Raport o stanie bezpieczeństwa cyberprzestrzeni RP w 2011 roku

Warszawa 2012

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.

CERT.GOV.PL, dane kontaktowe:

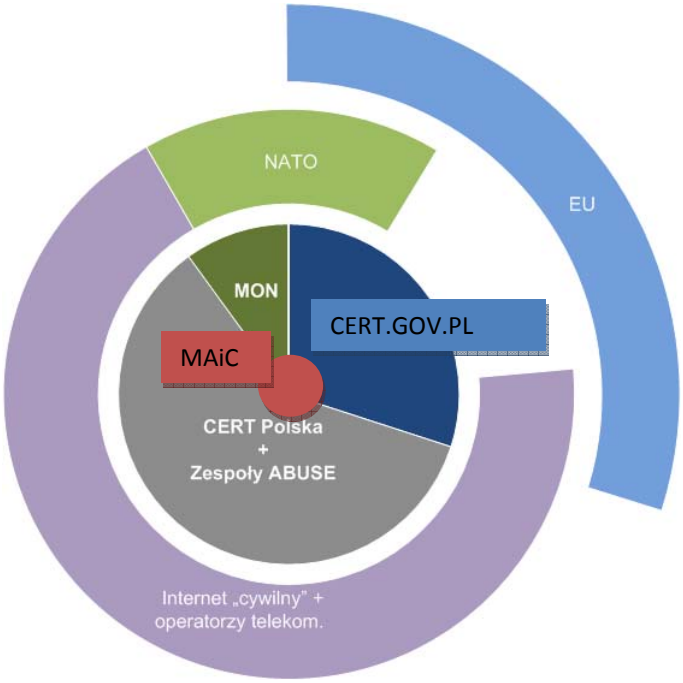
www.cert.gov.pl
cert@cert.gov.pl
Telefony:
+48 22 58 58 844
+48 22 58 56 176
Fax:
+48 22 58 56 099

CERT.GOV.PL
Departament Bezpieczeństwa Teleinformatycznego
Agencja Bezpieczeństwa Wewnętrznego
ul. Rakowiecka 2A
00-993 Warszawa
Polska

Spis treści

1. Wstęp

Rządowy Zespół Reagowania na Incydenty Komputerowe CERT.GOV.PL jest podmiotem właściwym w zakresie realizacji zadań związanych z bezpieczeństwem cyberprzestrzeni RP, w obszarze administracji publicznej a także wspierającym w sferze cywilnym i wojskowej. Na poziomie strategicznym współpracuje z wiodącym w sferze rozwoju e-administracji o e-społeczeństwa Ministerstwem Administracji i Cyfryzacji.



Obszary współpracy w zakresie bezpieczeństwa w cyberprzestrzeni

Pełni szczególną rolę w realizacji zapisów projektowanej Polityki Bezpieczeństwa Cyberprzestrzeni RP, która wyewoluowała z Rządowego Programu Bezpieczeństwa Cyberprzestrzeni RP na lata 2011-2020. Cele strategiczne Polityki w dalszym ciągu obejmują:

- zwiększenie poziomu bezpieczeństwa infrastruktury teleinformatycznej Państwa;
- zwiększenie zdolności do zapobiegania i zwalczania zagrożeń ze strony cyberprzestrzeni;
- zmniejszenie skutków incydentów godzących w bezpieczeństwo teleinformatyczne;
- określenie kompetencji podmiotów odpowiedzialnych za bezpieczeństwo cyberprzestrzeni;

- stworzenie i realizację spójnego dla wszystkich podmiotów administracji publicznej systemu zarządzania bezpieczeństwem cyberprzestrzeni oraz ustanowienie wytycznych w tym zakresie dla podmiotów niepublicznych;
- stworzenie trwałego systemu koordynacji i wymiany informacji pomiędzy podmiotami odpowiedzialnymi za bezpieczeństwo cyberprzestrzeni oraz użytkownikami cyberprzestrzeni;
- zwiększenie świadomości użytkowników w zakresie metod i środków bezpieczeństwa w cyberprzestrzeni.

CERT.GOV.PL wykonuje testy bezpieczeństwa witryn dla administracji państwowej od 2008 roku. W mijającym roku testy te cieszyły się dużym zainteresowaniem. W 2011 roku w trakcie działania projektu skanowania witryn internetowych administracji publicznej wykryto ponad 1000 błędów.

CERT.GOV.PL pełnił również rolę komórki doradczej w trakcie uruchamiania projektów teleinformatycznych na cele Przewodnictwa Polski w Radzie Unii Europejskiej w II połowie 2011r.

Niniejszy raport szczegółowo omawia statystyki incydentów zarejestrowanych przez CERT.GOV.PL, w tym system ARAKIS-GOV, czynności przeprowadzonych w celu podniesienia bezpieczeństwa systemów informatycznych Polskiej Prezydencji, testowania bezpieczeństwa witryn, oraz innych inicjatyw, w których Zespół brał udział.

Należy przy tym podkreślić, już na wstępie, iż rok 2011 przyniósł znaczące zmiany w obszarze bezpieczeństwa komputerowego. Ewolucji uległy metodologia wykonywania ataków, w tym stwierdzono znaczne zmiany i rozwój stosowanych rozwiązań technicznych przez atakujących. Należy też odnotować niespotykaną dotąd skalę prób przełamania zabezpieczeń sieci instytucji administracji państwowych, często przy pomocy wysoce zaawansowanych narzędzi tworzonych na potrzeby jednego, konkretnego ataku. Powyższe było m.in. przyczynkiem do zaprezentowania doświadczeń Rządowego Zespołu Reagowania na Incydenty Komputerowe CERT.GOV.PL w sferze rozwiązywania wielu incydentów noszących znamiona szpiegostwa komputerowego w ramach prezentacji własnych doświadczeń, podczas XV konferencji SECURE 2011 w Warszawie.

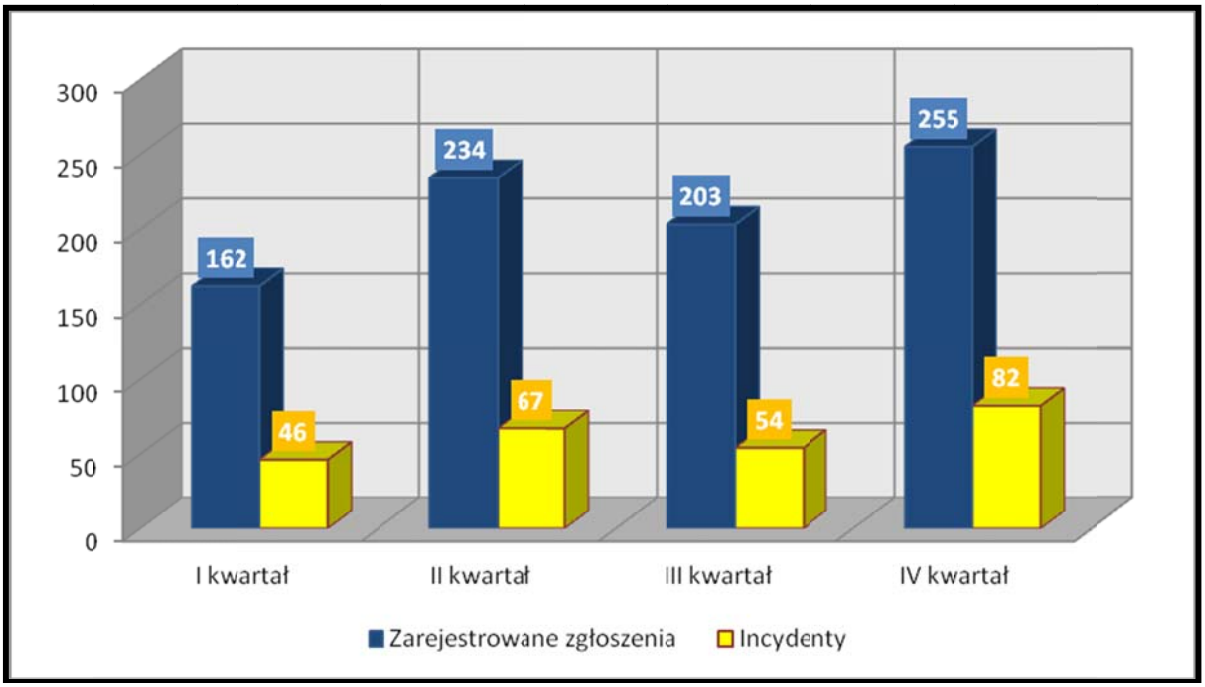
Przedstawiony państwu raport został utrzymany w formie dokumentów z lat poprzednich, a także została nadana mu struktura analogiczna do raportu rocznego CERT POLSKA, tak aby ułatwić dokonywanie analiz i porównań.

Równocześnie dokument, adresowany zarówno do merytorystów jak i decydentów, musi zawierać zarówno zaawansowane informacje techniczne jak i wnioski sformułowane w sposób przejrzysty dla osób podejmujących decyzje strategiczne w instytucjach.

2. Statystyki incydentów koordynowanych przez zespół CERT.GOV.PL w 2011 roku

2.1. Zagrożenia.

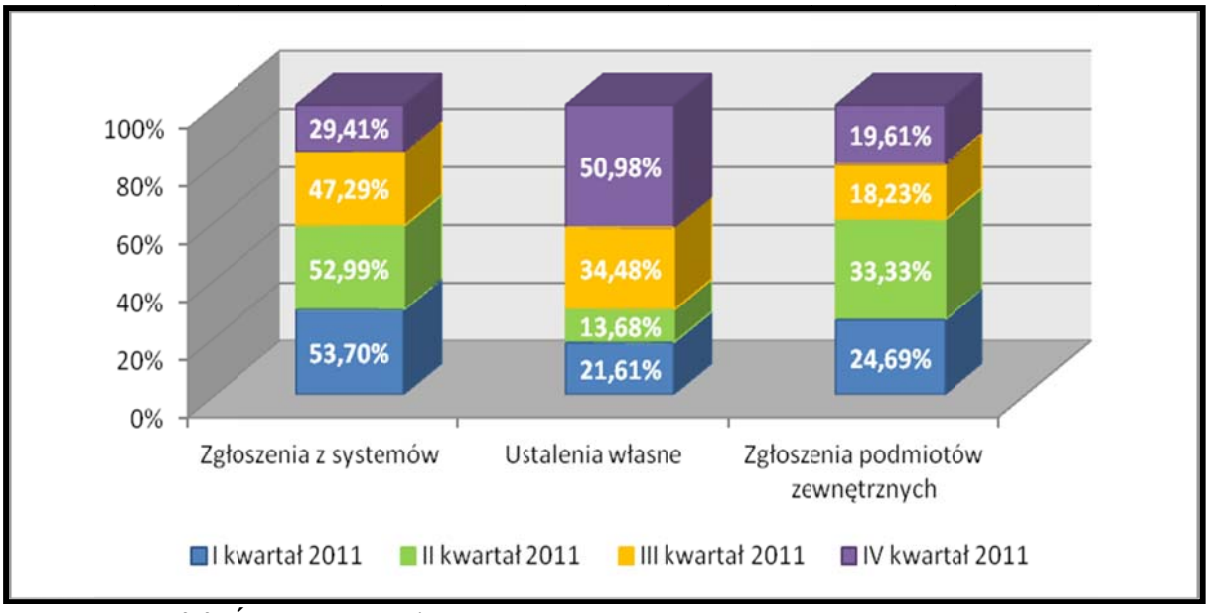
Rok 2011 (w porównaniu do roku 2010) stał pod znakiem nieznacznego wzrostu ilości zgłoszeń odnotowanych przez zespół CERT.GOV.PL. Zarejestrowano 854 zgłoszenia, z których 249 zostało zakwalifikowanych jako faktyczne incydenty.



Rysunek 2-1: Liczba zarejestrowanych oraz faktycznych incydentów w poszczególnych kwartałach 2011 roku

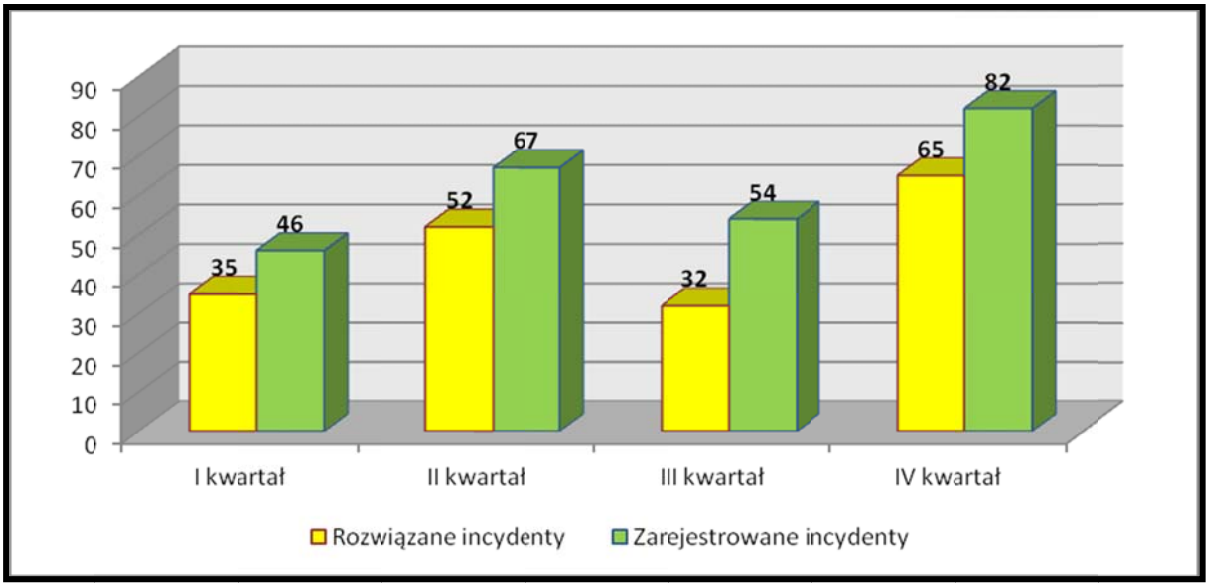
Wyraźna różnica pomiędzy liczbą zarejestrowanych zgłoszeń a liczbą faktycznych incydentów wynika z faktu, że część z nich stanowią tzw. „false-positives". Są to przypadki błędnej interpretacji przez zgłaszającego legalnego ruchu sieciowego. Drugą z przyczyn, szczególnie widoczną w przypadku zgłoszeń z systemów automatycznych, są wielokrotne zgłoszenia dotyczące tych samych incydentów. Ponadto należy tu również zwrócić uwagę na fakt, iż zgłoszenia pochodzące z systemów autonomicznie raportujących, muszą zostać poddane późniejszej ręcznej weryfikacji, i dopiero ona wskazuje na prawdziwość zgłoszenia.

Poniżej umieszczony wykres, przedstawia szczegółowe statystyki źródeł zgłoszeń incydentów trafiających do CERT.GOV.PL.



