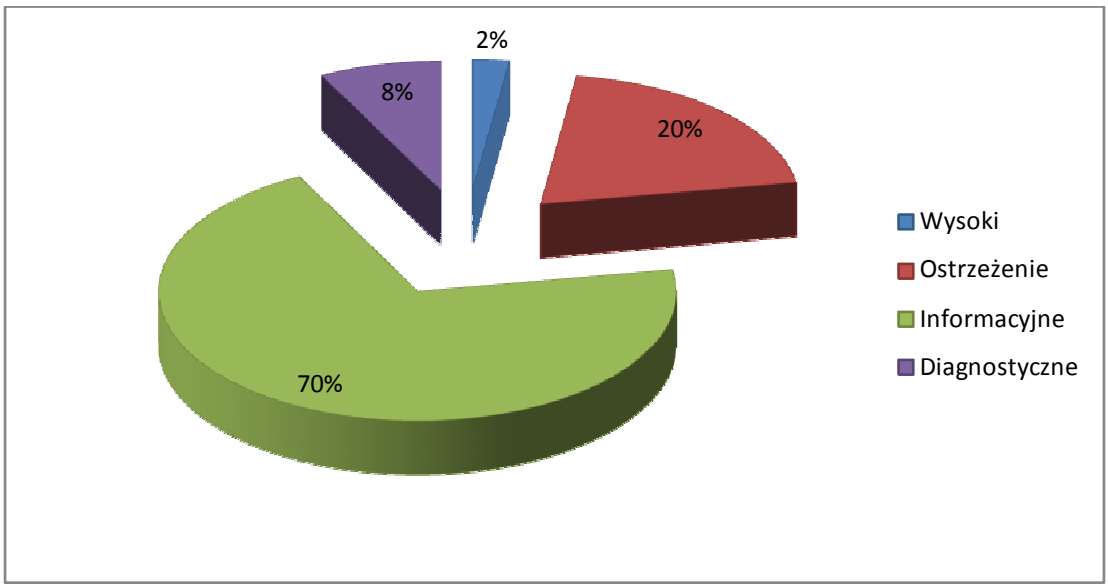
Dane kontaktowe:

- E-mail: cert@cert.gov.pl
- Telefon: +48 22 58 56 152 / +48 22 58 56 176
- 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]

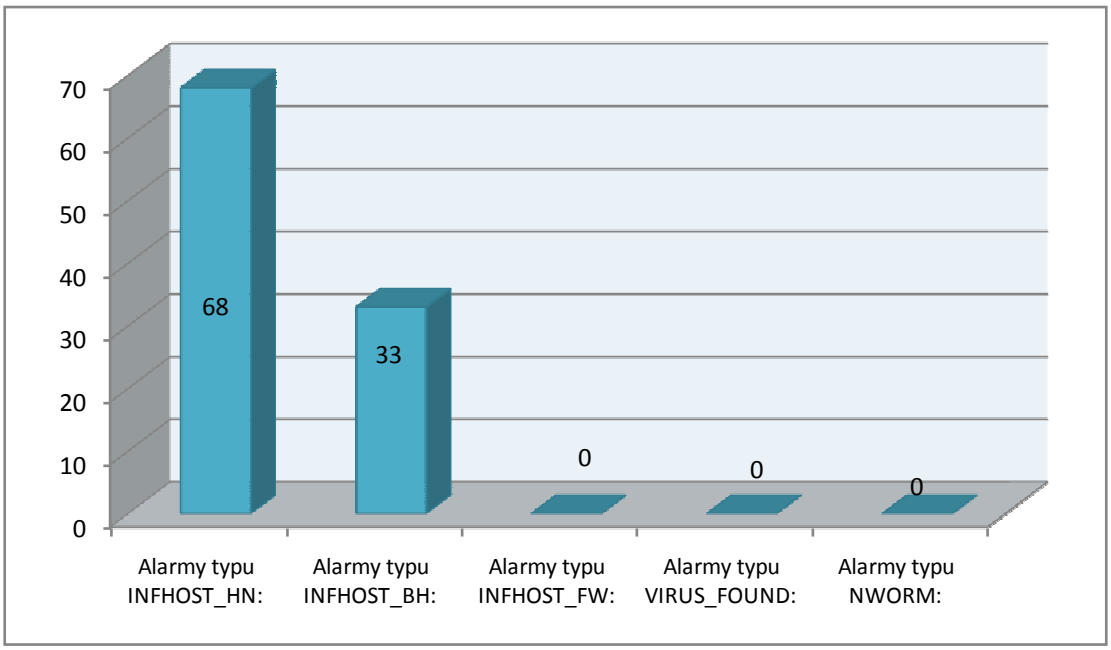
W ostatnim kwartale 2011 roku zdecydowaną większość stanowiły alarmy informacyjne, które stanowiły aż 70 procent wszystkich zarejestrowanych przez system ARAKIS-GOV. Alarmy o priorytecie średnim stanowiły 20%, natomiast alarmy diagnostyczne 8%. System zgłosił najmniej alarmów o priorytecie wysokim – 101, co stanowiło 2% wszystkich alarmów.



Rysunek 1 - Procentowy rozkład ważności alarmów

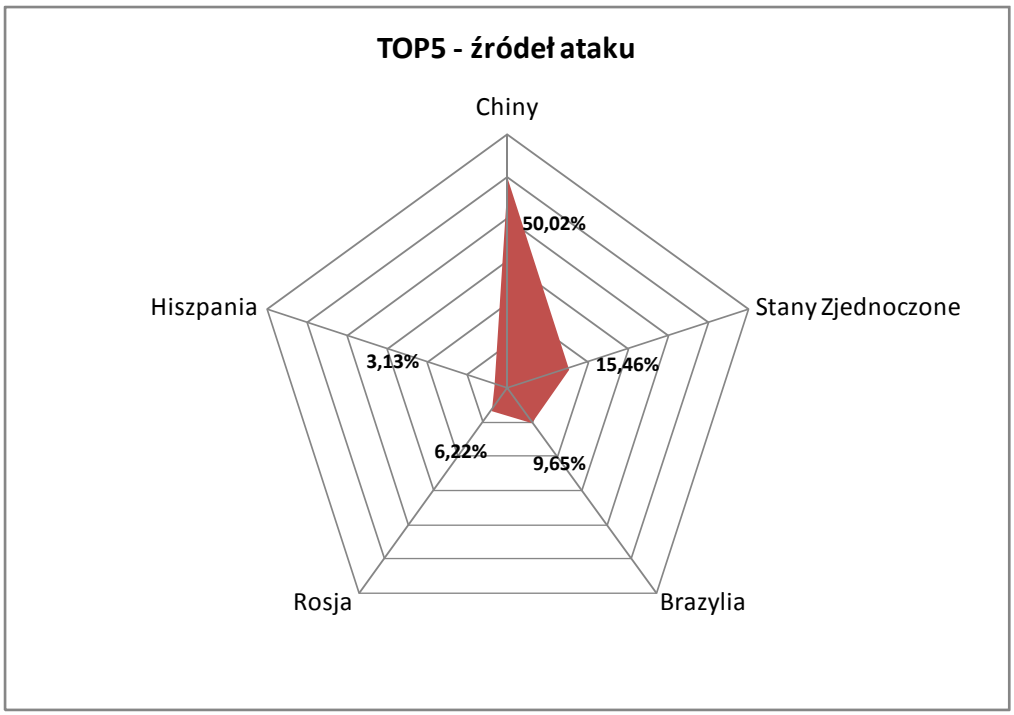
Wśród alarmów o priorytecie wysokim zaobserwowano 68 alarmów typu INFHOST_HN[2], 33 alarmów typu INFHOST_BH[3]. Nie odnotowano alarmów typu INFHOST_FW[4], VIRUS_FOUND[5] i NWORM[6].

[1] ARAKIS-GOV jest pasywnym systemem wczesnego ostrzegania o zagrożeniach w sieci Internet. W chwili obecnej został wdrożony w ponad 60 instytucjach państwowych.
[2] Alarm INFHOST_HN oznacza potencjalne wykrycie zainfekowanego hosta w sieci wewnętrznej instytucji chronionej systemem ARAKIS-GOV. Alarm ten generowany jest na podstawie analizy danych z systemów typu honeypot.
[3] Alarm INFHOST_BH oznacza wykrycie połączenia z domeną, która oznaczona została jako złośliwa tzn. przy pomocy której propagowane jest oprogramowanie złośliwe.
[4] Alarm 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 VIRUS_FOUND oznacza wykrycie infekcji wirusowej w sieci wewnętrznej chronionej instytucji. Alarm ten generowany jest na podstawie informacji pochodzących ze skanerów antywirusowych serwerów pocztowych
[6] Alarm NWORM oznacza potencjalne wykrycie nowego, szybko rozprzestrzeniającego się zagrożenia sieciowego (robaka sieciowego) – w tym przypadku wszystkie 3 alarmy były alarmami fałszywymi (false-positive)



Rysunek 2 - Statystyki alarmów o wysokim priorytecie.