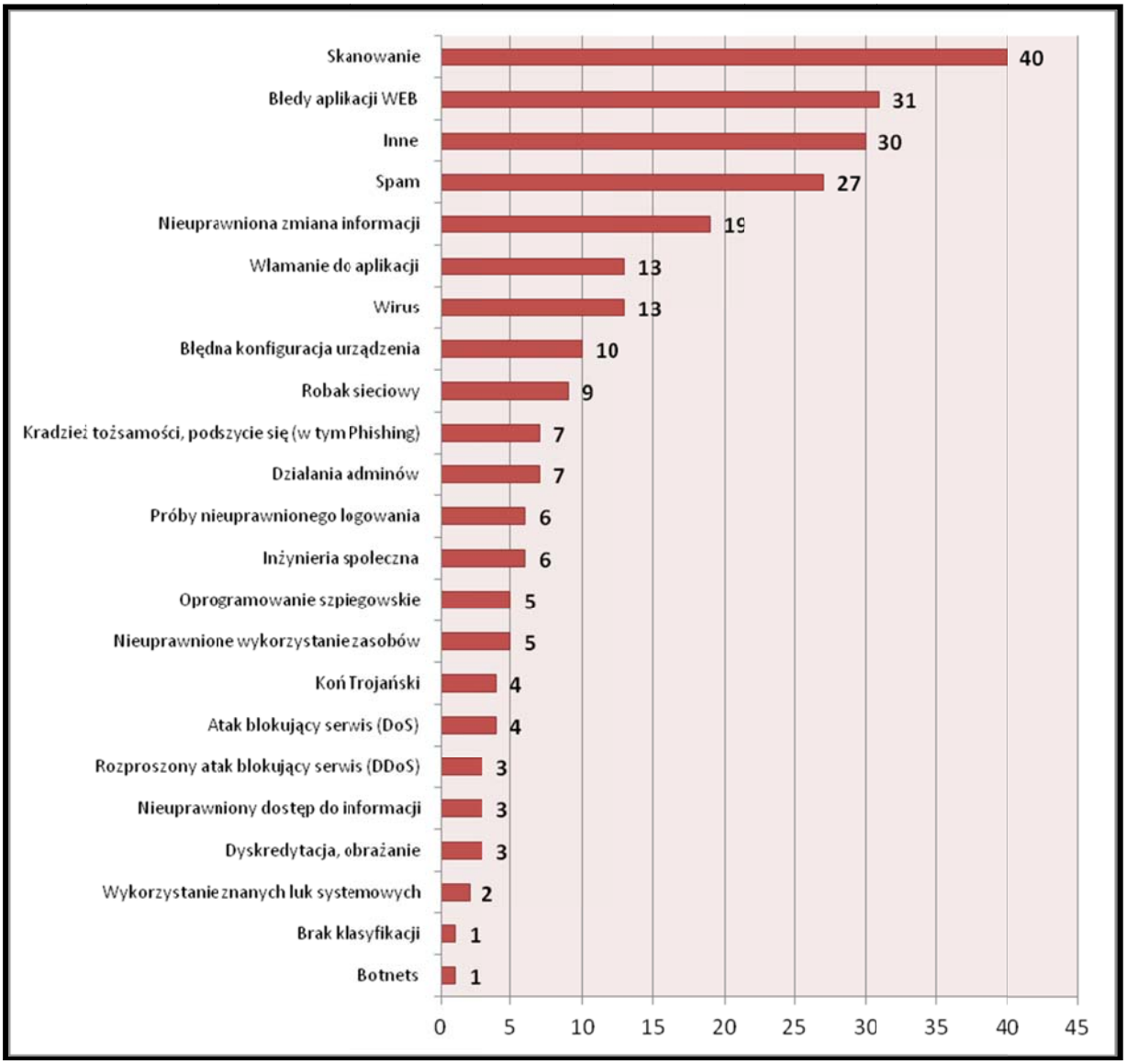
Rysunek 2-2: Źródła zgłoszeń incydentów

Porównanie liczby incydentów zarejestrowanych i zrealizowanych przez zespół CERT.GOV.PL w 2011 roku ilustruje poniższy rysunek.



Rysunek 2-3: Porównanie liczby incydentów zarejestrowanych i zrealizowanych w poszczególnych kwartałach 2011 roku

Podział zarejestrowanych incydentów na poszczególne kategorie przedstawia się następująco:



Rysunek 2-4: Statystyka incydentów za rok 2011 z podziałem na kategorie

Należy podkreślić, że znaczny wzrost liczby zarejestrowanych zgłoszeń, oraz incydentów w 2011 roku wynika z faktu zacieśnienia współpracy z podmiotami zewnętrznymi, jak również wdrożenia dodatkowych autonomicznych narzędzi, które to szerzej informują o nieprawidłowościach w sieciach należących do obszaru zespołu CERT.GOV.PL.

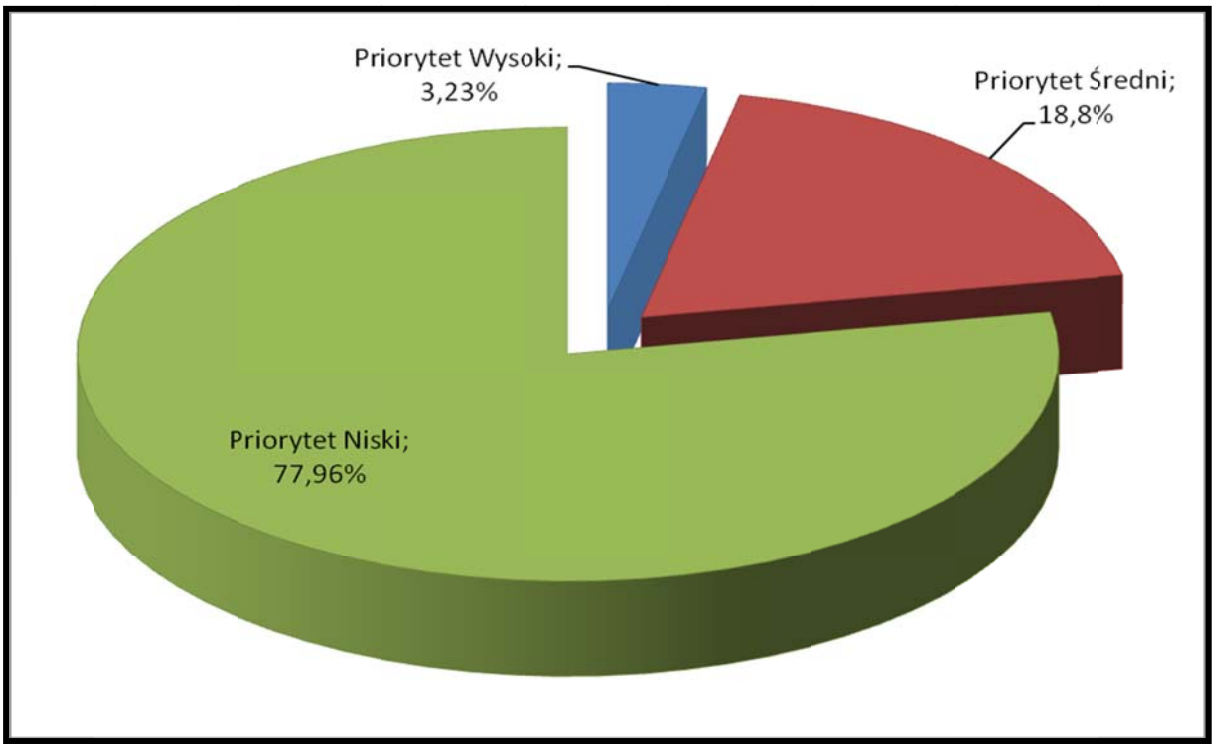
Z punktu widzenia systemów administracji publicznej, niepokojąca jest pozycja trzecia „Inne – 30", świadczy to ciągłym wzroście zdarzeń nietypowych, w tym ataków dedykowanych opartych o podatności zazwyczaj niewykrywalne przez standardowe oprogramowanie i systemy bezpieczeństwa. Wiąże się to m.in. z obserwowanymi na całym

świecie coraz częściej stosowanymi atakami ukierunkowanymi w celu wykradzenia szczególnie cennych informacji przetwarzanych w systemach wewnętrznych. Należy sądzić, iż udział takiego typu ataków będzie rósł w nadchodzącym czasie.

Przypadek sklasyfikowany jako „Botnet" odnosi się do wykrytego klienta botnetu „Coreflood". Był to typowy botnet ukierunkowany na przechwytywanie danych służących do logowania się do banków, a przez to umożliwienie nieupoważnionego dostępu do pieniędzy. Było to realizowane poprzez przechwytywanie znaków, które użytkownik wpisywał na klawiaturze oraz umożliwienie zdalnego dostępu do zarażonego komputera. Należy zwrócić uwagę, iż te same metody mogą służyć do wykradania haseł dostępu do systemów wewnętrznych w instytucji.

2.2. Analiza alarmów w sieci Internet na podstawie systemu ARAKIS-GOV.

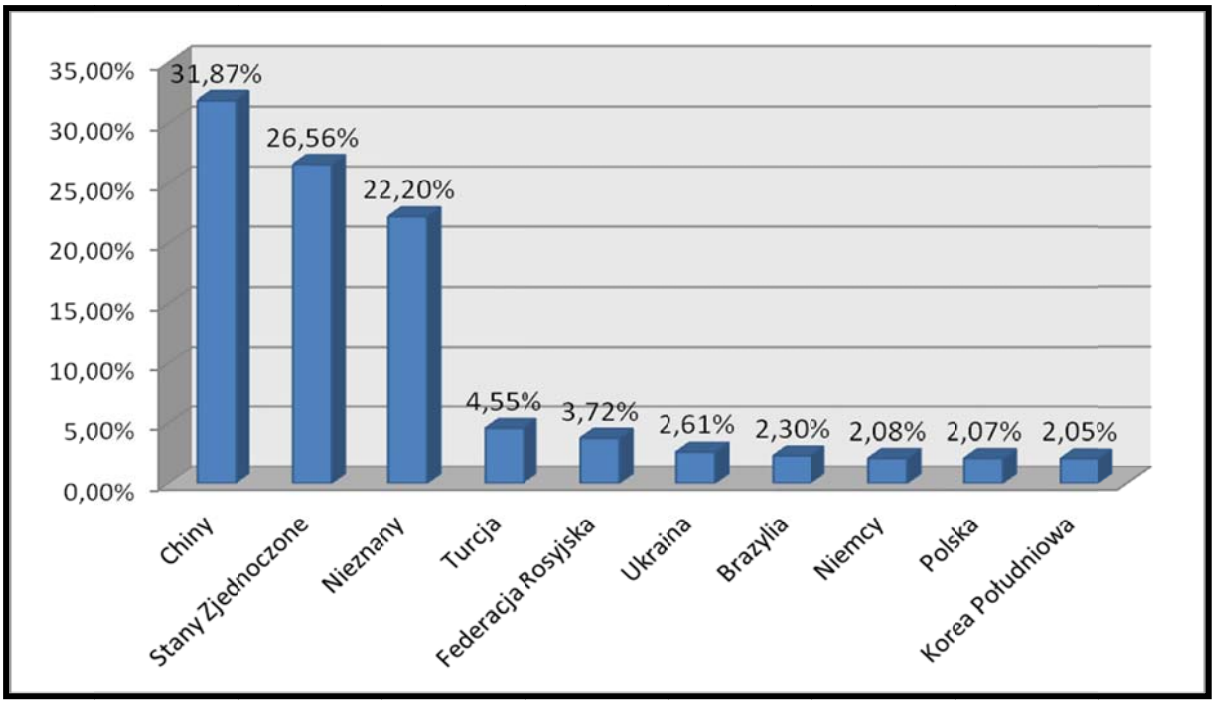
System ARAKIS-GOV[1] w 2011 roku zarejestrował 20634 alarmy, co stanowi znaczny spadek w porównaniu do poprzedniego roku, gdzie odnotowano ich 28109. Mając na uwadze poziom istotności i zagrożenia, alarmy podzielono na trzy główne kategorie. Najmniej odnotowano alarmów najgroźniejszych o priorytecie „wysokim" - 667, co stanowi 3,23% wszystkich zarejestrowanych. Najwięcej natomiast odnotowano alarmów o priorytecie „niskim", które stanowiły 77,96% ogółu. Pozostałe alarmy to priorytet „średni", których odnotowano 3880.



Rysunek 2-5: Rozkład procentowy alarmów ze względu na priorytety.

Informacje gromadzone i analizowane przez system ARAKIS-GOV pozwalają na określenie lokalizacji geograficznej źródła, z których wykonywano ataki na polskie sieci administracji publicznej objęte działaniem systemu. Do najczęściej występujących należą adresy IP przypisane do Chin (blisko 32%) i stanów Zjednoczonych – przeszło 26%.

[1] System ARAKIS-GOV jest systemem wczesnego ostrzegania przed zagrożeniami w sieci Internet. Jego architektura oparta jest na rozproszonym zestawie sensorów instalowanych w chronionych instytucjach na styku sieci produkcyjnej z siecią Internet. Centralna część systemu stanowią serwery dokonujące m.in. korelacji zdarzeń otrzymanych z poszczególnych źródeł, prezentujące wyniki analizy na witrynie WWW.

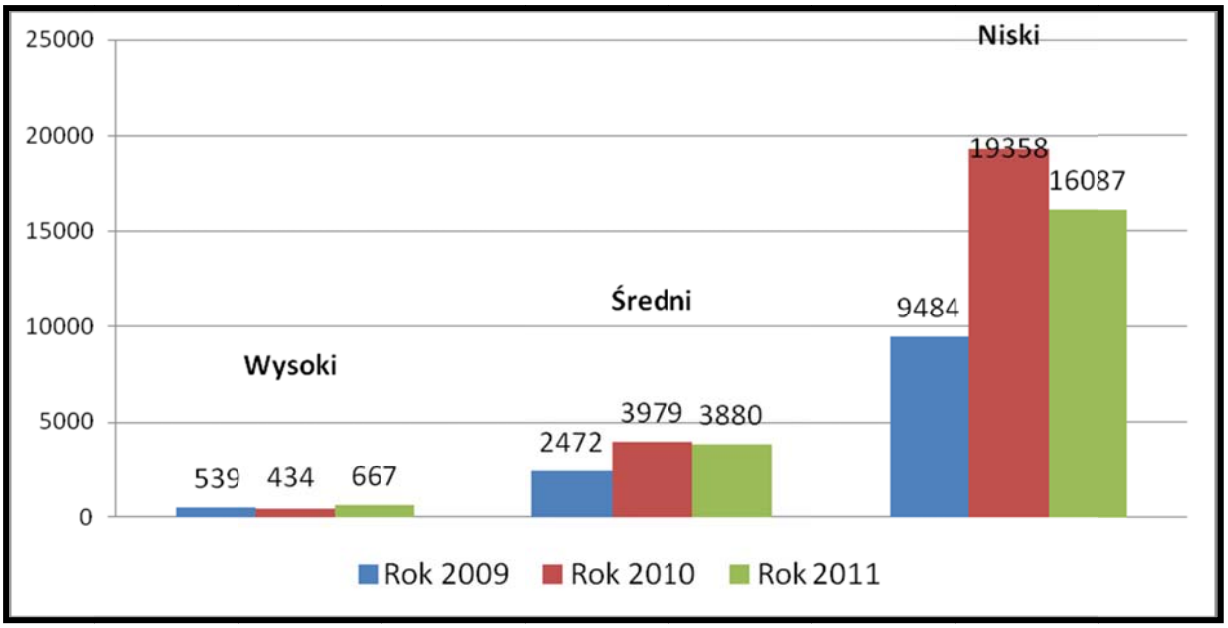


Rysunek 2-6: Rozkład procentowy źródeł ataków na monitorowane sieci przez system ARAKIS-GOV.

W powyższym wykresie dotyczącym statystyk źródeł ataków, trzecie miejsce zajmuje kategoria „Nieznany". Określenie to dotyczy adresów IP, które w chwili obecnej nie są przypisane do żadnego podmiotu – oznacza to, iż dokonano podszycia się (podmiany prawdziwego źródłowego adresu IP).

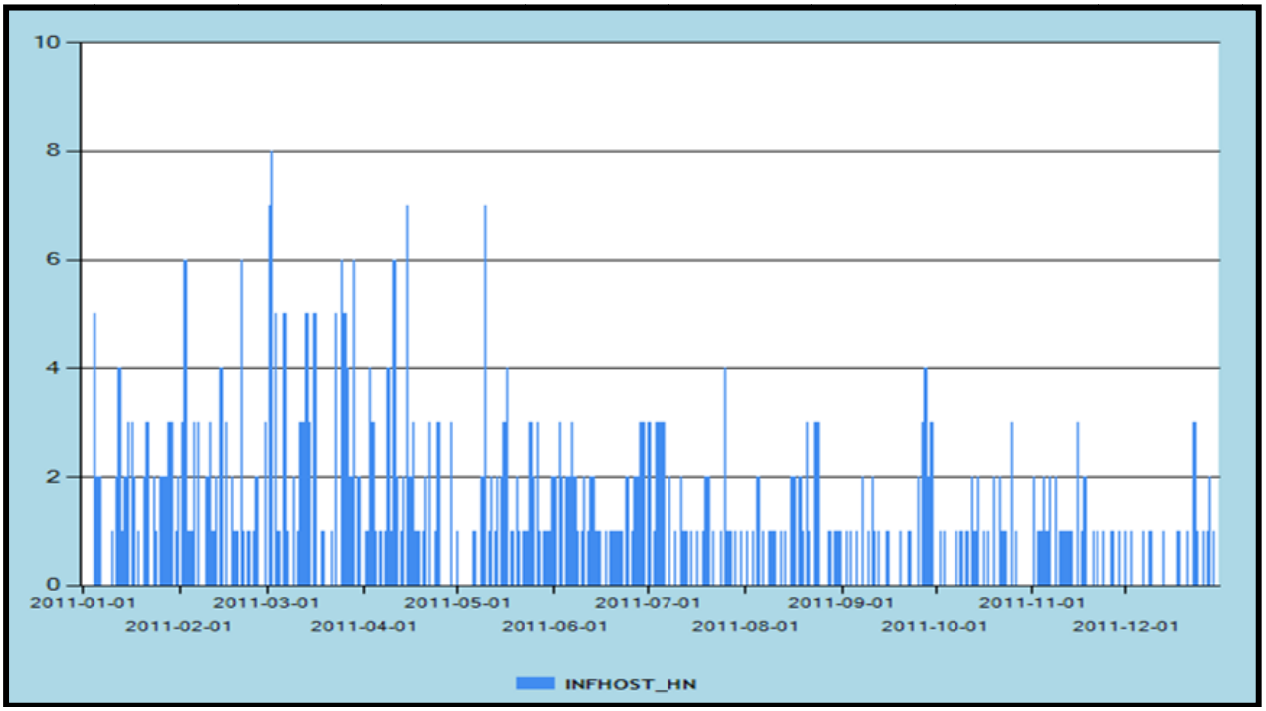
Należy także dodać, że specyfika protokołu TCP/IP sprawia, iż nie można bezpośrednio łączyć źródła pochodzenia pakietów z rzeczywistą lokalizacją zleceniodawcy ataku. Wynika to z faktu, iż w celu ukrycia swej tożsamości i fizycznej lokalizacji atakujący mogą wykorzystywać serwery pośredniczące (proxy) lub słabo zabezpieczone, bądź nieaktualizowane komputery, nad którymi wcześniej przejmują kontrolę.

W stosunku do lat poprzednich, system ARAKIS-GOV odnotował więcej ataków o priorytecie „Wysokim", co wynika z większej ilości zainstalowanych sond i monitorowanego obszaru. Natomiast na mniejszą ilość odnotowanych alarmów priorytetu „Niskiego" i „Średniego" składa się udoskonalona konfiguracja mechanizmów korelacyjnych systemu. W efekcie zarejestrowano mniejszą ilości alarmów typu „false-positives" oraz powielania się alarmów, dotyczących tych samych anomalii, czy incydentów.



Rysunek 2-7: Rozkład alarmów ze względu na priorytety w latach 2009-2011.

Poniżej na wykresie przedstawiono rozkład dzienny alarmów najpoważniejszych, wskazujących na prawdopodobną infekcję w sieciach instytucji chronionych systemem. Należy tu zwrócić uwagę, że część poniższych alarmów stanowią działania lokalnych administratorów, bądź błędna konfiguracja urządzeń.



Rysunek 2-8: Rozkład alarmów typu Infected_host w 2011 roku.

2.3. Testy bezpieczeństwa witryn internetowych administracji publicznej

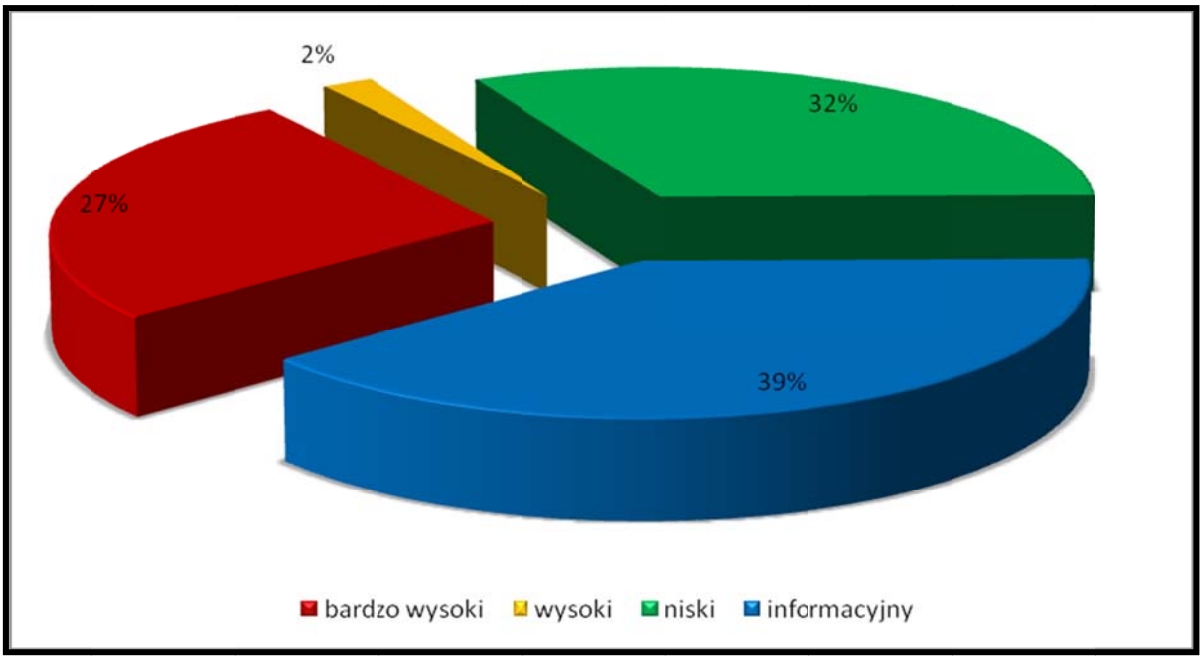
Od dnia 1 lipca 2008 r. CERT.GOV.PL prowadzi program sukcesywnego badania stanu zabezpieczeń witryn internetowych należących do instytucji administracji publicznej. Działania te mają na celu określenie poziomu bezpieczeństwa aplikacji WWW instytucji publicznych, a także usunięcie wykrytych nieprawidłowości. Instytucje, których witryny zostały przebadane, zostały poinformowane o wynikach audytu, wykrytych podatnościach istniejących w ich systemach i poinstruowane jak podatności te usunąć.

W 2011 roku przebadano 95 witryn należących do 33 instytucji państwowych. Stwierdzono ogółem 1000 błędów w tym: 269 błędów o bardzo wysokim poziomie zagrożenia, 20 błędów o wysokim poziomie zagrożenia, 320 błędy o niskim poziomie zagrożenia i 391 błędów oznaczonych jako informacyjne.

Ważniejsze ministerstwa i instytucje, których witryny zostały przebadane przez zespół CERT.GOV.PL w 2011r. to:

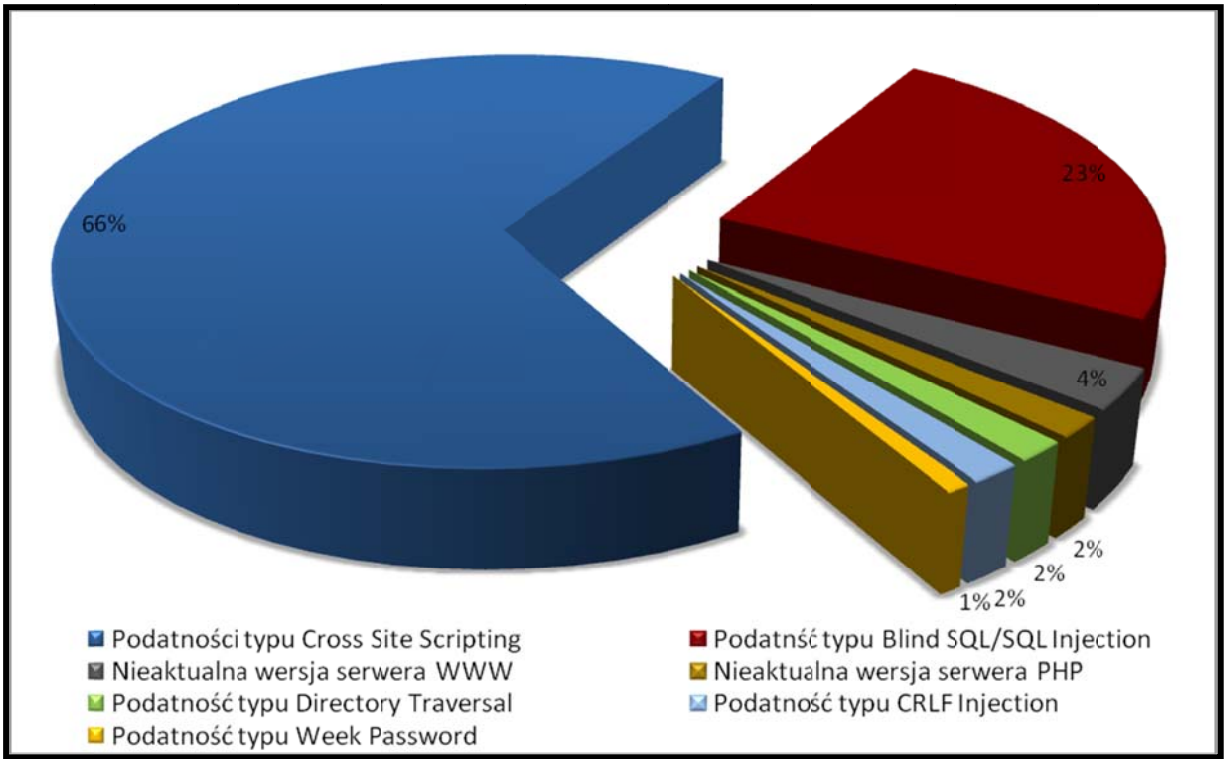
1. Ministerstwo Spraw Wewnętrznych i Administracji
2. Ministerstwo Spraw Zagranicznych
3. Ministerstwo Edukacji Narodowej
4. Ministerstwo Rozwoju Regionalnego
5. Biuro Bezpieczeństwa Narodowego
6. Agencja Restrukturyzacji i Modernizacji Rolnictwa
7. Instytut Ochrony Środowiska
8. Główny Urząd Miar
9. Polska Agencja Rozwoju Przedsiębiorczości
10. strony WWW należące do Ministerstwa Finansów (Izby Celne i Urzędy Skarbowe)

W trakcie skanowania witryn stwierdzono, że 30% przebadanych z nich zawierało przynajmniej jedną podatność, którą należało uznać za krytyczną dla bezpieczeństwa serwera i publikowanych na stronie treści. Tylko w nielicznych przypadkach, zabezpieczenia stron były skuteczne i nie stwierdzono w nich żadnych podatności. Tak duże różnice w jakości zabezpieczeń systemów świadczą o bardzo zróżnicowanej wiedzy związanej z bezpieczeństwem wśród osób odpowiedzialnych za administrację i utrzymanie systemów.



Rysunek 2-9: Statystyka wykrytych podatności w witrynach WWW należących do administracji publicznych według poziomu zagrożenia

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



Rysunek 2-10: Procentowy rozkład najpoważniejszych błędów

Należy zwrócić uwagę, iż ujawnione podatności krytyczne najczęściej znajdują się w warstwie usługowej systemu (np. serwerze www 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.

Tabela 1: Ilość witryn instytucji pod względem krytycznych błędów.

Stan bezpieczeństwa przebadanych witryn	Ilość stron
Bardzo dobry poziom bezpieczeństwa	31
Średni poziom bezpieczeństwa	39
Niski poziom bezpieczeństwa	25

Niski poziom bezpieczeństwa wynika z wykrytych podatności:

- Podatności typu Blind Sql/SQL injection

SQL injection / Blind SQL Injection jest podatnością pozwalającą atakującemu podmienić strukturę logiczną zapytania SQL, kierowanego do produkcyjnej bazy danych, z której korzysta witryna WWW. Zagrożenie występuje wówczas, gdy aplikacja dołącza do zapytania SQL dane otrzymane od użytkownika strony, bez filtrowania z niedozwolonych znaków.