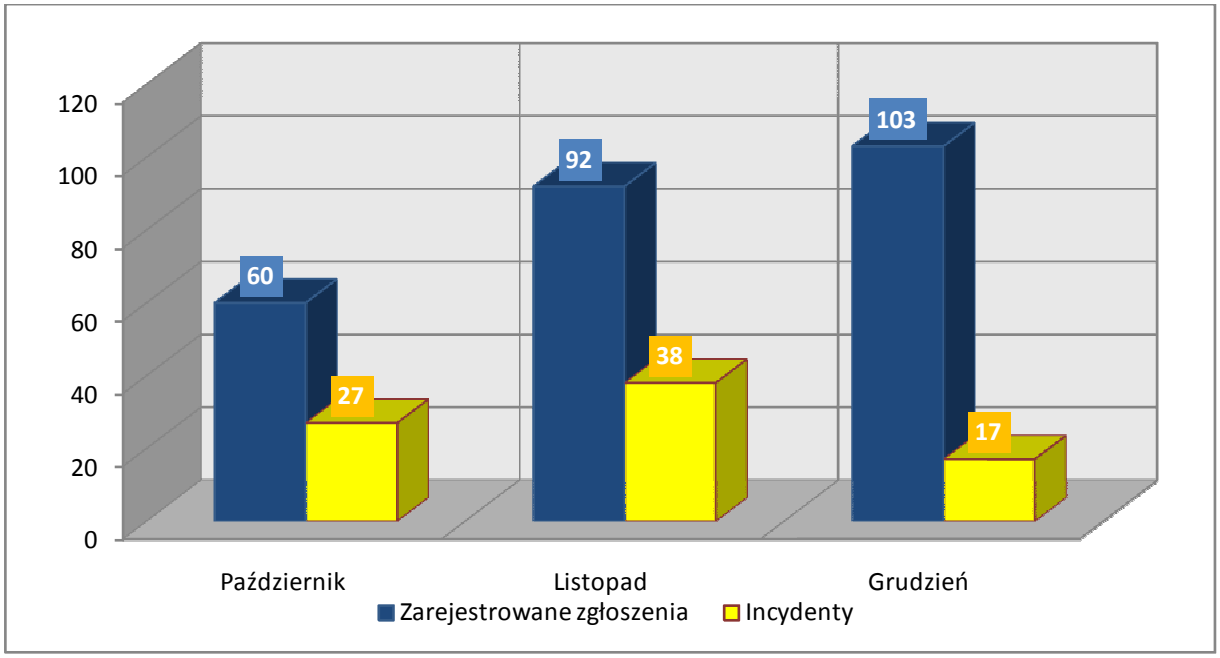
W wyniku analizy zarejestrowanych połączeń stwierdzono, iż w większości źródłem ataku były sieci komputerowe przypisane do Chin, Stanów Zjednoczonych, Brazylii, Rosji oraz Hiszpanii. Jednakże mając na uwadze specyfikę protokołu TCP/IP, nie można bezpośrednio łączyć źródła pochodzenia pakietów z faktyczną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

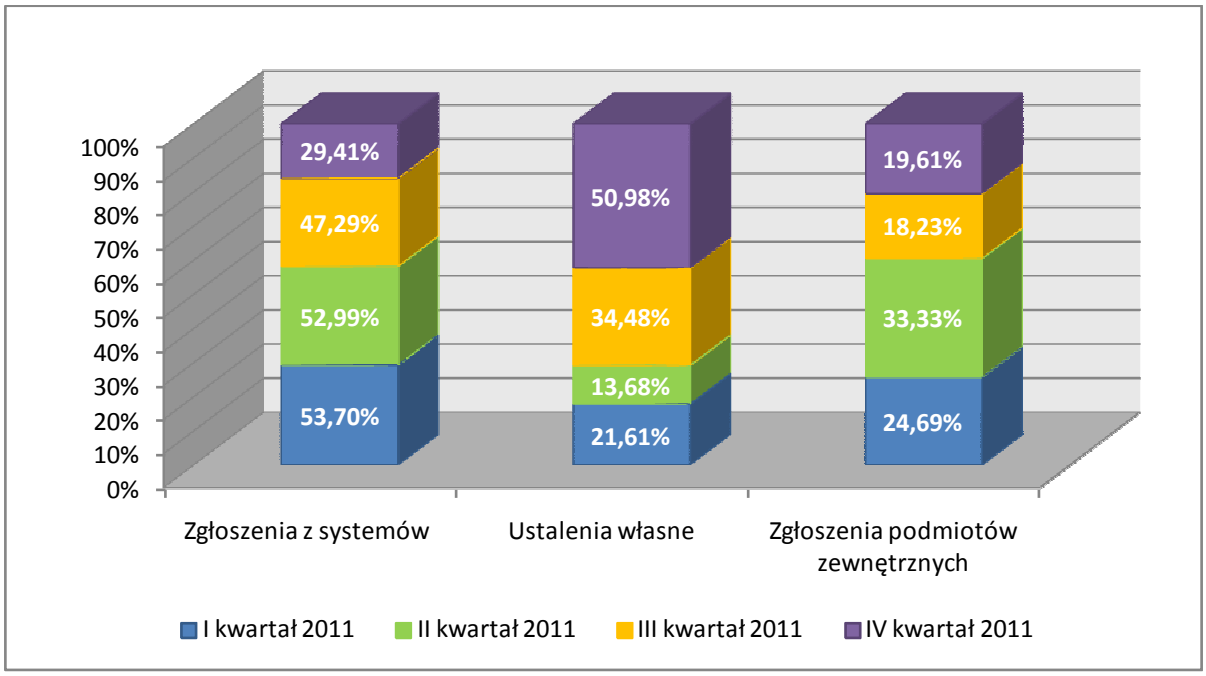
3. Statystyki incydentów

W czwartym kwartale 2011 roku do zespołu CERT.GOV.PL wpłynęło 255 zgłoszeń, z których 82 zostały zakwalifikowane jako incydenty.



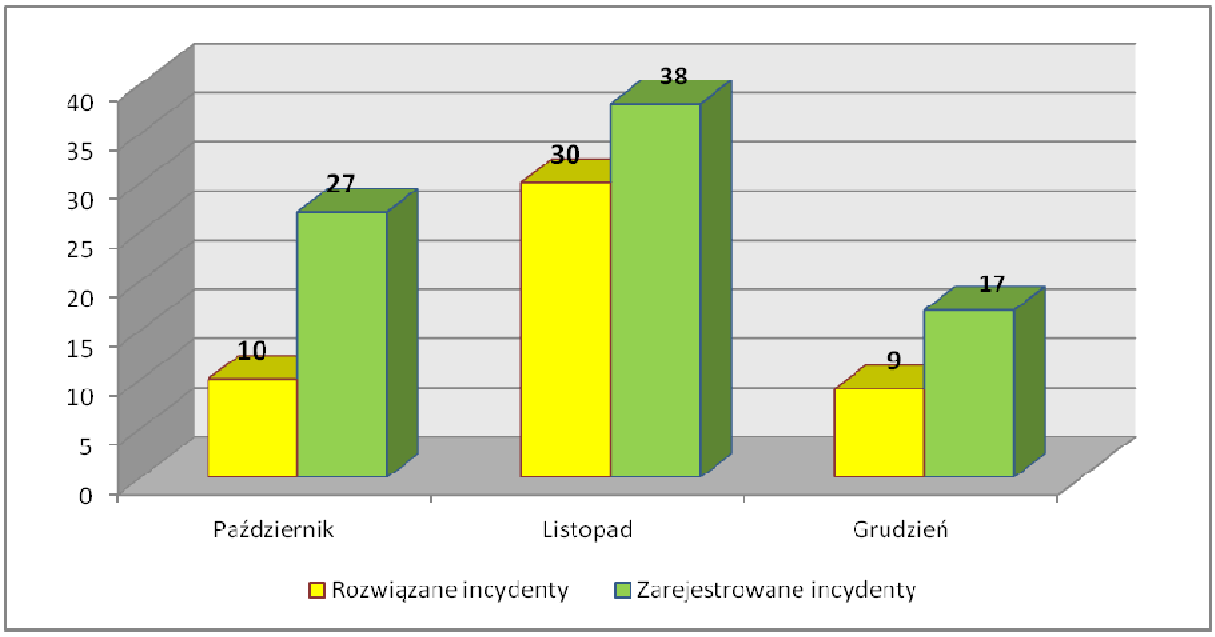
Rysunek 4 - Liczba zgłoszeń oraz faktycznych incydentów w poszczególnych miesiącach czwartego kwartału 2011