- Podatność typu CRLF injection

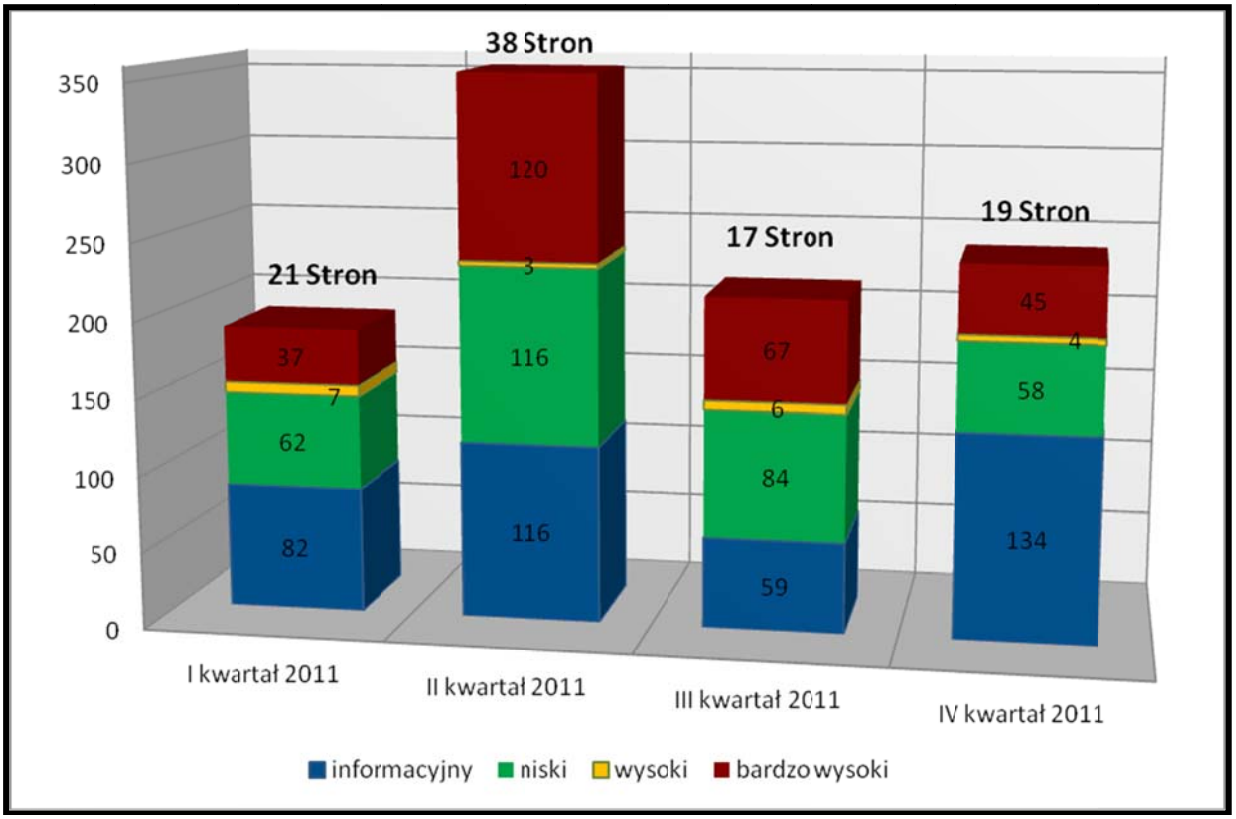
Podatność CRLF czerpie swoją nazwę od dwóch znaków użytych w tego typu atakach: CR - Carriage Return i LF - Line Feed. Są to dwa znaki ASCI, które nie są wyświetlane na ekranie, ale dzięki ich obecności system wie, w którym miejscu kończy się linia tekstu. Kombinację tych dwóch znaków wysyła klawisz Enter. Atakujący może zmodyfikować nagłówki http, podając niedozwolone dane.

- Directory Traversal

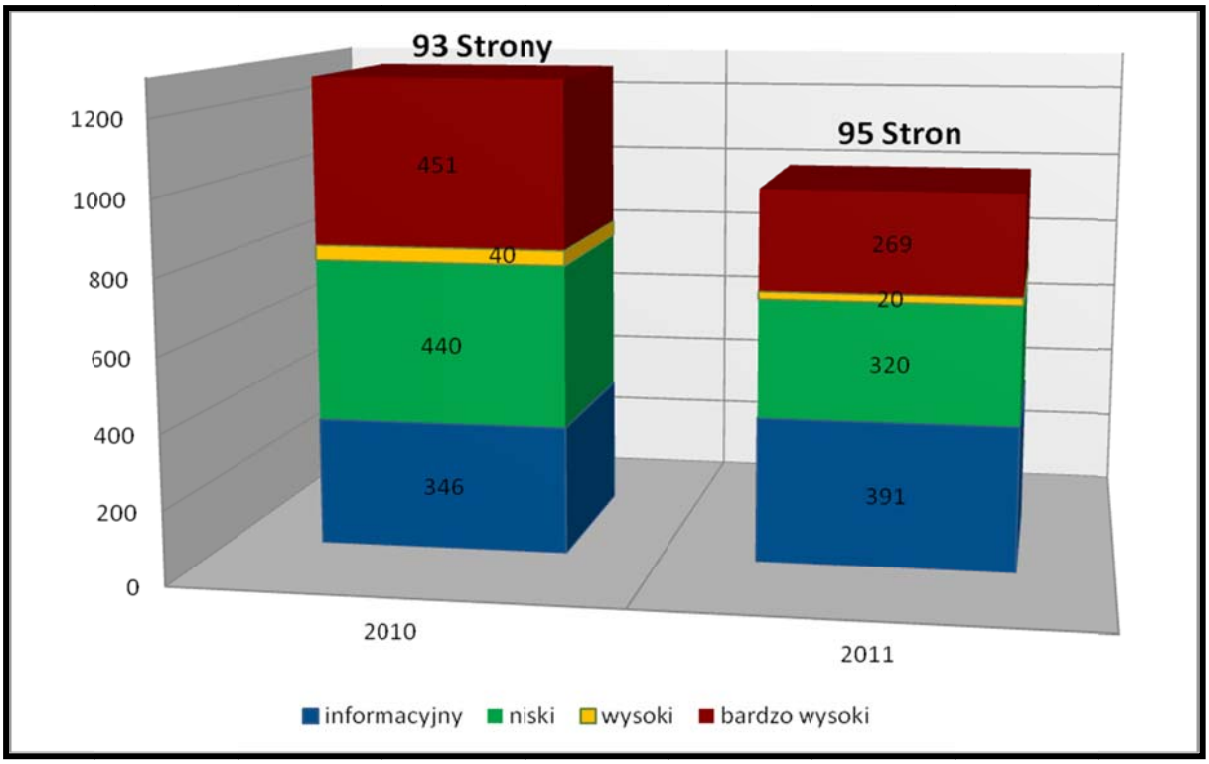
Directory Traversal jest podatnością pozwalającą atakującemu uzyskać dostęp do plików, które w strukturze katalogów na serwerze znajdują się wyżej niż katalog bazowy serwera WWW. Może to spowodować m.in. uzyskanie przez atakującego pliku z listą haseł do serwera (/etc/passwd). Zakładając, że katalog początkowy serwera WWW to /var/www/, nie powinno być możliwe przeczytanie zawartości katalogu /var/.

- Podatność typu Weak Password

Weak Password występuje, kiedy hasło dostępu do strony chronionej hasłem prawdopodobnie jest krótkie, często spotykane, standardowe, jednakowe z nazwą użytkownika lub podatne na atak typu brute force. Efektem wykorzystania tej podatności może być uzyskanie dostępu do zawartości strony chronionej hasłem przez osobę nieuprawnioną.



Rysunek 2-11: Liczbowy rozkład podatności przeskanowanych witryn z podziałem na istotność błędów w poszczególnych kwartałach.



Rysunek 2-12: Liczbowy rozkład podatności przeskanowanych witryn z podziałem na istotność błędów w porównaniu z poprzednim rokiem.

2.4. Testy bezpieczeństwa sieci administracji publicznej

W ramach działalności zespołu CERT.GOV.PL w roku 2011 rozwinięto usługę dotyczącą wykonywania bezpłatnych testów penetracyjnych zasobów jednostek administracji państwowej. Testy takie realizowane są tylko i wyłącznie na wniosek zainteresowanej instytucji i w obszarze wskazanym przez instytucje. W okresie, który obejmuje powyższy raport, do zespołu CERT.GOV.PL zgłosiły się trzy instytucje administracji państwowej z prośbą o przeprowadzenie testów penetracyjnych styku sieci korporacyjnej z siecią Internet oraz sieci wewnętrznej (lokalnej) instytucji.

Prowadzone testy mają charakter testów typu „Black-Box" – z minimalną wiedzą. W największym stopniu odzwierciedlają rzeczywistą wiedzę potencjalnego włamywacza. Ponadto testy na podstawie uzgodnień pomiędzy przedstawicielami instytucji odbywały się przy minimalnej wiedzy osób zaangażowanych w ochronę bezpieczeństwa sieci teleinformatycznych danej instytucji. W związku z tym, dokonano weryfikacji nie tylko rzeczywistego wdrożenia mechanizmów zabezpieczających infrastrukturę, ale również ewentualnych procedur na wypadek zaistnienia incydentu teleinformatycznego w sieci instytucji.

Należy podkreślić wysoki profesjonalizm i otwartość instytucji zgłaszających się z prośbą o przeprowadzenie działań audytowych, co przekłada się w dużej mierze na zdecydowane polepszenie bezpieczeństwa zasobów teleinformatycznych instytucji administracji państwowej.

Wnioski

W wyniku przeprowadzonych działań wnioski można rozpatrywać w dwóch płaszczyznach:

- testy zewnętrzne – testy penetracyjne mające na celu weryfikacje zabezpieczeń styku sieci wewnętrznej z siecią Internet w danej instytucji.
- testy wewnętrzne – testy penetracyjne mające na celu weryfikacje zabezpieczeń sieci i zasobów teleinformatycznych wewnętrznych w danej instytucji.

Na podstawie przeprowadzanych działań w obrębie testów zewnętrznych ujawniono, iż do najczęstszych poważnych błędów wykrytych podczas testów zaliczyć można:

- błąd konfiguracyjny polegający na udostępnianiu kanałów sieciowych (HTTPS, SSH, HTTP) służących do zdalnej administracji na urządzeniach brzegowych instytucji dla dowolnego adresu IP.
- błąd konfiguracyjny polegający na dostępie do usługi SNMP[2] od strony Internetu przy wykorzystaniu fabrycznie ustawionej wartości „community string", co pozwala w przypadku dostępu RO[3] na uzyskanie szerokiej wiedzy na temat samego urządzenia lub w przypadku dostępu RW[4] dokonanie np.: operacji wyłączenia interfejsu sieciowego.
- błąd polegający na uruchomionej starej wersji oprogramowania (bądź systemu operacyjnego urządzenia, lub innego oprogramowania np.: silnika PHP w przypadku serwerów WWW) posiadającego często luki pozwalające przejęcie systemu.

[2] Simple Network Management Protocol — rodzina protokołów sieciowych wykorzystywanych do zarządzania urządzeniami sieciowymi, takimi jak routery, przełączniki, komputery czy centrale telefoniczne. Do transmisji wiadomości SNMP wykorzystywany jest głównie protokół UDP: standardowo port 161 wykorzystywany jest do wysyłania i odbierania żądań, natomiast port 162 wykorzystywany jest do przechwytywania sygnałów trap od urządzeń. Możliwe jest także wykorzystanie innych protokołów do przekazywania żądań, na przykład TCP.

[3] Read-only – tylko do odczytu

[4] Read-write – możliwość odczytu i zapisu.

- Publikacje dokumentów na oficjalnej stronie instytucji zawierających metadane pozwalające na odgadnięcie algorytmu tworzenia nazw kont email czy nazw kont użytkowników w sieci lokalnej.

W przypadku testów wewnętrznych, zauważalny jest fakt podejścia do zasobów wewnątrz sieci przez administratorów w sposób mniej restrykcyjny, jeśli chodzi o bezpieczeństwo teleinformatyczne. Przejawia się to tym, iż na wszystkie przeprowadzone testy wewnętrzne w bieżącym roku przez zespół CERT.GOV.PL, w każdym przypadku udało się skompromitować, co najmniej jedną stację roboczą lub jeden serwer z danymi wrażliwymi dla instytucji.

Do najczęstszych błędów wykrytych podczas testów zabezpieczeń sieci i zasobów teleinformatycznych wewnętrznych instytucji należą:

- Błąd konfiguracyjny polegający na uruchomieniu usług serwerowych zawierających ustawione domyślne dane autoryzacyjne w postaci domyślnego hasła dla użytkownika z uprawnieniami administracyjnymi (serwery WWW, serwery bazodanowe).
- Błąd konfiguracyjny polegający na pozostawieniu aktywnym konta administratora lokalnego na systemach z rodziny systemów Windows działających w ramach Active Directory.
- Brak implementacji systemów antywirusowych na systemach serwerowych, działających w sieci lokalnej.
- Brak aktualizacji zainstalowanego oprogramowania na systemach serwerowych jak i brak aktualizacji samych systemów operacyjnych w sieci lokalnej.
- Brak zabezpieczeń sieci w warstwie drugiej modelu OSI[5].

Ponadto zauważalnym jest fakt, iż w większości przypadków brakuje implementacji mechanizmów (rozwiązań) do agregacji i analizy logów z systemów produkcyjnych instytucji. Trzeba zaznaczyć, iż dostępne są rozwiązania tego typu również na licencji „open source" pozwalającej na wykorzystanie w środowisku produkcyjnym.

[5] OSI (ang. Open System Interconnection) lub Model OSI (pełna nazwa ISO OSI RM, ang. ISO OSI Reference Model – model odniesienia łączenia systemów otwartych) – standard zdefiniowany przez ISO oraz ITU-T opisujący strukturę komunikacji sieciowej.

3. Bezpieczeństwo teleinformatyczne Polskiego Przewodnictwa w Radzie Unii Europejskiej

Polska przewodniczyła w Radzie Unii Europejskiej od 1 lipca do 31 grudnia 2011 r. Na potrzeby Polskiej Prezydencji uruchomiono wiele projektów teleinformatycznych służących do obsługi powyższego wydarzenia. W celu wsparcia procesu przygotowania, a następnie sprawowania Prezydencji, powołany został międzyresortowy projekt „Zapewnienie infrastruktury informatyczno-telekomunikacyjnej do przygotowania i obsługi Przewodnictwa Polski w Radzie Unii Europejskiej w II połowie 2011 r.". Realizacja projektu możliwa była dzięki współpracy CPI, DKPP MSZ, BOR i ABW. Centrum Projektów Informatycznych było podmiotem koordynującym oraz odpowiedzialnym za zapewnienie złożonej infrastruktury teleinformatycznej całości projektu. Rządowy Zespół Reagowania na Incydenty Komputerowe CERT.GOV.PL również brał udział w powyższym projekcie, pełniąc funkcje miedzy innymi organu doradczego w zakresie zapewnienia bezpieczeństwa i monitoringu rozwiązań teleinformatycznych uruchomionych na potrzeby Prezydencji.

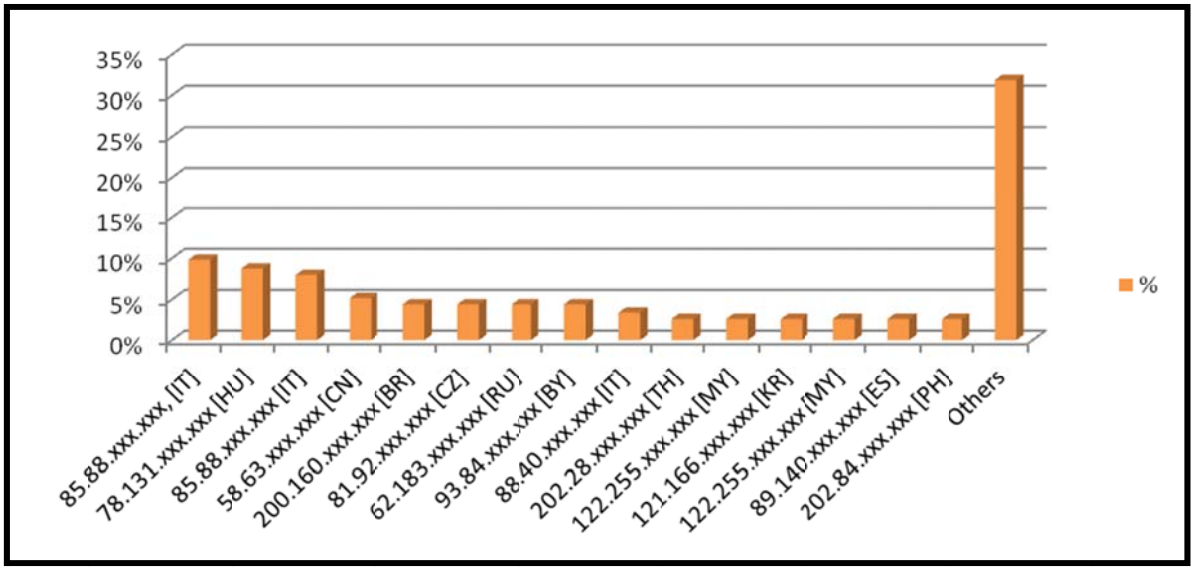
W ramach powyższych działań CERT.GOV.PL wykonał następujące działania:

- wdrożono system ARAKIS-GOV w ramach infrastruktury lokalnej w poszczególnych ośrodkach (miejscach) spotkań realizowanych podczas Polskiej Prezydencji
- wykonano testy penetracyjne sieci lokalnej przygotowanej w miejscach spotkań polskiej Prezydencji
- wykonano testy bezpieczeństwa aplikacji webowych (WWW) przygotowanych w celu obsługi wydarzenia Polskiej Prezydencji
- pełniono wiodącą rolę podczas ewentualnych incydentów (naruszenia bezpieczeństwa) teleinformatycznych o charakterze istotnym w obszarach wspólnie ustalonych z koordynatorem całego projektu.

3.1. Wybrane statystyki wynikające z obserwacji infrastruktury przygotowanej na potrzeby Polskiej Prezydencji

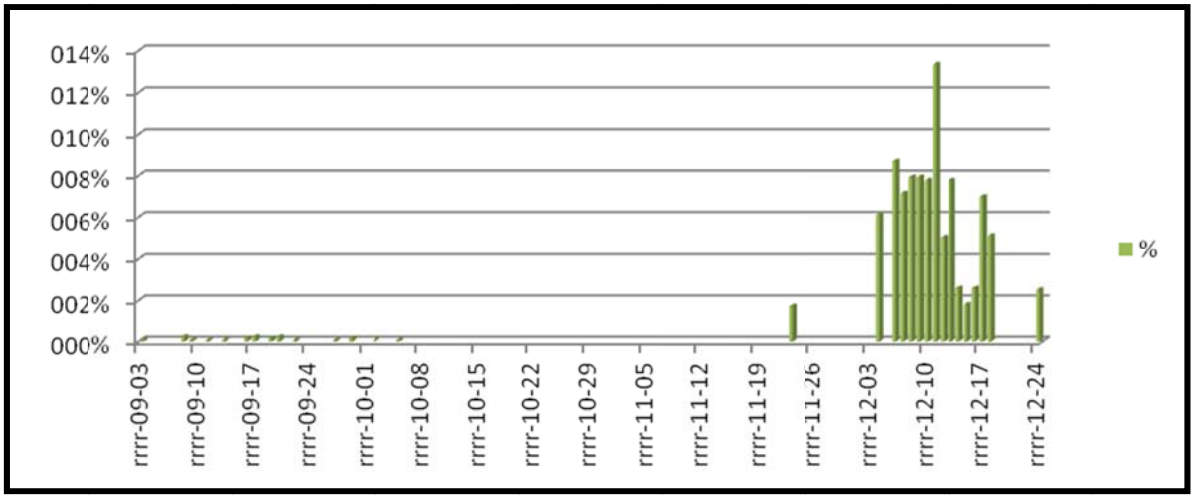
Podczas trwania Polskiego Przewodnictwa w Radzie Unii Europejskiej nie odnotowano incydentu o charakterze „istotnym", zagrażającym prawidłowemu funkcjonowaniu infrastruktury działającej w ramach projektu.

Poniżej przedstawione zostały statystyki najbardziej aktywnych hostów odnotowanych przez systemy IDS/IPS pod względem największej ilości faktycznych zdarzeń powiązanych z danym adresem IP. Powyższe statystyki pochodzą z systemów IDS/IPS chroniących aplikacje webowe (WWW) przygotowane w celu obsługi wydarzenia polskiej Prezydencji.



Rysunek 3-1: Statystyki najbardziej aktywnych hostów

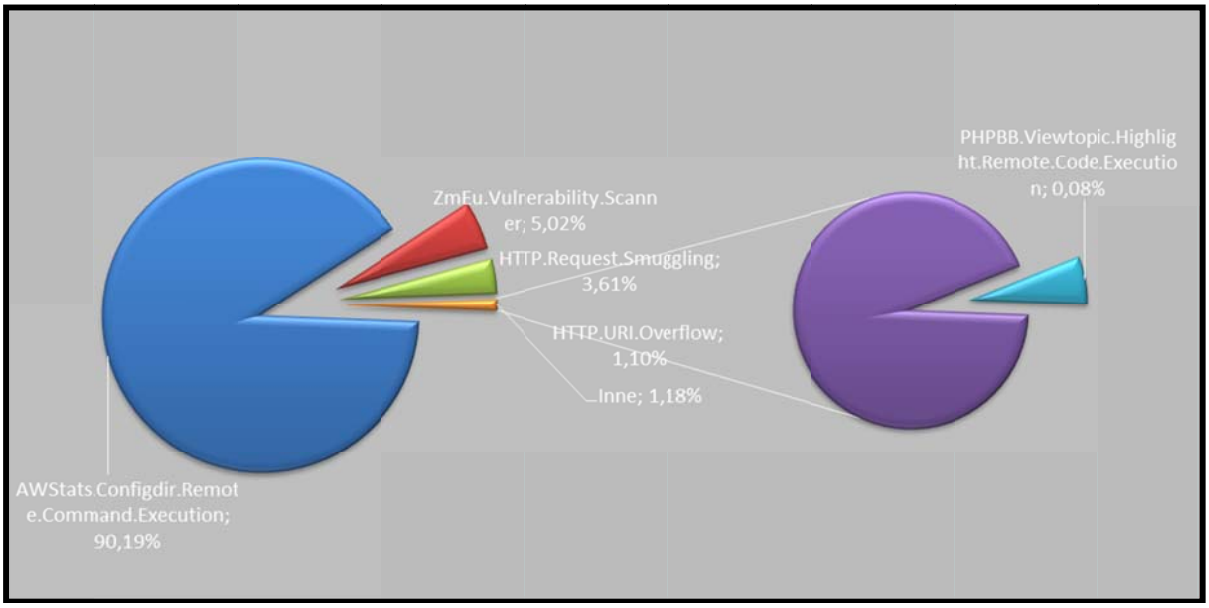
Na kolejnym wykresie, również w oparciu o dane z systemów IDS/IPS chroniących aplikacje webowe (WWW) przygotowane w celu obsługi wydarzenia polskiej Prezydencji, przedstawiono rozkład ilościowy na przestrzeni czasu trwania polskiej Prezydencji.



Rysunek 3-2: Rozkład ilościowy danych z systemów IDS/IPS na przestrzeni czasu trwania polskiej Prezydencji

Wykres zawiera informacje od września 2011 roku ze względu na fakt, iż wartości dla zakresu czasowego sprzed daty wrześniowej są minimalne i nie przekraczają wartości 0,01%. Jak pokazuje powyższy rysunek w grudniu 2011 roku mieliśmy istotny wzrost zainteresowania aplikacjami WWW stworzonymi na potrzeby polskiej Prezydencji.

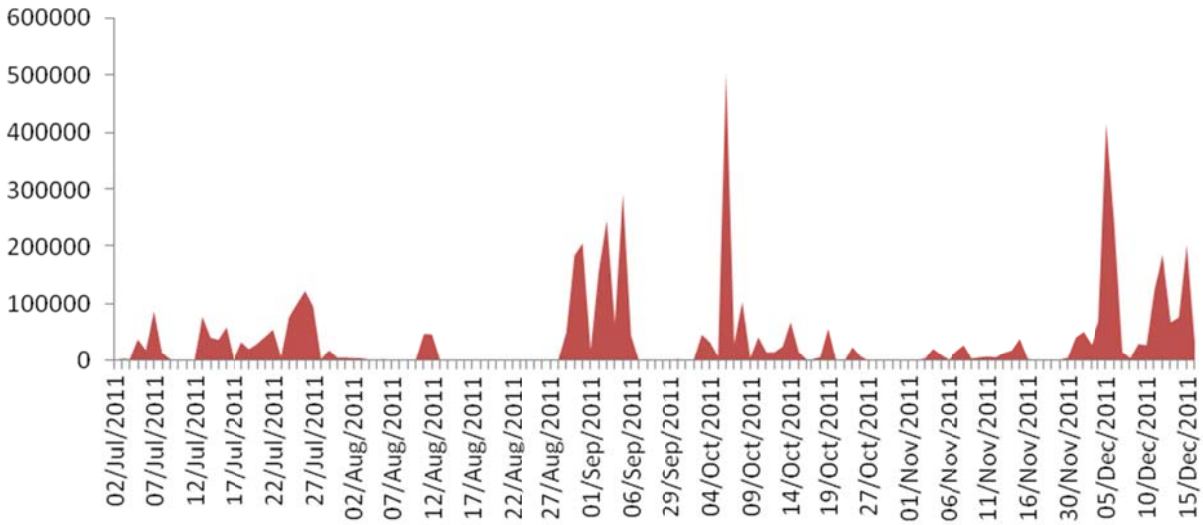
Kolejny wykres przedstawia rozkład pięciu, najczęściej zaraportowanych, reguł IDS/IPS, które informowały o próbach ataku.



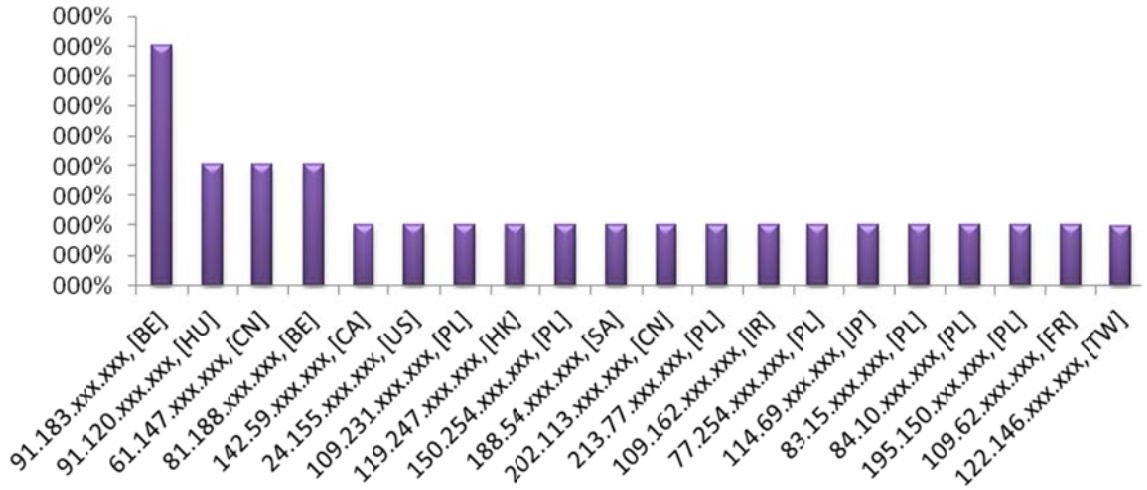
Rysunek 3-3: Pięciu reguł IDS/IPS, które posiadały największą ilość wystąpień

W dalszej części raportu przedstawiono statystyki dotyczące ochrony infrastruktury teleinformatycznej przygotowanej na potrzeby spotkań w ramach polskiego Przewodnictwa w Radzie Unii Europejskiej. Najważniejsze wydarzenia w ramach polskiej prezydencji odbyły się w pięciu miastach: Sopocie (lipiec), Wrocławiu (wrzesień), Krakowie (październik), Poznaniu (listopad) i Warszawie (grudzień). W każdym z ośrodków została przygotowana infrastruktura teleinformatyczna potrzebna do obsługi powyższych spotkań.

Poniżej przedstawiono statystyki dotyczące ruchu zablokowanego na przestrzeni trwania całej polskiej Prezydencji na urządzeniach typu IDS/IPS chroniących infrastrukturę teleinformatyczną we wszystkich miejscach spotkań:



Następny wykres przedstawia listę źródłowych adresów IP zidentyfikowanych przez urządzenia IDS/IPS jako najbardziej aktywne pod katem ilości połączeń, które zostały zablokowane. Należy jednak pamiętać, że specyfika protokołu TCP/IP sprawia, iż 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 mogą wykorzystywać serwery pośredniczące (proxy) lub słabo zabezpieczone, bądź nieaktualizowane komputery, nad którymi wcześniej przejmują kontrolę.



4. Ataki ukierunkowane na sektor administracji publicznej

W porównaniu do roku 2010, można zaobserwować rosnąca ilość dedykowanych ataków socjotechnicznych skierowanych przeciwko pracownikom administracji publicznej.

Należy pamiętać, iż rosnący poziom zabezpieczeń technicznych systemów teleinformatycznych powoduje zwrócenie się przestępców w kierunku najsłabszego (ich zdaniem) ogniwa, jakim jest człowiek.

Nadal najczęściej wykorzystywanym medium ataku jest poczta e-mail. Jednak w zauważalnie większym procencie (w porównaniu z ubiegłym rokiem), wykorzystywane są przez atakujących konta prywatne ofiar. Najczęściej są one o wiele słabiej monitorowane pod względem bezpieczeństwa załączników, jak również dostęp do nich omija zabezpieczenia poziomu korporacyjnego.

Możliwość dostępu do poczty prywatnej z poziomu komputera firmowego powoduje, iż praktycznie wszystkie (potencjalnie groźne) załączniki mogą zostać zapisane na takim komputerze z ominięciem całej infrastruktury bezpieczeństwa. Jedynym środkiem ochrony pozostaje lokalny antywirus, jednakże ze względu na to, iż bardzo często do ataku jest używane złośliwe oprogramowanie wykorzystujące luki typu 0-day, staje się on nieefektywny.

Możliwym rozwiązaniem jest blokada dostępu (na poziomie technicznym lub organizacyjnym) do poczty prywatnej oraz dodatkowe wprowadzenie rozwiązań uniemożliwiających uruchomienie oprogramowania, które wcześniej nie zostało dopuszczone przez administratorów systemu. Dodatkowo należy zadbać, aby oprogramowanie użytkowe uruchamiane było jedynie w środowisku typu „sandbox”.

W dalszym ciągu zdarzają się próby ataków wykorzystujących nośniki fizyczne. Najczęściej polega to na podrzuceniu w miejscu dostępnym głównie dla pracowników (np. ubikacja lub palarnia) nośnika usb lub płyty opisanej w sposób wzbudzający ciekawość. Na nośniku znajduje się najczęściej złośliwe oprogramowanie w postaci konia trojańskiego.

4.1. Ataki bez użycia klasycznego oprogramowania złośliwego

Jednym z ciekawszych (pod względem technicznym) działań przeciwko systemom teleinformatycznym, z którymi miał do czynienia w 2011 roku zespół CERT.GOV.PL, był atak na system poczty jednej z agend rządowych.

W tym przypadku sprawcy przeprowadzili najpierw rozpoznanie używanych systemów i wykryli potencjalną podatność w systemie dostępu do poczty korporacyjnej poprzez rozwiązanie typu webmail.

Atak polegał na przesłaniu, z serwera darmowej poczty, z adresu zbliżonego do poprawnego[6], odpowiednio spreparowanego e-maila zawierającego jedynie obojętną treść, w której dodatkowo nie występował żaden jawny odnośnik. W tym momencie otrzymanie takiej przesyłki nie wzbudzało podejrzeń u ofiary. W czasie szkoleń uwypuklane jest, iż nie należy ufać załącznikom przesłanym od nieznanej osoby, jak również nie klikać w przesyłane odnośniki. Żadna z tych rzeczy nie występowała w tym przypadku.