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



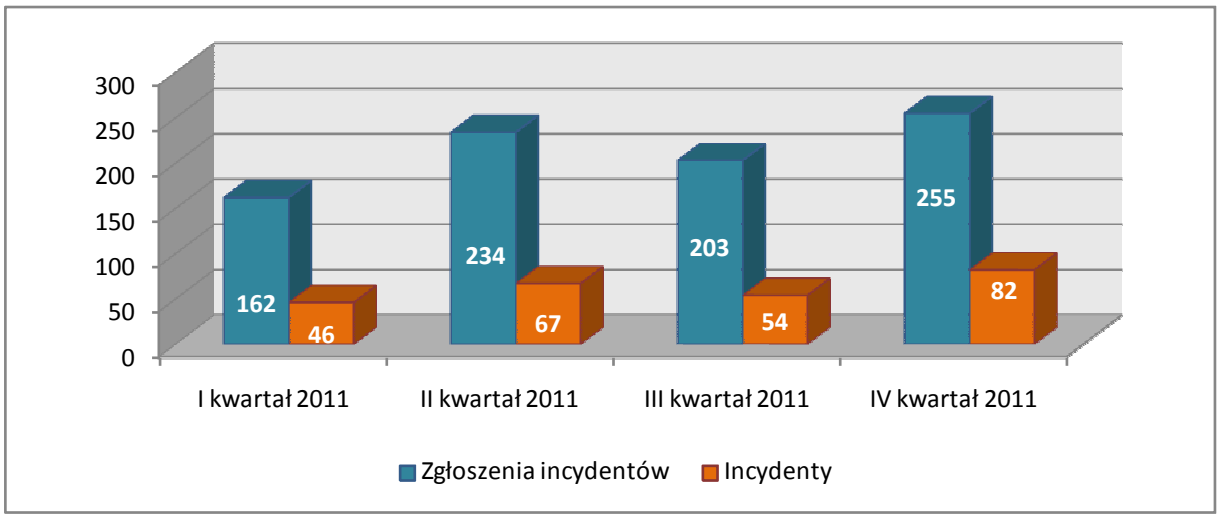
Rysunek 5 - Źródła zgłoszeń incydentów

Rozkład miesięczny incydentów zarejestrowanych oraz incydentów, które zostały rozwiązane, przedstawia się następująco: w październiku 2011 zarejestrowano 27 incydentów, rozwiązanych natomiast zostało 10, w listopadzie 2011 odnotowano 38 incydentów, z czego 30 zostało rozwiązano. W grudniu natomiast przyjęto do realizacji 17 incydentów, z czego 9 jeszcze w tym samym miesiącu zostało zakończonych. Pozostałe incydenty są w trakcie dalszej analizy.



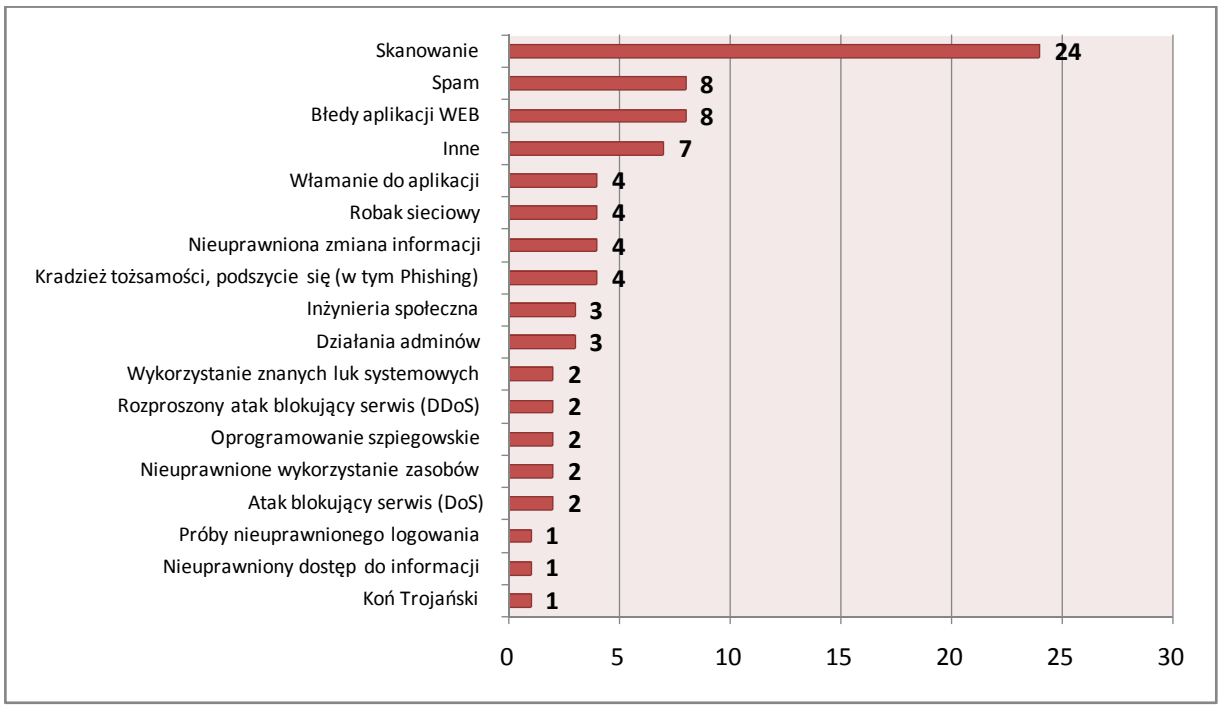
Rysunek 6 - Porównanie liczby incydentów otwartych i zamkniętych w poszczególnych miesiącach czwartego kwartału

Poniższy wykres obrazuje porównanie ilości zgłoszeń na tle faktycznych incydentów kwartalnie na przestrzeni całego 2011 roku. Na uwagę zasługuje fakt, że w ostatnim kwartale relatywnie wrosła ilość zgłoszeń incydentów. Wynika to z faktu zaimplementowania nowych własnych mechanizmów automatycznego powiadamiania o nieprawidłowościach w sieciach administracji publicznej. Ma to również swoje potwierdzenie w wykresie przedstawiającym szczegółowe statystyki źródeł zgłoszeń incydentów trafiających do CERT.GOV.PL (Rys. 5), który pokazuje blisko 51 procent-owy udział zgłoszeń własnych za ostatni kwartał 2011 roku.



Rysunek 7 - Porównanie ilości zgłoszeń incydentów i incydentów w ostatnich czterech kwartałach

Podział zarejestrowanych incydentów na kategorie przedstawia się następująco:



Rysunek 8 - Statystyka incydentów z podziałem na kategorie

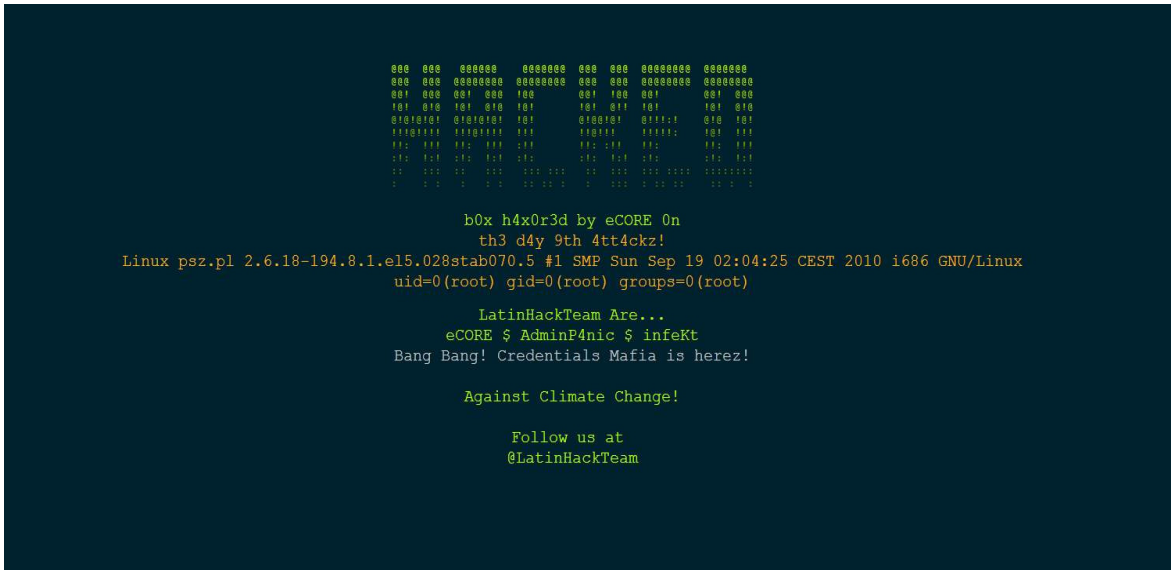
Analizując powyższy wykres, można stwierdzić, że zdecydowaną większość obsługiwanych incydentów stanowią tradycyjne skanowania w poszukiwaniu usług. „Popularne" są jak zwykle błędy w aplikacjach WEB, czy wiadomości typu SPAM.