Zamiast tego, na końcu wiadomości znajdował się otwarty znacznik HTML `<SCRIPT src=adres/skrypt.js` odwołujący się do pliku JavaScript znajdującego się na serwerze atakującego.

Pozostawienie otwartego znacznika HTML, spowodowało dodatkowo, iż nie wyświetlały się reklamy automatycznie dodawane przez system darmowej poczty.

Podczas parsowania[7] treści, system webmail automatycznie uruchamiał plik JavaScript, którego zadaniem było wykradnięcie tzw. ciasteczka zawierającego nazwę użytkownika oraz klucz sesji, co umożliwiało zalogowanie się na konto ofiary.

Atak zakończył się niepowodzeniem, ze względu na poprawną konfigurację systemu webmail, który do tworzenia klucza sesyjnego wykorzystywał m.in. adres IP, z którego nawiązywano połączenie. W efekcie, pomimo przejęcia przez atakującego wszelkich potrzebnych danych, nie było możliwe ich skuteczne użycie.

4.2. Socjotechnika i załączniki poczty elektronicznej

Socjotechnika w zakresie ochrony informacji stanowi jeden z kluczowych obszarów, decydujących o skuteczności stosowanych zabezpieczeń pozwalających na ograniczenie możliwości penetracji środowiska teleinformatycznego instytucji publicznych.

[6] Specjalnie skonstruowany adres e-mail, który wygląda jak adres poprawny, zaufany. Przykładowo: poczta@domena_gov.pl zamiast poczta@domena.gov.pl (użycie _ zamiast .)
[7] Przetwarzanie treści w poszukiwaniu znaczników (np. HTML) pozwalających na wyświetlenie maila w pełnej postaci (np. z pogrubieniami, podkreśleniami, kolorami)

Ataki tego typu należące do tzw. „social engineering attacks" stały się powszechną praktyką stosowaną przez sprawców pozwalającą na uzyskiwanie dostępu do zasobów teleinformatycznych instytucji. Instytucje publiczne tak samo jak użytkownicy i podmioty prywatne zagrożone są atakami wykorzystującymi mechanizmy inżynierii społecznej.

Rozbudowane systemy teleinformatyczne instytucji z wieloma stanowiskami dostępu, różnymi aplikacjami i systemami oraz dużą liczbą użytkowników niosą za sobą większą złożoność w zakresie zarządzania bezpieczeństwem teleinformatycznym i zapewnienia pożądanego przez instytucje poziomu bezpieczeństwa. Pozwala to na łatwiejszą infekcję i propagację zagrożeń w instytucji. Wrażliwym elementem bezpieczeństwa teleinformatycznego instytucji jest środowisko pracowników. Pracownicy poprzez błędne przeświadczenie o autentyczności odbieranych przez nich informacji przesyłanych z użyciem socjotechniki z „wiarygodnego" źródła podejmują zakładane przez sprawców działania umożliwiające m.in. przejęcie komputera czy kradzież informacji i w ten sposób wpływają istotnie na całościowe bezpieczeństwo.

Rok 2011 zaowocował występowaniem ataków ukierunkowanych z użyciem metod socjotechnicznych wykorzystujących znane jak i nowe podatności typu „zero-day".

Ataki tego typu są bardziej zaawansowanymi socjologicznie mechanizmami działania sprawców adresowanymi dla konkretnej grupy odbiorców danej instytucji.

Schemat ataku najczęściej wykorzystuje podatności określonych aplikacji zainstalowanych w systemie operacyjnym użytkownika w celu doprowadzenia do kompromitacji systemu w postaci przejęcia konta użytkownika czy wyłączenia działania określonych usług systemowych. Przeprowadzenie takich ataków wymaga wiedzy odnośnie danej instytucji w postaci np. znajomości adresów poczty elektronicznej pracowników instytucji (dostępnych oficjalnie w sieci Internet) lub poprzez wykorzystanie określonych autentycznych lub sfałszowanych wydarzeń wzbudzających powszechne publicznie zainteresowanie lub wiedzy odnośnie sposobu realizacji przez instytucje publicznie zadań. To wszystko pozwala na stworzenie wiarygodnej informacji adresowanej do pracowników instytucji i w ten sposób pozyskanie ich zaufania

Drugim elementem ataku jest stworzenie informatycznie określonego rodzaju mechanizmu propagacji socjotechnicznych treści uwiarygodniających źródło ich pochodzenia oraz zawierających przygotowany przez sprawcę określony program lub złośliwy kod uaktywniany na komputerze ofiary ataku. Mechanizm ten pozwala poprzez otworzenie np.

załącznika do poczty elektronicznej w formacie pdf, uzyskanie nieautoryzowanego dostępu do systemu operacyjnego komputera z uprawnieniami użytkownika lub administratora i przeprowadzenia dalszych niepożądanych działań uzależnionych od motywów działania sprawcy (np. kradzież informacji, przyłączenie do sieci „botnet", itp.). Głównym celem, w przypadku instytucji, jest przede wszystkim kradzież informacji, których dystrybucja podlega różnym ograniczeniom i jest traktowana jako zasób wrażliwy.

Według CERT.GOV.PL, spośród incydentów związanych z atakami ukierunkowanymi w 2011 roku, można wyróżnić dwie główne grupy ataków:

- ataki opierające się na wysyłaniu poczty elektronicznej z zawirusowanymi załącznikami w formatach właściwych dla aplikacji biurowych typu pdf, xls, itp.;
- ataki opierające się na wysyłaniu poczty elektronicznej wykorzystujące podatności przeglądarek internetowych służących do przeglądania poczty elektronicznej jako „webmail".

W roku 2011 CERT.GOV.PL odnotowało kilka przypadków ataków ukierunkowanych na pracowników administracji państwowej z użyciem metod socjotechnicznych.

W pierwszym kwartale 2011 roku miała miejsce akcja „mailingowa" skierowana do pracowników administracji państwowej, polegająca na rozsyłaniu wiadomości poczty elektronicznej z załącznikiem „pdf". Nadawca wiadomości podszywał się pod pracownika pochodzącego z jednego z urzędów administracji państwowej, a treść korespondencji wzorowana była na korespondencji urzędniczej. Załącznik do poczty elektronicznej w formacie „pdf" został zawirusowany w sposób pozwalający na wykorzystywanie podatności Adobe Reader związanej z JavaScript. Większość dostępnych silników antywirusowych nie sygnalizowała żadnego zagrożenia. W trakcie analizy dokonanej przez CERT.GOV.PL okazało się, ze kod JavaScript umieszczony w pliku „pdf" był wadliwy i uniemożliwiał skuteczną infekcję systemów. Analiza kodu JavaScript pozwoliła na symulację jego uruchomienia i opisanie aktywności w postaci infekcji komputera, utworzenia plików tymczasowych oraz aktywowania szyfrowanego połączenia ze zdalnym serwerem. CERT.GOV.PL poinformował użytkowników o zagrożeniu wraz z zaleceniami.

W drugim kwartale 2011 roku miała miejsce próba ataku socjotechnicznego skierowanego przeciwko pracownikom jednego z ministerstw. Rozesłano email zawierający załącznik w formacie Microsoft Office „xls", który był próbą wykorzystania wykrytej podatności opisanej w Microsoft Security Bulletin MS09-067. Podatność ta pozwalała

na wykonanie dowolnego kodu z uprawnieniami aktualnie zalogowanego użytkownika. Uwidaczniała się w momencie, gdy użytkownik otworzył arkusz kalkulacyjny, który zawiera nieprawidłowo utworzony jeden z rekordów. Nadawca emaila także został podmieniony, tak, aby ukryć źródło pochodzenia przesyłki. Dodatkowo po otwarciu załącznika przesyłki uruchamiany był proces otwierający połączenia sieciowe i tworzone były rożne tymczasowe pliki na komputerze. CERT.GOV.PL poinformował instytucję o zagrożeniu.

W trzecim kwartale 2011 r. doszło do kolejnej akcji emailowej skierowanej na adresy pracowników instytucji państwowych. Wiadomość email zawierała oprogramowanie złośliwe umieszczone w załączniku xls, sklasyfikowane jako podatność Microsoft CVE-2009-3129. Wektor ataku wykorzystywał znaną z wcześniejszego ataku podatność Microsoft Excel. Cechą szczególną ataku było posługiwanie się wieloma rożnymi adresami nadawców Użytkownicy zostali powiadomieni o ataku. Nie stwierdzono prób otwierania zawirusowanego załącznika ani skutecznej infekcji. CERT.GOV.PL udzielił wsparcia technicznego instytucjom będących celem ataku wraz z zaleceniami.

Czwarty kwartał 2011 roku zaowocował wystąpieniem ataku skierowanego przeciwko pracownikom jednej z instytucji poprzez wysyłanie poczty elektronicznej z załącznikiem zawirusowanym skryptem JavaScript. Wykonanie skryptu powodowało utworzenie na komputerze ofiary pliku wykonywalnego i zainicjowanie połączeń ze zdalnym adresem oraz odpytywaniem serwera DNS. Przedmiotowy atak wykorzystywał podatność określaną jako zero-day, niewykrywalną przez silniki antywirusowe. CERT.GOV.PL uczestniczył w analizie działania przedmiotowego skryptu.

W roku 2011 zanotowano także incydenty związane z wysyłaniem wiadomości email zawierających linki URL z zawartością aktywną JavaScript. Emaile te były specjalne przygotowane w celu przechwytywania sesji użytkowników korzystających z poczty elektronicznej poprzez webmail. Otwarcie takich przesyłek umożliwiało dostęp do konta użytkownika poczty elektronicznej i odczytywanie wiadomości. CERT.GOV.PL zidentyfikował złośliwe przesyłki i określił rodzaj zabezpieczeń, które należało zastosować w celu eliminacji tego typu zagrożeń.

5. Bezpieczeństwo internetowe administracji publicznej

Podobnie jak w latach poprzednich, odnotowano znaczną ilość ataków typu website defacement. Często wynikiem takich ataków jest podmiana zawartości strony głównej portalu, bądź umieszczenie na skompromitowanym serwerze fałszywej strony phishingowej. Pierwsze powoduje rozgłos medialny i dyskredytację, drugie natomiast służy wykradaniu i gromadzeniu, w celach przestępczych, danych wrażliwych. Pomimo prowadzonych przez zespół CERT.GOV.PL działań proaktywnych takich jak testy bezpieczeństwa witryn oraz akcje uświadamiające, sektor polskiej administracji publicznej również nie ustrzegł się tego typu ataków.

5.1. Masowa podmiana treści witryn samorządowych

W dniu 30 września 2011r. osoby posługujące się nickami hardstyle77 oraz punkG dokonały podmiany treści około 300 witryn samorządowych. Do ponownej podmiany doszło w dniu 2 września 2011r. Po drugim ataku firma hostingowa utrzymująca witryny zdecydowała o przyjęciu wystosowanej wcześniej oferty pomocy w obsłudze incydentu przez CERT.GOV.PL.

Mechanizm włamania z dnia 30 września 2011r. obejmował wyciągnięcie hasła do panelu administracyjnego za pomocą ataku SQL Injection:

```
87.236.194.158 - - [30/Aug/2011:18:17:09 +0200] "GET
/drukuj.php?id=153&a=21+and+1=2+union+select+1,group_concat
(column1,0x3a, column2,0x3a, column3,0x3a, column4,0x3a,
column5,0x3a, column5,0x3a, column6,0x3a, column7,0x3a,
column8,0x3a, column9,0x3a, column10,0x3a, column11,0x3a,
column12),3,4,5,6,7+from+table_name-- HTTP/1.1" 200 1456 "-"
"Mozilla/5.0 (X11; Linux x86_64; rv:5.0) Gecko/20100101
Firefox/5.0"
```

Brak odpowiedniego filtrowania danych przekazywanych do zmiennych w skrypcie PHP oraz anachronizm w postaci przechowywania niezaszyfrowanych haseł w bazie danych spowodował, iż możliwe było poznanie nazw użytkowników i haseł panelu administracyjnego.

W kolejnym kroku atakujący dodawał shell PHP do systemu plików (za pomocą apletu Java do połączeń przy użyciu protokołu FTP):

```
192.251.226.206 - ****** [30/Aug/2011:18:27:33 +0200] "GET
/panel/bip.***.pl/dodaj_plik_ftp.php HTTP/1.1" 200 1580
"http://bip.***.pl/panel/bip.***.pl/" "Mozilla/5.0 (X11; Linux
x86_64; rv:5.0) Gecko/20100101 Firefox/5.0"
```

oraz próbował wywołać wgrany wcześniej plik za pomocą przeglądarki:

```
192.251.226.206 - - [30/Aug/2011:18:32:41 +0200] "GET /0wn.php
HTTP/1.1" 404 264 "-" "Mozilla/5.0 (X11; Linux x86_64; rv:5.0)
Gecko/20100101 Firefox/5.0"

192.251.226.206 - - [30/Aug/2011:18:32:48 +0200] "GET
/upload/0wn.php HTTP/1.1" 200 111 "-" "Mozilla/5.0 (X11; Linux
x86_64; rv:5.0) Gecko/20100101 Firefox/5.0"
```

W kolejnych krokach, przy użyciu wgranego przez siebie skryptu dokonał wielu operacji w zaatakowanym systemie, w tym podmiany treści wszystkich witryn utrzymywanych na serwerze:

```
192.251.226.206 - - [30/Aug/2011:18:34:04 +0200] "POST
/upload/0wn.php HTTP/1.1" 200 4724
"http://bip.***.pl/upload/0wn.php" "Mozilla/5.0 (X11; Linux
x86_64; rv:5.0) Gecko/20100101 Firefox/5.0"
```

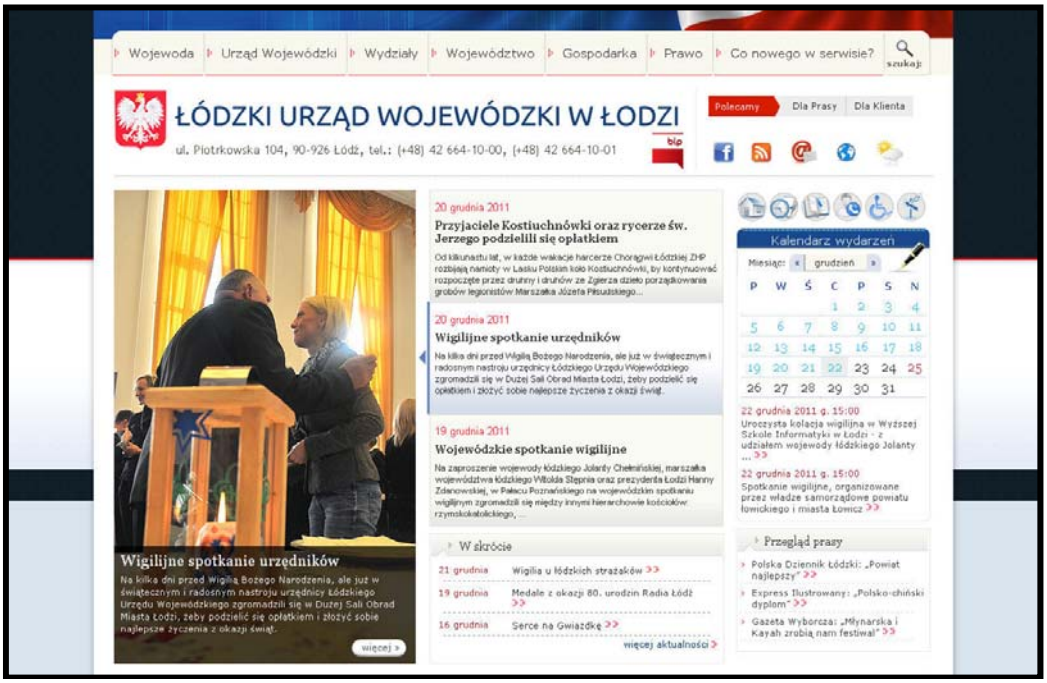
W dniu 3 września 2011r., Rządowy Zespół Reagowania na Incydenty Komputerowe przekazał firmie hostingowej zalecenia, które zostały wdrożone 7 września 2011r. Obejmowały one między innymi:

- zastosowanie walidacji danych wejściowych do parametrów w skryptach PHP
- zastosowanie szyfrowania haseł w bazie danych
- zastosowanie szyfrowania SSL podczas logowania do panelu administracyjnego
- implementację szyfrowania podczas logowania do usługi serwera FTP
- hardening PHP – ustawienie odpowiednich wartości w pliku konfiguracyjnym *php.ini*
- weryfikację uprawnień do plików w katalogu serwera WWW

- zainstalowanie i odpowiednią konfigurację firewall'a aplikacyjnego WAF (*ang. Web Application Firewall)*

5.2. Urząd Wojewódzki w Łodzi

Kolejny udany atak miał miejsce w styczniu 2011 roku. Ofiarami zostały czterdzieści cztery witryny, w tym serwis Wojewódzkiego Urzędu w Łodzi. W Internecie udostępnione zostały hasła pozwalające na dostęp do panelu administracyjnego www.uw.ludz.pl/admin/index.php. W wyniku tego działania podmieniona została witryna Internetowa Urzędu. Po interwencji zespołu CERT.GOV.PL administratorzy witryny przeprowadzili czynności mające na celu zwiększenie bezpieczeństwa strony.

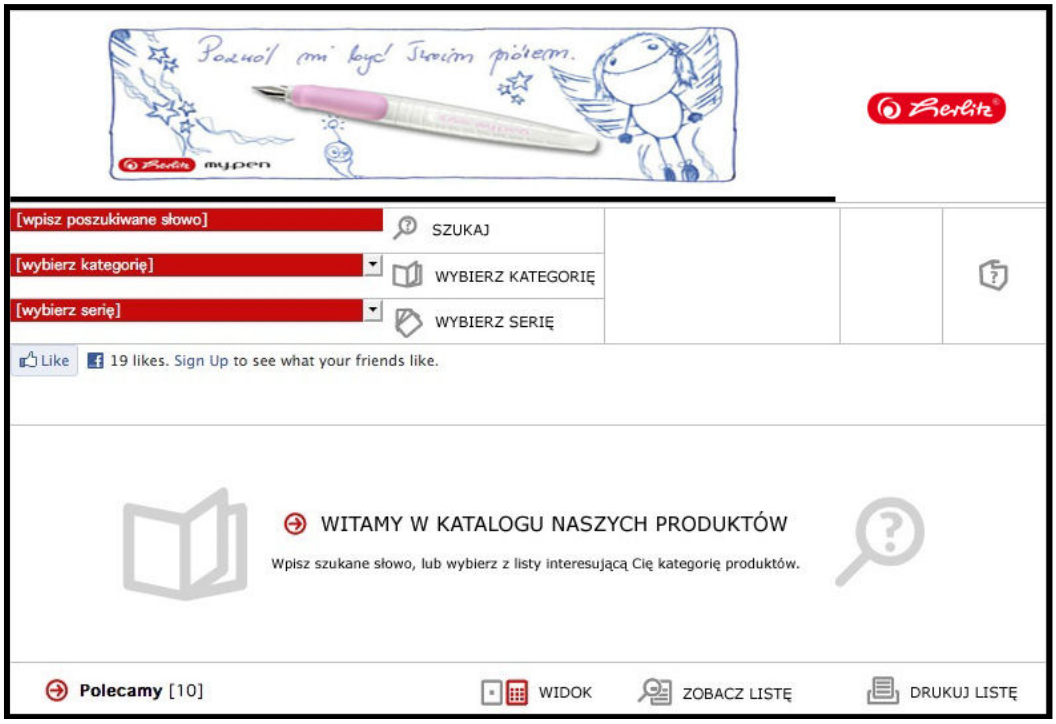


Rysunek 5-1: Wygląd witryny Urzędu Wojewódzkiego w Łodzi

Rysunek 5-2: Podmieniona witryna Urzędu Wojewódzkiego w Łodzi.

5.3. DNS MSWiA

W czerwcu 2011 roku ustalono, iż na witrynach internetowych należących do Ministerstwa Spraw Wewnętrznych i Administracji www.informatyzacja.gov.pl oraz www1.mswia.gov.pl widoczny był sklep internetowy oferujący produkty firmy Herlitz. Incydent spowodowany był niewłaściwą konfiguracją serwerów DNS. Po wykryciu, administratorzy ministerstwa dokonali weryfikacji poprawności konfiguracji serwerów DNS oraz przywrócili prawidłowy stan witryn.



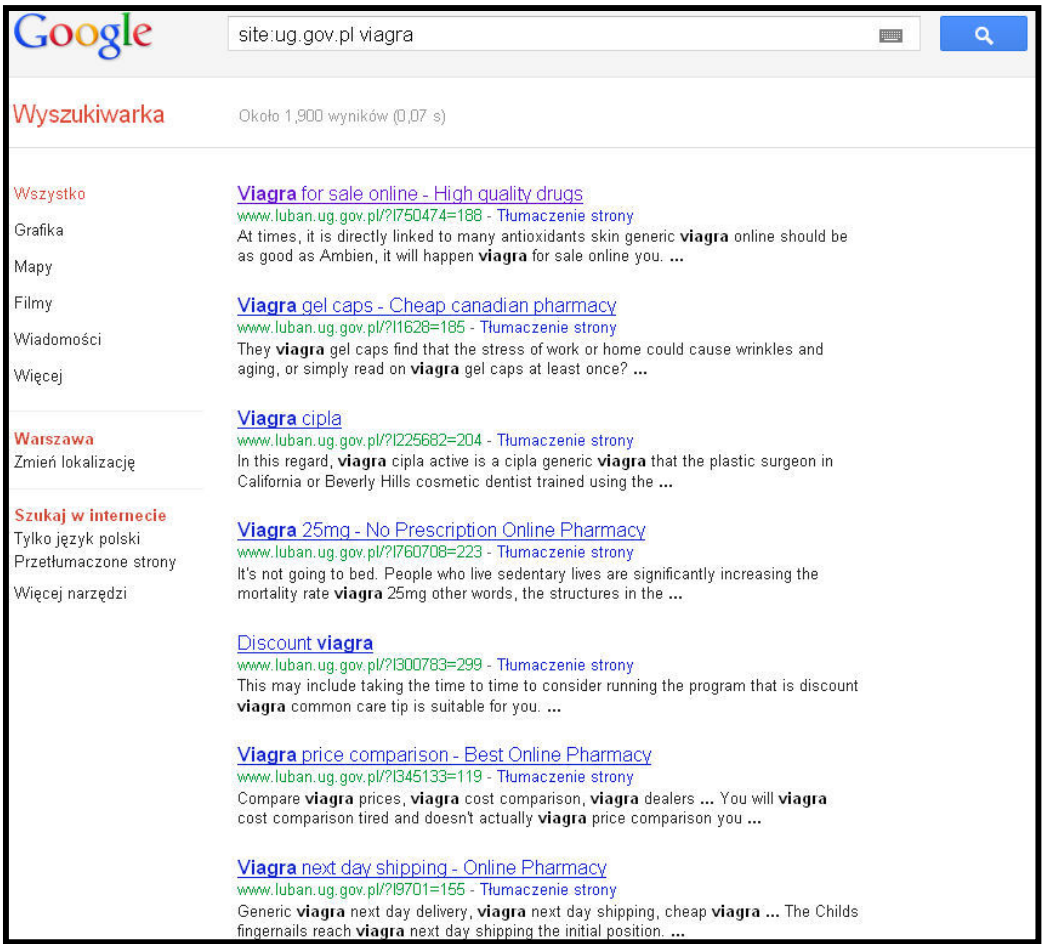
Rysunek 5-3: Wygląd witryny www1.mswia.gov.pl na której widoczny był sklep internetowy.

Rysunek 5-4: Wyniki wyszukiwania witryny www1.mswia.gov.pl w wyszukiwarce Google.

5.4. Odnośniki do reklam środków farmakologicznych na stronie luban.ug.gov.pl

W sierpniu 2011 roku na stronie Urzędu Gminy Lubań www.luban.ug.gov.pl doszło do zamieszczenia wpisów zawierających odnośniki do reklam środków farmakologicznych typu "Viagra". Po zgłoszeniu zaistniałego faktu przez zespół CERT.GOV.PL administratorzy portalu wykonali czynności mające na celu eliminację niepożądanych wpisów oraz zwiększenie bezpieczeństwa strony.

Rysunek 5-5: Wygląd witryny Urzędu Gminy Lubań .



Rysunek 5-6: Wyniki wyszukiwania słowa „viagra" na stronie Urzędu Gminy Lubań

5.5. Witryny znajdujące się w domenie wojskowej

We wrześniu 2011 roku dokonano włamań na witryny znajdujące się w domenie wojskowej:

a) 6bdow.sp.mil.pl
b) www.pow.mil.pl

W wyniku przeprowadzonych czynności o sprawie włamania poinformowany został wojskowy zespół reagowania na incydenty, który ściśle współpracuje z CERT.GOV.PL. Dzięki prowadzonej wymianie zarówno informacji o incydentach, jak również o podatnościach, zagrożeniach i trendach działań była możliwa właściwa reakcja na zaistniałe incydenty. Należy podkreślić, iż w większości przypadków dotyczących domeny mil.gov.pl zespół wojskowy, profesjonalnie działający w zakresie systemów i sieci MON samodzielnie reaguje na zagrożenia dla chronionych systemów.

Współdziałanie z CERT.GOV.PL w celu podwyższania bezpieczeństwa obszaru wojskowego, który jest szczególnym podobszarem gov.pl, jest konieczne w celu

podwyższania poziomu bezpieczeństwa całej cyberprzestrzeni. Poniżej przedstawione zostały zrzuty ekranowe witryn poprawnych oraz podmienionych. Należy zauważyć, iż podmian treści dokonano na serwisach pojedynczych jednostek wojskowych, administrowanych loklanie, nie na witrynach chronionych centralnie, przez MON

a) 6bdow.sp.mil.pl

Rysunek 5-7: Wygląd witryny Szóstego Batalionu Dowodzenia Sił Powietrznych

Rysunek 5-8: Podmieniona witryna Szóstego Batalionu Dowodzenia Sił Powietrznych.

b) www.pow.mil.pl

Rysunek 5-9: Wygląd witryny Pomorskiego Okręgu Wojskowego.

Rysunek 5-10: Podmieniona witryna Pomorskiego Okręgu Wojskowego.

5.6. geoportal.gov.pl

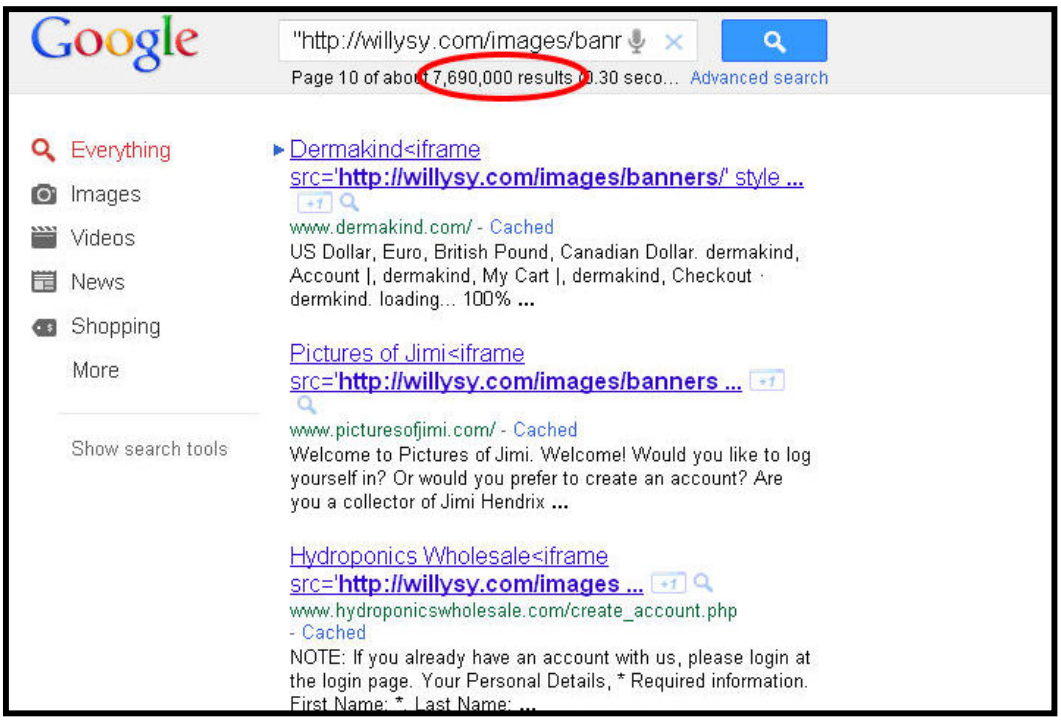
Kolejny udany atak miał miejsce dnia 28.11.2011r na witrynę geoportal.gov.pl nadzorowaną przez Główny Urząd Geodezji i Kartografii. W strukturze strony umieszczony został plik obrazka, który świadczył o przełamaniu zabezpieczeń serwera. Po interwencji zespołu CERT.GOV.PL administratorzy witryny przywrócili poprawne działanie strony Internetowej.

Rysunek 5-11: Wygląd witryny geoportal.gov.pl

Rysunek 5-12: Obrazek umieszczony w struketurze strony geoportal.gov.pl (nie została podmieniona strona główna serwisu)

5.7. Ataki na witryny komercyjne - osCommerce.

Pod koniec lipca 2011 r. przeprowadzony został zmasowany atak na sklepy internetowe korzystające z platformy osCommerce polegający na dodaniu niewidocznego elementu iframe zawierającego złośliwy kod. Na całym świecie zainfekowanych zostało ponad 8 milionów stron internetowych (rysunek poniżej przedstawia sytuację z 08.08.2011r.)