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

- w październiku odnotowano fakt wykorzystywania błędnie skonfigurowanego forum jednej z witryn administracji publicznej, do umieszczania odnośników do stron zawierającymi treści pornograficzne, reklamujące nielegalne środki farmakologiczne,

ale również wykorzystywane do pozycjonowania stron WWW. Poinformowano administratora forum w wyniku czego wprowadzono poprawki konfiguracyjne dla serwera hostującego serwis forum;

- początek października, to również atak ukierunkowany na jedno z ministerstw, w którym wykorzystano masową wysyłkę wiadomości mailowych wraz z załączonym złośliwym plikiem .pdf. Przedmiotowy załącznik zawierał złośliwe oprogramowania, które po uruchomieniu na podatnej maszynie, wykonywało połączenia z jednym z państw afrykańskich. Sama wiadomość została wysłana z państwa europejskiego;
- w październiku miała miejsce podmiana zawartości strony głównej witryny należącej do jednego z resortów;



Rysunek 9 - Przykład podmienionej strony

- w październiku także wystąpił rozproszony atak odmowy usługi na Krajowe Biuro Wyborcze. Źródłem ataku były głównie adresy IP przypisane do Rumunii i Polski. Poinformowane zostały zespoły abuse właściwych dostawców telekomunikacyjnych;
- w październiku pojawiła się także strona o nazwie korespondującej wizualnie do domeny jednego z ministerstw. Strona została zablokowana i usunięta z serwera;
- w październiku doszło do podmiany strony jednego z urzędów pracy. Przełamujący wykorzystali technikę „SQL injection" i uzyskali w ten sposób dane kont użytkowników w postaci nazw kont i haseł. Błąd spowodowany był brakiem walidacji danych w zapytaniach SQL. Powodem tego było m.in. użytkowanie starszej wersji CMS-a na serwer www. Zalecenia przekazane zostały administratorowi strony;

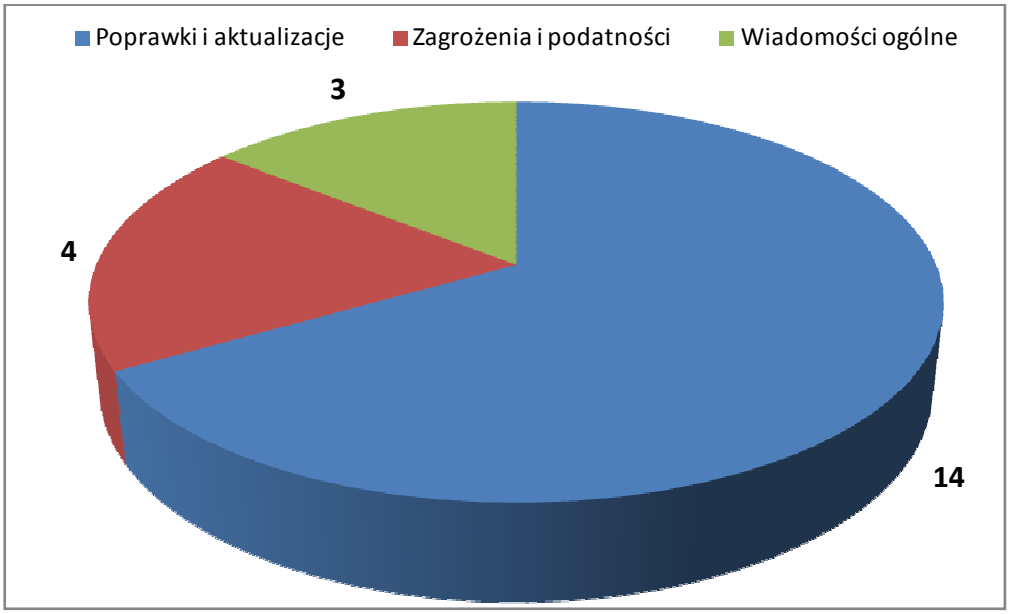
- w listopadzie notowano wzrost incydentów związanych z atakami typu *brute-force* na popularne usługi, takie jak *ssh*, bądź *ftp*. Kraje, skąd miały miejsce wspomniane próby to m.in.: Brazylia, Ukraina, czy Federacja Rosyjska;
- w listopadzie pojawiła się strona podszywająca się pod jedną z instytucji, która przekierowywała w swojej ramce do autentycznej strony instytucji. Stronę zablokowano;
- ponadto w listopadzie zarejestrowano także kilka nieautoryzowanych podmian zawartości strony głównej podmiotów administracji publicznej;
- grudzień to przede wszystkim odnotowany wzrost ilości wysłanych maili wyłudzających dane do logowania oraz maili phishingowych różnych instytucji finansowych, a które trafiały do użytkowników sektora publicznego. Nadal ujawniane były incydenty związane z przeprowadzaniem tzw. „targeted attacks" polegających na wysyłaniu poczty email ze z złośliwymi załącznikami PDF zawierającymi skrypty Java Script. Po uruchomieniu pliku PDF z włączona obsługą Java Script dochodziło do utworzenia lokalnych plików na komputerze użytkownika oraz uruchomienia procesów, które otwierały połączenia sieciowe na inne adresy IP. Przez popularne silniki antywirusowe załączniki wykrywane były jako exploit, co oznaczało, że nie były to bardzo zaawansowane mechanizmy infekcji użytkowników. Email-e zostały poddane kwarantannie i po analizie usunięte;
- dominowały także zgłoszenia dotyczące przełamywania zabezpieczeń stron internetowych instytucji i podmieniania zawartości w postaci plików ze zdjęciem albo podmiany treści strony za pomocą np. umieszczania w kodzie źródłowym strony skryptów Java Scripts;

4. Istotne podatności, zagrożenia i biuletyny zabezpieczeń

Witryna http://www.cert.gov.pl stanowi źródło specjalistycznych danych związanych z bezpieczeństwem teleinformatycznym. Publikowane są tam między innymi aktualne informacje o istotnych zagrożeniach, nowych podatnościach w popularnych systemach i aplikacjach, najpopularniejszych formach ataków sieciowych oraz sposobach ochrony. Dodatkowo na powyższej witrynie umieszczane są biuletyny bezpieczeństwa udostępnione przez producentów sprzętu i oprogramowania.

W czwartym kwartale 2011 roku na witrynie www.cert.gov.pl umieszczono:

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



Rysunek 10 - Statystyka publikacji na stronie CERT.GOV.PL w IV kwartale 2011 roku

Najistotniejsze publikacje dotyczące zagrożeń w czwartym kwartale 2011 roku:

- **Microsoft Security Bulletin październik 2011**

Firma Microsoft opublikowała październikowy biuletyn bezpieczeństwa, w którym poinformowała o usunięciu ośmiu błędów w swoich produktach. Dwie aktualizacje posiadają status "krytycznych", pozostałe sześć zostało sklasyfikowane jako "ważne".

Biuletyny określone jako "krytyczne":

- MS11-078 - biuletyn dotyczy podatności w aplikacjach .NET Framework oraz Silverlight;

- MS11-081 - biuletyn usuwa osiem luk w zabezpieczeniach przeglądarki Internet Explorer.

Biuletyny określone jako "ważne":

- MS11-075 - biuletyn dotyczy podatności w Microsoft Active Accessibility;

- MS11-076 - biuletyn dotyczy podatności w aplikacji Windows Media Center;

- MS11-077 - biuletyn dotyczy czterech podatności w systemie Microsoft Windows. Najpoważniejsza z tych luk może pozwolić na zdalne wykonanie kodu, pod warunkiem, że użytkownik otworzy specjalnie spreparowany plik czcionki (.fon) w udziale sieciowym, lokalizacji UNC lub WebDAV, lub jako załącznik poczty e-mail;

- MS11-079 - biuletyn dotyczy pięciu podatności w Forefront Unified Access Gateway;

- MS11-080 – biuletyn dotyczy podatności w Microsoft Windows Ancillary Function Driver (AFD);

- MS11-082 – biuletyn dotyczy podatności w Host Integration Server.

- **Zbiór aktualizacji bezpieczeństwa Apple**

Firma Apple wydała zbiór aktualizacji bezpieczeństwa dla produktów: Apple iOS, Safari 5.1.1, OS X Lion v10.7.2, iWork 09 oraz Apple TV 4.4. Aktualizacje usuwają wiele luk w zabezpieczeniach, których wykorzystanie mogłoby pozwolić atakującemu na wykonanie dowolnego kodu, przeprowadzenie ataku typu odmowa usługi (denial-of-service), uzyskanie poufnych informacji lub obejście wymogów bezpieczeństwa.

- **Zbiór krytycznych aktualizacji ORACLE**

Firma Oracle wydała dwa zbiory krytycznych aktualizacji dla produktów oznaczonych jako Oracle Critical Patch Update Advisory - October 2011 oraz Oracle Java SE Critical Patch Update Advisory – October 2011.

Lista poprawek dotyczy: 5 poprawek dla Oracle Database Server, 10 poprawek dla Oracle Fusion Middleware, 5 poprawek dla Oracle E-Business Suite, 1 poprawki dla Oracle Supply Chain Products Suite, 7 poprawek dla Oracle PeopleSoft Products, 3 poprawek dla Oracle Siebel Suite, 2 poprawek dla Oracle Industry Applications, 22 poprawek dla Oracle Sun Products Suite, 1 poprawki dla Oracle Linux, 1 poprawki dla Oracle Virtualization oraz 20 poprawek dla Oracle Java SE.

- **Aktualizacje Cisco**

Firma Cisco wydała sześć aktualizacji usuwających błędy w produktach CiscoWorks Common Services, Cisco Show and Share, Cisco Unified Contact Center, Cisco WebEx Player, Cisco Security Agent oraz Cisco Unified Communication Manager. Wykryte luki umożliwiały atakującemu wykonanie dowolnego kodu lub wykradzenie poufnych informacji.

- **Microsoft Security Bulletin Listopad 2011**

Firma Microsoft opublikowała listopadowy biuletyn bezpieczeństwa, w którym usunięte zostały cztery błędy. Jedna aktualizacja posiada status „krytyczny", dwie kolejne zostały sklasyfikowane jako „ważne", natomiast ostatnia została określona jako "umiarkowana".

Podatności uznane jako „krytyczne":

- MS11-083 - luka ta może pozwolić na zdalne wykonanie kodu, gdy atakujący będzie wysyłać na zamknięty port systemu docelowego ciągły strumień specjalnie spreparowanych pakietów UDP.

Podatności uznane jako „ważne":

- MS11-085 - podatność umożliwia zdalne wykonanie kodu, w sytuacji gdy użytkownik uruchomi plik (np. .eml lub .wcinv), znajdujący się w tym samym katalogu sieciowym, co specjalnie spreparowany plik biblioteki dołączanej dynamicznie (DLL) oraz odwiedzi niezaufaną zdalną lokalizację systemu plików lub udział WebDAV;

- MS11-086 - dotyczy błędów w zabezpieczeniach usługi Active Directory. Aktualizacja zabezpieczeń pozwala usunąć usterki w usłudze Active Directory, Active Directory Application Mode oraz Active Directory Lightweight Directory Service.

Podatności uznane jako „umiarkowane":

- MS11-084 - aktualizacja zabezpieczeń usuwa usterki wykryte w jądrze systemu Windows.

- **Microsoft Security Bulletin Grudzień 2011**

Firma Microsoft opublikowała grudniowy biuletyn bezpieczeństwa, który objął czternaście aktualizacji, z których trzy określono jako „krytyczne", natomiast pozostałe zostały sklasyfikowane jako „ważne".

Podatności uznane jako „krytyczne":

- MS11-087 – aktualizacja dotycząca podatności w Windows Kernel-Mode Drivers;

- MS11-090 – zbiorcza aktualizacja dotycząca ActiveX;
- MS11-092 – aktualizacja dotycząca podatności w Windows Media Player i Windows Media Center.

Podatności uznane jako „ważne”:

- MS11-088 – aktualizacja dotycząca podatności Microsoft Office IME;
- MS11-089 – aktualizacja dotycząca podatności Microsoft Office;
- MS11-091 – aktualizacja dotycząca podatności Microsoft Publisher;
- MS11-093 – aktualizacja dotycząca podatności w Object Linking and Embedding;
- MS11-094 – aktualizacja dotycząca podatności Microsoft PowerPoint;
- MS11-095 – aktualizacja dotycząca podatności Active Directory, Active Directory Application Mode i Active Directory Lightweight Directory Service;
- MS11-096 – aktualizacja dotycząca podatności Microsoft Excel;
- MS11-097 – aktualizacja dotycząca podatności klient - serwer run-time;
- MS11-098 – aktualizacja dotycząca podatności Windows Kernel;
- MS11-099 – zbiorcza aktualizacja dotycząca Internet Explorer.

- **Microsoft .NET Framework**

Firma Microsoft opublikowała biuletyn bezpieczeństwa MS11-100, w którym poinformowała o wykryciu luk w zabezpieczeniach Microsoft .NET Framework.

Najpoważniejsza z wykrytych podatności może pozwolić na podniesienie uprawnień poprzez wysłanie odpowiednio przygotowanego żądania skierowanego do atakowanej strony. Wykorzystując tę lukę atakujący może wykonać dowolne czynności w kontekście istniejącego konta między innymi wykonać dowolne polecenie. W celu przeprowadzenia ataku napastnik musi zarejestrować konto na stronie ASP.NET oraz musi znać nazwę istniejącego użytkownika. Wykryte błędy są oznaczone jako krytyczne dla poniższych wersji Microsoft .NET Framework w wersjach: 1.1 Service Pack 1, 2.0 Service Pack 2, 3.5 Service Pack 1, 3.5.1 oraz 4.

- **Podatności FreeBSD**

W popularnym systemie operacyjnym FreeBSD wykryte zostały następujące podatności:

- błąd w Pluggable Authentication Modules i Pluggable Authentication Modules Secure Shell;
- luka w wirtualnym terminalu protokołu telnetd demon;
- podatność w systemowym wywołaniu chroot;
- błąd w oprogramowaniu BIND (Berkeley Internet Name Domain).

- **Biuletyn Adobe**

Firma Adobe opublikowała nowy biuletyn bezpieczeństwa dotyczący produktów Adobe Reader i Adobe Acrobat. Wykryto podatności zezwalające atakującemu na przeprowadzenie ataku typu Denial-of-Service lub przejęcie kontroli nad zaatakowanym systemem. Użycie trybu Protected Mode w programie Adobe Reader X oraz Protected View w Adobe Acrobat uniemożliwia wykorzystanie tej luki.

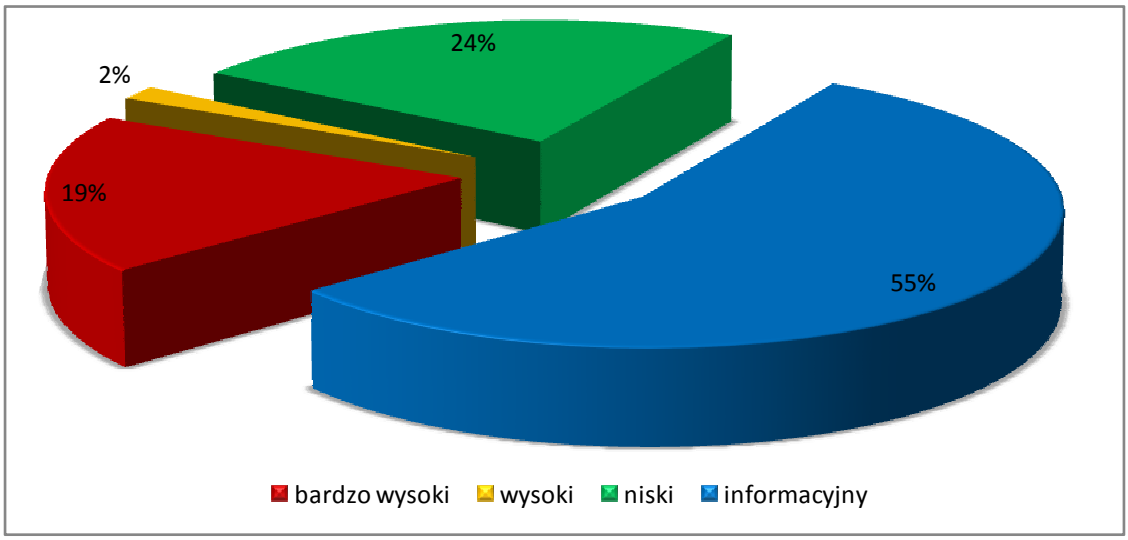
Podatne wersje oprogramowania:

- Adobe Reader X/Acrobat X w wersji 10.1.1 i wcześniejsze wersje dla systemów Windows i Macintosh;
- Adobe Reader/Acrobat w wersji 9.4.6 i wcześniejsze wersje dla systemów Windows, Macintosh i UNIX.

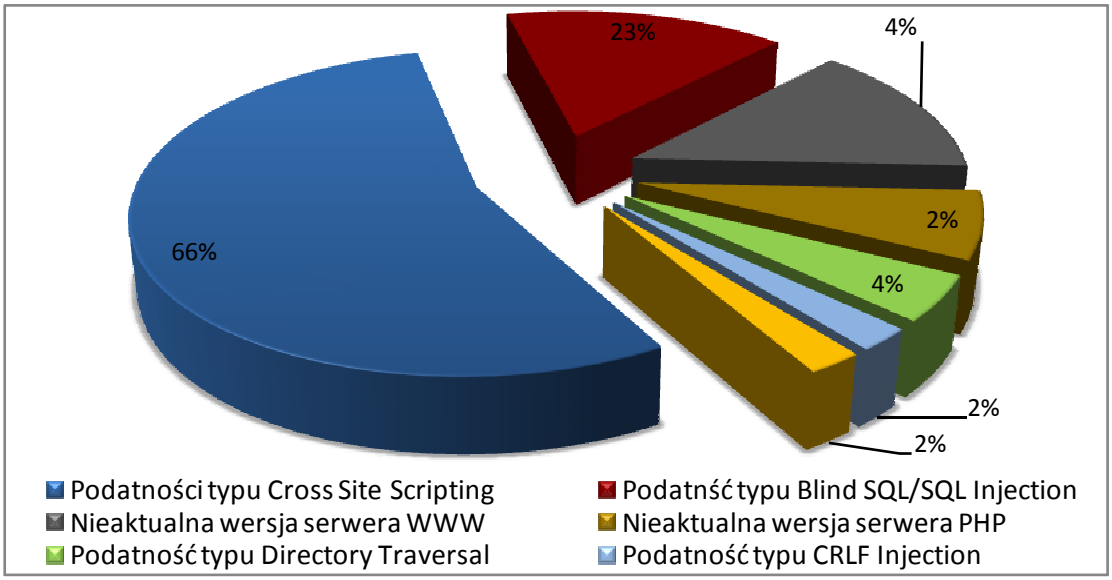
5. Testy bezpieczeństwa witryn WWW instytucji państwowych

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

W IV kwartale 2011 roku przebadano 19 witryn należących do 6 instytucji państwowych. Stwierdzono ogółem 241 błędów w tym: 45 błędów o bardzo wysokim poziomie zagrożenia, 4 błędy o wysokim poziomie zagrożenia, 58 błędów o niskim poziomie zagrożenia i 134 błędy oznaczone jako informacyjne.

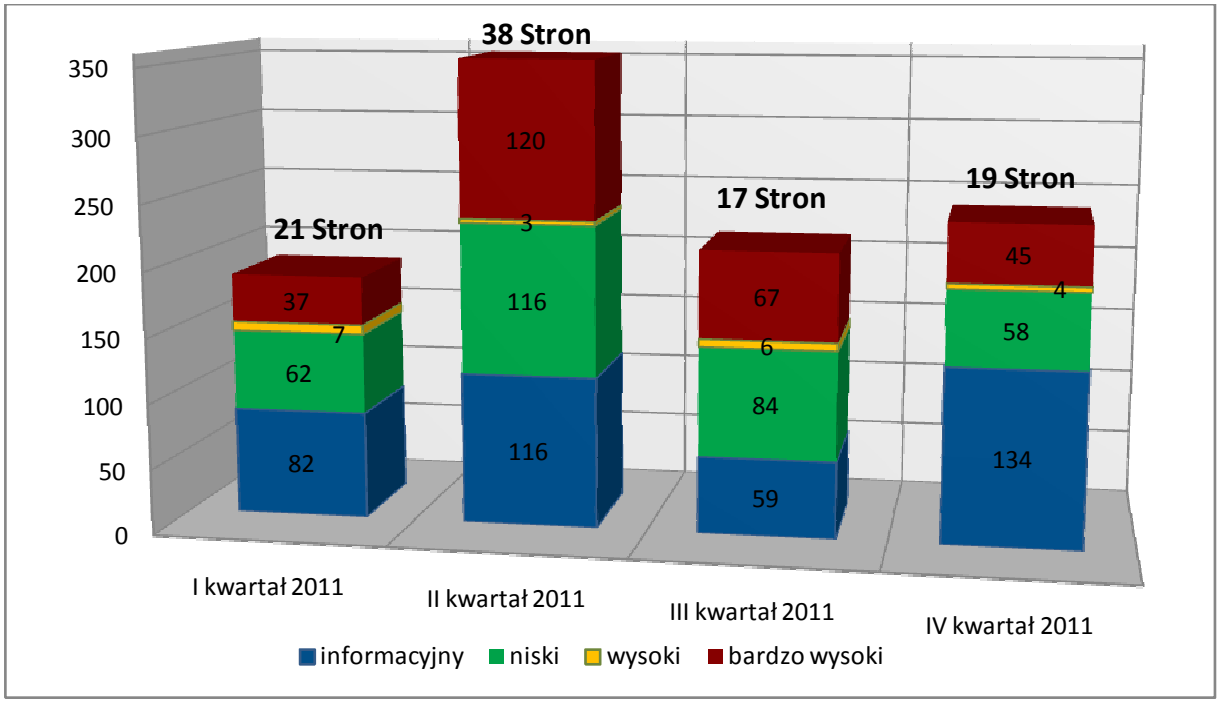


Rysunek 11 - Statystyka wykrytych podatności w rządowych witrynach WWW według poziomu zagrożenia



Rysunek 12 - Procentowy rozkład najpoważniejszych błędów

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



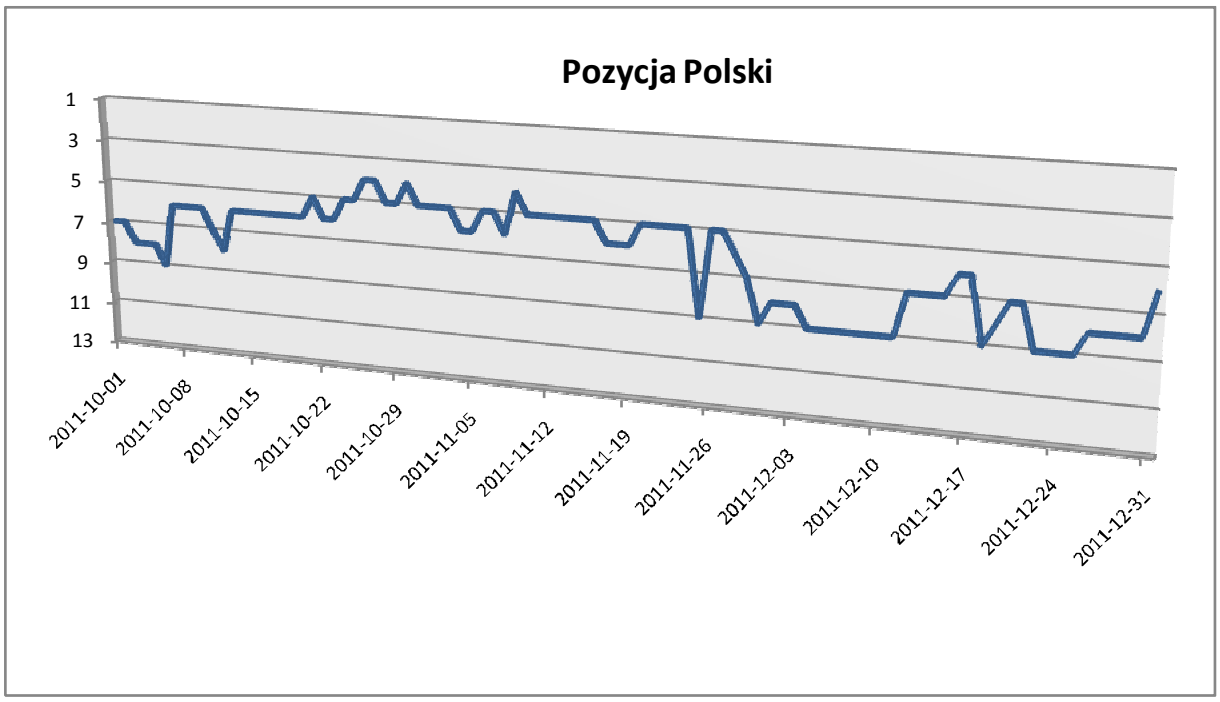
Rysunek 13 - Liczbowy rozkład podatności przeskanowanych witryn z podziałem na istotność błędów w poszczególnych kwartałach.

6. Informacje z systemów zewnętrznych

6.1. System ATLAS

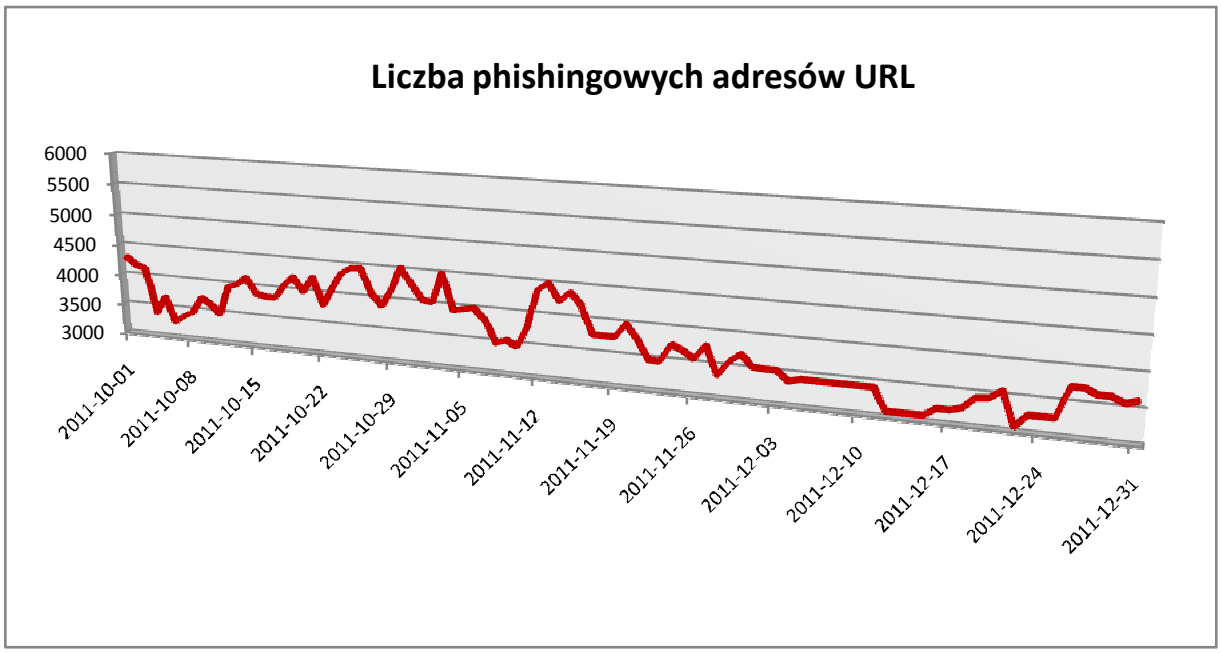
System ATLAS[7] gromadzi istotne informacje na temat zagrożeń teleinformatycznych w sieci Internet i agreguje je pod względem m.in. klas adresowych poszczególnych państw oraz poszczególnych typów niebezpieczeństw. Na podstawie tych danych każdemu z krajów przydzielane jest miejsce w statystyce pokazującej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

W czwartym kwartale 2011 roku Polska zajmowała nadal stosunkowo niską siódmą pozycję w statystykach aby pod koniec kwartału spaść w rankingu nawet na dziewiąte miejsce. Pozycja Polski w rankingu uwarunkowana jest w dużej mierze liczbą adresów phishingowych URL, która początkowo oscylowała pomiędzy wartościami 3000 - 4500 aby pod koniec czwartego kwartału spać na poziom zawarty pomiędzy 3000 – 4000.



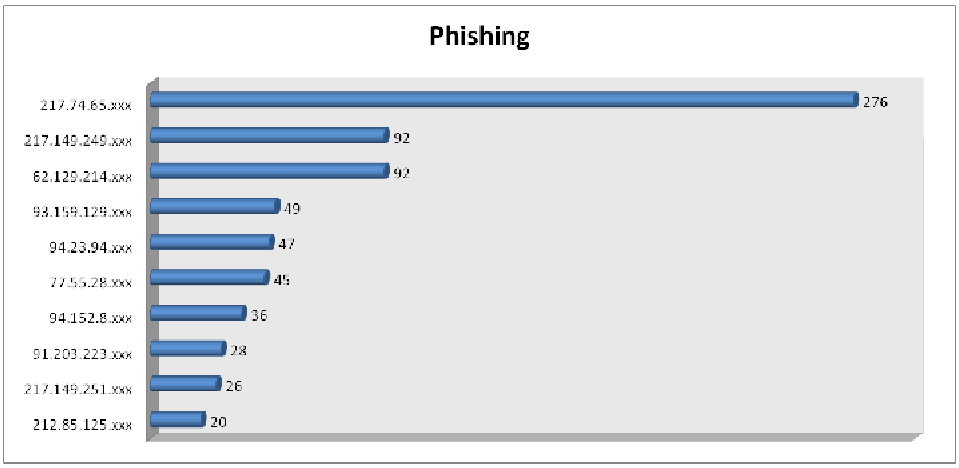
Rysunek 14 - Pozycja Polski w rankingu ATLAS

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

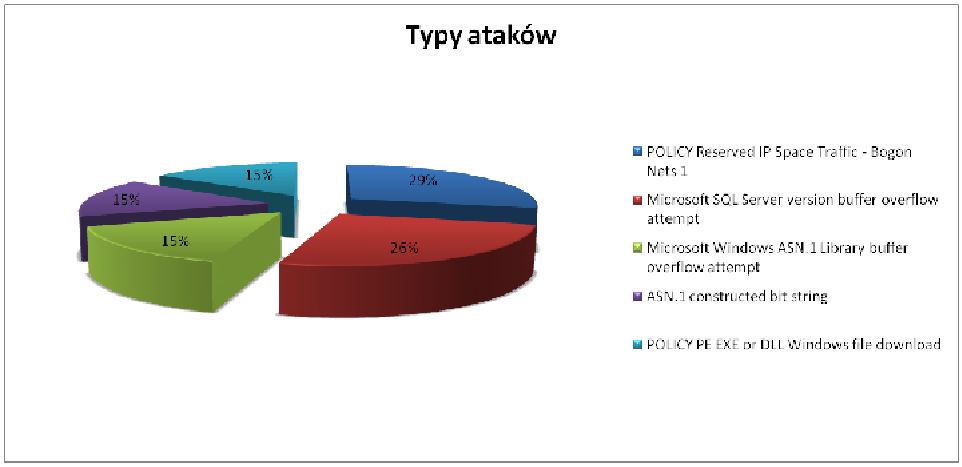


Rysunek 15 - Liczba phishingowych adresów URL wg ATLAS

Liczba phishingowych adresów URL odnotowanych przez system Atlas w polskiej cyberprzestrzeni pozostaje dalej znaczna i wynika z penetracji źle zabezpieczonych serwerów WWW umożliwiając propagację i parkowanie „złych" domen zagnieżdżonych w strukturze strony bez zmiany jej zawartości.



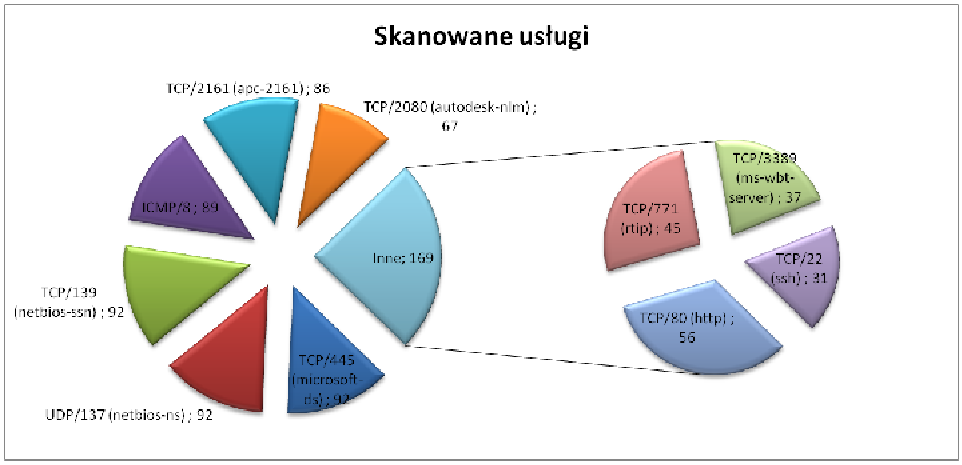
Rysunek 16 - Statystyki phishingu wg systemu Atlas – w czwartym kwartale 2011r. (ilości wystąpień najbardziej aktywnych hostów lub ich sumy dla wystąpień w ramach jednej podsieci)



Rysunek 17 - Statystyki ataków wg systemu Atlas (IV kwartał 2011r.)

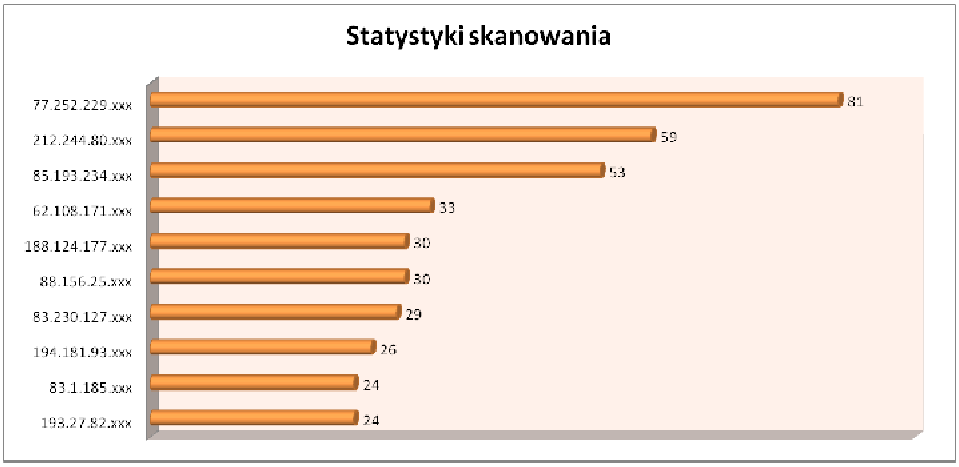
Pięć najczęściej występujących typów ataków wg systemu ATLAS – w czwartym kwartale 2011r. (udział procentowy liczony tylko dla tych usług)

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



Rysunek 19 - Statystyki skanowania wg systemu Atlas (IV kwartał 2011r.)

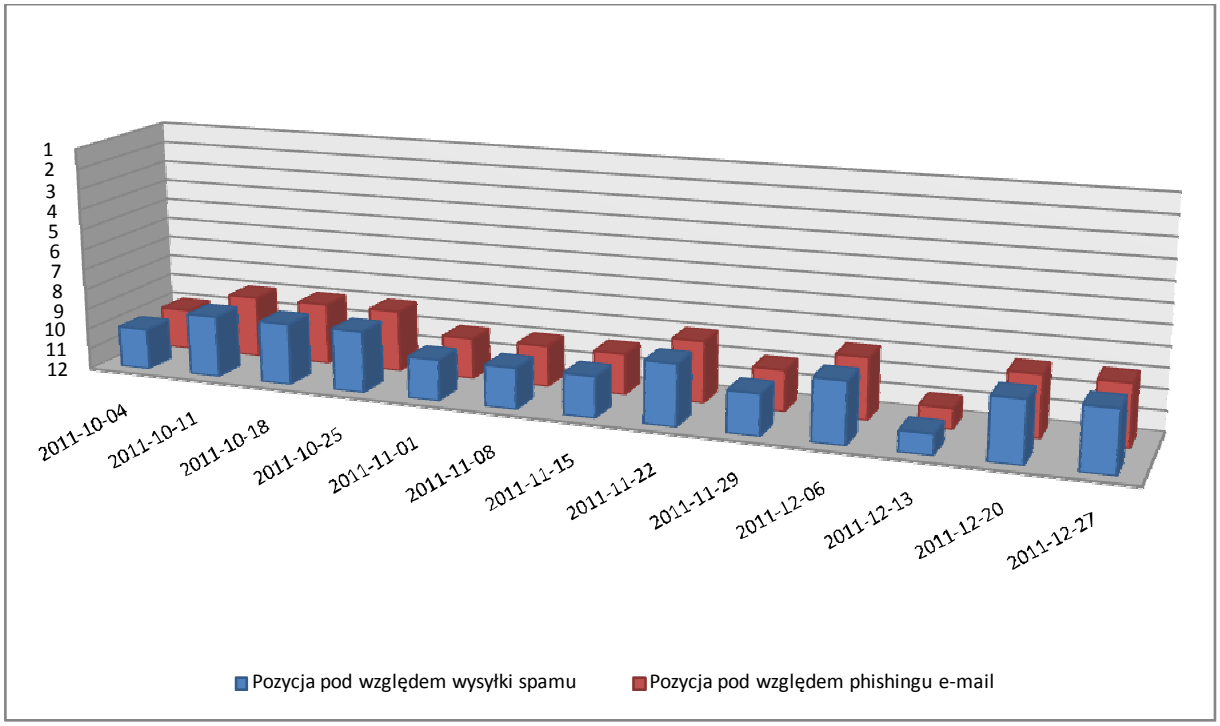
Najczęściej skanowane porty/usługi wg systemu ATLAS – w czwartym kwartale 2011r. – odnotowane ilości wystąpień



Rysunek 20 - Najbardziej aktywne hosty w Polsce wg systemu ATLAS – w czwartym kwartale 2011r. (ilości wystąpień lub ich sumy dla hostów w jednej podsieci)

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

Polska, podobnie jak w poprzednich kwartałach, nadal utrzymuje się w dolnych częściach statystyki krajów, zarówno pod względem przesyłek phishingowych jak i ilości wysyłanego spamu.

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

7. Inne działania CERT.GOV.PL

7.1. Ocena zagrożeń występujących w czwartym kwartale 2011 roku

Charakteryzując incydenty, które miały miejsce w czwartym kwartale 2011 roku należy zwrócić uwagę na:

- powtarzające się akcje spamowe zawierające przesyłki email z załącznikami PDF, doc, itp. z malware o różnym stopniu zaawansowania technicznego najczęściej wykrywane i blokowane przez silniki antywirusowe albo stanowiące nierzadko malware typu „zero-day";
- włamania na strony internetowe słabo zabezpieczone funkcjonujące w oparciu o nieaktualizowane wersje CMS-ów oraz z domyślnymi ustawieniami serwera WWW lub napisane w sposób niegwarantujący właściwej walidacji danych przetwarzanych przez serwer;
- przeprowadzanie ataków typu „brute force" skierowanych na usługi SSH, FTP lub skierowanych na aktywne panele administracyjne do CMS-ów stron WWW;
- liczne skanowania portów TCP/UDP testujących występowanie usług, które mogą być przedmiotem potencjalnego ataku;

Zagrożenia stwarzane przez tego typu incydenty prowadzą do naruszania bezpieczeństwa w zakresie dostępności i integralności zasobów instytucji i są typowe dla usług udostępnianych w sieci Internet.

7.2. International Cyber Defense Workshop

Rządowy Zespoł Reagowania na Incydenty Komputerowe CERT.GOV.PL po raz kolejny wziął udział w międzynarodowych warsztatach International Cyber Defense Workshop. Warsztaty składały się zarówno z wykładów jak i ćwiczeń praktycznych, a ich celem było zaznajomienie uczestników z aktualnymi trendami m.in. w zakresie najnowszych metod i sposobów stosowanych przez cyberprzestępców. Głównym celem warsztatów była przede wszystkim tematyka związana z właściwym reagowaniem

na zagrożenia ukierunkowane, z uwzględnieniem m.in. systemów SCADA oraz analiza powłamaniowa.

Ponadto, w świetle zagrożeń wynikających bardzo często z błędnej konfiguracji urządzeń brzegowych, przedstawione zostały techniki właściwej konfiguracji jak również odpowiedniej implementacji systemów służących do wykrywania włamań.

7.3. Cyber Coalition

W czwartym kwartale zespół CERT.GOV.PL wziął udział w międzynarodowych ćwiczeniach NATO Cyber Coalition testujących zdolność obrony przed cyberatakami. Głównymi symulowanymi celami była infrastruktura krytyczna kraju.

Ćwiczenia Cyber Coalition skoncentrowane są w głównej mierze na praktycznych działaniach w przypadku serii międzynarodowych incydentów teleinformatycznych skierowanych przeciwko krytycznej infrastrukturze państw NATO. Zadaniem zaangażowanych w ćwiczenia zespołów bezpieczeństwa jest nie tylko reagowanie i zarządzanie incydentami, lecz również wykrycie „modus operandi" sprawców, jak również źródła pochodzenia ich aktywności. Osiągnięcie tak postawionych zadań możliwe jest za pośrednictwem współpracy międzynarodowej umożliwiającej przeprowadzenie wspólnie analizy powłamaniowej czy analizy typu „live forensics" związanych z rejestrowanym incydentami.

Ćwiczenia Cyber Coalition są intensywnym sprawdzianem gotowości zespołów bezpieczeństwa do kompleksowego odparcia ataków na krytyczną infrastrukturę teleinformatyczną kraju.