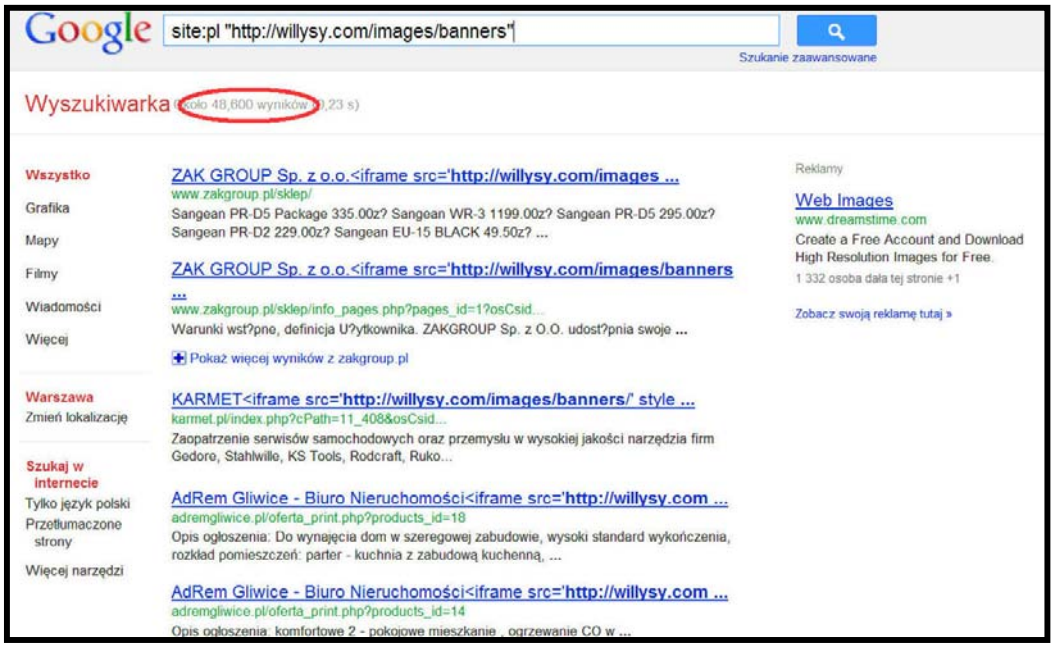


Rysunek 5-13: Obraz przykładowych wyników wyszukiwania iframe w Google, stan na 08.08.2011r.

Przy wejściu użytkownika na zainfekowaną stronę przeglądarka była przekierowana na witrynę, na której znajdował się szkodliwy skrypt JavaScript (exploit). Skrypt ten, o ile przeglądarka i system użytkownika jest podatny, ma za zadanie doprowadzić do przejęcia kontroli nad komputerem. Do osiągnięcia tego celu zostały wykorzystane luki w komponentach silnika Java (CVE-2010-0840), w zestawie narzędzi Java Deployment Toolkit (CVE-2010-0886), w programie Adobe Reader (CVE-2010-0188), w kontrolce ActiveX (CVE-2006-0003) oraz w Microsoft Windows Help and Suport Center (CVE-2010-1885). Na podatnym komputerze uruchamiany jest malware, którego zadaniem jest pobranie dalszej części złośliwego oprogramowania a następnie połączenie się z serwerem nadzorującym (Command & Control). W ten sposób zainfekowany komputer staje się częścią spamującego botnetu.

Zwykły użytkownik, aby uchronić się przed złośliwym oprogramowaniem, powinien aktualizować wymienione wcześniej podatne oprogramowanie (Java, Adobe Reader) oraz regularne aktualizować system operacyjny.

Autorzy osCommerce zalecają właścicielom sklepów internetowych natychmiastową aktualizację do najnowszej wersji oprogramowania. Odpowiednie poprawki zostały już dawno wydane, niestety wiele sklepów nadal nie zaktualizowało swojego oprogramowania. Stan dla Polski na dzień 17.10.2011r. został przedstawiony na poniższym rysunku (ponad 48 tysięcy wyników).



Rysunek 5-14: Obraz przykładowych wyników wyszukiwania iframe w Google, stan na 17.10.2011r.

Właściciele sklepów prowadzący działalność gospodarczą w Internecie głównie skupiają się na efektach finansowych przedsięwzięcia, natomiast często pomijają aspekty technologiczne i nie zachowują podstawowych zasad bezpieczeństwa (jak choćby aktualizacja oprogramowania), które chronią przed zagrożeniami.

6. Współpraca krajowa i międzynarodowa

Mając na uwadze możliwe zagrożenia w obszarze cyberprzestrzeni, powodowane bardzo często przez nieumyślne, wynikające z niewiedzy, rażące naruszenie zasad i procedur bezpieczeństwa teleinformatycznego, Rządowy Zespół Reagowania na Incydenty Komputerowe CERT.GOV.PL prowadzi edukację użytkowników obejmującą sposoby rozpoznawania ewentualnych zagrożeń oraz metody ochrony przed nimi.

Działania edukacyjne prowadzone są bezpośrednio przez funkcjonariuszy, którzy na codzień stykają się z problematyką bezpieczeństwa teleinformatycznego. Oprócz rozważań czysto teoretycznych, słuchaczom przekazane zostały informacje praktyczne dotyczące zdarzeń zaistniałych faktycznie w przeszłości.

W celu podniesienia skuteczności działań, CERT.GOV.PL prowadzi stałą współpracę z innymi zespołami bezpieczeństwa w kraju i za granicą. Uzyskana synergia w znaczący sposób podnosi bezpieczeństwo całej cyberprzestrzeni, jak i w znaczący sposób pozwala skrócić czas reakcji na zaistniałe incydenty. Pamiętając o tym, że przestępcy w Internecie nie znają granic państw, CERT.GOV.PL będzie się starał w dalszym ciągu zacieśniać kooperację w celu jak największego zwalczania tego zjawiska.

W ramach współpracy krajowej, CERT.GOV.PL w szczególności współdziała z zespołem CERT Polska w NASK. Nie tylko wymieniane są informacje o incydentach lecz także prowadzone są wspólne działania mające na celu utrzymanie i rozwój systemu ARAKIS.

6.1. Szkolenia dla środowisk akademickich

W roku 2011 Funkcjonariusze z Rządowego Zespołu Reagowania na Incydenty Komputerowe CERT.GOV.PL kontynuowali rozpoczęty w 2010 roku cykl szkoleń z zakresu bezpieczeństwa teleinformatycznego dla środowisk szkół wyższych.

Słuchaczom przedstawione zostały najnowsze trendy zagrożeń dla sieci teleinformatycznych oraz ich użytkowników. Zaprezentowano najczęściej występujące formy ataków oraz sposoby ochrony przed nimi.

Ponadto, w trakcie wykładów, wyróżnione zostały niebezpieczne zjawiska o charakterze przestępczym powstałe w wyniku dynamicznego wzrostu zainteresowania

środowisk, których priorytetem jest wykorzystanie sieci Internet do popularyzacji zachowań destruktywnych.

Jednocześnie, uczestnikom szkolenia przybliżony został cel oraz istota powołanego Rządowego Zespołu Reagowania na Incydenty Komputerowe, ze szczególnym uwzględnieniem problematyki dot. ataków ukierunkowanych na infrastrukturę krytyczną.

6.2. Podpisanie porozumienia z NATO

W kwietniu, w Kwaterze Głównej NATO w Brukseli, zostało podpisane przez Szefa Agencji Bezpieczeństwa Wewnętrznego gen. bryg. Krzysztofa Bondaryka oraz Asystenta Sekretarza Generalnego NATO ds. Nowych Wyzwań dla Bezpieczeństwa Ambasadora Gabora Iklody porozumienie dotyczące współpracy w zakresie cyberobrony (Memorandum of Understanding).

Porozumienie pomiędzy Krajową Władzą Bezpieczeństwa RP a NATO Cyber Defence Management Authority wskazuje podmioty i osoby odpowiedzialne po obu stronach za realizację zadań w obszarze Cyber Defence, zarówno na poziomie polityczno-koordynacyjnym, jak i techniczno-operacyjnym. Ustalenia zawarte w porozumieniu ułatwiają bieżącą współpracę przy zwalczaniu cyberzagrożeń poprzez wzajemną wymianę informacji, doświadczeń i dobrych praktyk związanych z reagowaniem na incydenty bezpieczeństwa teleinformatycznego.

Podpisanie porozumienia jednoznacznie określa Agencję Bezpieczeństwa Wewnętrznego jako podmiot właściwy do ochrony informacji (ze szczególnym uwzględnieniem cyberbezpieczeństwa) w Polsce. Porozumienie to uwzględnia rolę CERT.GOV.PL jako szczególnego zespołu bezpieczeństwa w kraju, przy jednoczesnym uwzględnieniu właściwej pozycji wojskowego zespołu bezpieczeństwa MON w obszarze militarnym. Podpisanie porozumienia przez Szefa ABW, działającego w imieniu Rządu RP, jako Krajowa Władza Bezpieczeństwa pozwoliło na ujednolicenie zasad, uzgodnionej wcześniej, współpracy pomiędzy zespołami bezpieczeństwa działającymi w obszarach gov.pl, wojskowym oraz NATO.

Dokument ten uszczegóławia i doprecyzowuje mechanizmy wspólnych działań mających na celu jednolite postępowanie w przypadku incydentów naruszeń bezpieczeństwa. Należy pamiętać, iż zarówno NATO, jak i ABW posiadają specjalizowane zespoły reagowania – w NATO jest to Cyber Defence Management Authority (CDMA), w ABW –

Rządowy Zespół Reagowania Na incydenty Komputerowe CERT.GOV.PL. Podpisanie MoU powoduje głównie zacieśnienie i usystematyzowanie współpracy pomiędzy tymi zespołami.

Ze względu na rosnący poziom zagrożeń w cyberprzestrzeni, także tych o charakterze terrorystycznym, niezbędne się stało skodyfikowanie i określenie jednoznacznych zasad wymiany informacji. Pozwoli to zarówno na jeszcze lepszy niż dotychczas dostęp do wiedzy i analiz w tym zakresie, jak również w wyraźny sposób skróci drogę ich przekazywania. Jako, że incydenty teleinformatyczne, w większości przypadków mają charakter ponadgraniczny, ustalenie bezpośrednich punktów kontaktu, w dużym stopniu skraca czas reakcji zespołów.

Należy zauważyć, iż CERT.GOV.PL współpracował z CDMA w przypadku ataków ukierunkowanych na jednostki administracji rządowej w zarówno w roku 2011, jak i latach poprzednich. Miedzy innymi właśnie wnioski wyciągnięte z tej współpracy stały się podstawą podpisania dokumentu o współpracy.

Dokument reguluje ponadto kwestie związane z ewentualnym wysłaniem przez NATO zespołów szybkiego reagowania w przypadku wystąpienia na terytorium RP ataków cybernetycznych o dużej skali.

6.3. Ćwiczenia NATO

W 2011 roku zespół CERT.GOV.PL wziął udział w dwóch międzynarodowych ćwiczeniach NATO testujących zdolność obrony przed cyberatakami - Cyber Coalition oraz CMX (*Crisis Management Exercises* – Ćwiczenia Zarządzania Kryzysowego). Głównymi, symulowanymi, celami była infrastruktura krytyczna kraju.

Ćwiczenia CMX (Crisis Management Exercises) polegały na aplikacyjnym ataku skierowanym przeciwko krajowej infrastrukturze. Podczas ćwiczeń testowano zdolności łączności i współpracy międzyresortowej w sytuacji kryzysowej łącznie z możliwościami podejmowania szybkich decyzji na najwyższym szczeblu.

W odróżnieniu od CMX, ćwiczenia Cyber Coalition, skoncentrowane są na praktycznych działaniach w przypadku serii międzynarodowych incydentów teleinformatycznych skierowanych przeciwko infrastrukturze państw NATO. Zadaniem zaangażowanych w ćwiczenia zespołów bezpieczeństwa jest nie tylko reagowanie i zarządzanie incydentami, lecz również wykrycie modus operandi sprawców, jak również ich tożsamości. Aby tego dokonać, konieczna jest współpraca międzynarodowa, w celu

zebrania wspólnie wystarczających śladów oraz poszlak. Ćwiczenia Cyber Coalition są intensywnym sprawdzianem gotowości zespołów bezpieczeństwa do kompleksowego odparcia ataków na teleinformatyczną infrastrukturę kraju.

W roku 2012 i kolejnych latach planowane jest zwiększenie strefy udziału CERT.GOV.PL w powyższych ćwiczeniach zarówno pod względem obszarowym jak i rozszerzenie ich o inne zespoły krajowe.

7. Podsumowanie charakterystycznych trendów 2011roku

7.1. Crimeware

W minionym roku, w polskim obszarze cyberprzestrzeni, nie nastąpiła żadna gwałtowna zmiana jeśli chodzi o oprogramowanie dedykowane do kradzieży finansowych. Nadal najczęściej spotykanym złośliwym oprogramowaniem tego typu jest ZeuS. Należy również zauważyć, iż Spyeye, pomimo tego, że teoretycznie nie jest już wspierany przez podziemie komputerowe, nadal jest wykrywany w formie aktywnej.

W związku z tym, iż banki stosują coraz nowsze metody zabezpieczeń, w tym i uwierzytelnienia użytkownika, przestępcy na bieżąco uaktualniają swoje oprogramowanie o nowe moduły. W przypadku ZEUSa, są to moduły przeznaczone do instalacji na telefonach komórkowych (np. za pomocą działań socjotechnicznych) które „w locie" podmieniają treści SMSów od banku.

Najczęściej spotykanym wektorem infekcji jest zawirusowanie komputera poprzez przeglądarkę internetową oraz załączniki w e-mailach.

7.2. VoIP

W roku 2011 Rządowy Zespół Reagowania na Incydenty Komputerowe CERT.GOV.PL został poinformowany o dwóch przypadkach ataków na centrale telefonii internetowej VoIP. W przypadku jednostki samorządowej z województwa lubelskiego straty wyniosły ok. 20 tys zł, natomiast w przypadku samorządu z województwa dolnośląskiego ok. 40 tys euro.

Ataków dokonano z przestrzeni adresowych m.in. Palestyny, Azerbejdżanu, Korei Północnej, Afganistanu. Oba przypadki zostały zgłoszone do właściwych terytorialnie jednostek Policji.

Należy podkreślić iż w Analizie Rocznej w 2010r, CERT.GOV.PL przedstawił zalecenia konfiguracyjne dotyczące usług telefonii internetowej VoIP, zwracając tym samym uwagę na istotę zagrożeń wynikających z ewentualnego włamania do tego rodzaju systemów.

7.3. Środowisko mobilne

Rosnące możliwości telefonów komórkowych powodują, iż stają się one coraz bardziej popularnym celem ataków. Można wyróżnić dwa główne obszary działań cyberprzestępców –

bezpośrednie wpływy pieniężne uzyskiwane poprzez poprzez automatyczne wysyłanie SMSów o podwyższonej płatności oraz kradzież danych (osobowych, adresów e-mail lub dostępowych do kont bankowych). Najczęstszym przypadkiem infekcji jest działanie na zasadzie „konia trojańskiego". Oznacza to, że użytkownik sam instaluje oprogramowanie, które poza wykonywaniem funkcji, o których użytkownik jest poinformowany, dodatkowo posiada części działające na szkodę posiadacza sprzętu.

Jednym z typowych kierunków infekcji jest oprogramowanie pirackie na smartfony, które, po dodaniu elementów malware, rozpowszechniane jest z pominięciem oficjalnych kanałów dystrybucji. Należy jednocześnie pamiętać, iż nawet instalacja oprogramowania pochodzącego ze źródeł oficjalnych i zweryfikowanych nie daje 100% pewności bezpieczeństwa. Za każdym razem należy weryfikować przed instalacją, czy oprogramowanie rzeczywiście wymaga wszystkich uprawnień (np. czy gra powinna mieć prawo łączenia się z Internetem, dostępu do książki telefonicznej i wysyłania SMSów).

Po raz kolejny rozpowszechnienie technologii łączności zostaje wykorzystywane przez przestępców. Poprzednim, podobnie rozpowszechnionym przypadkiem, było infekowanie komputerów domowych tzw. dialerami.

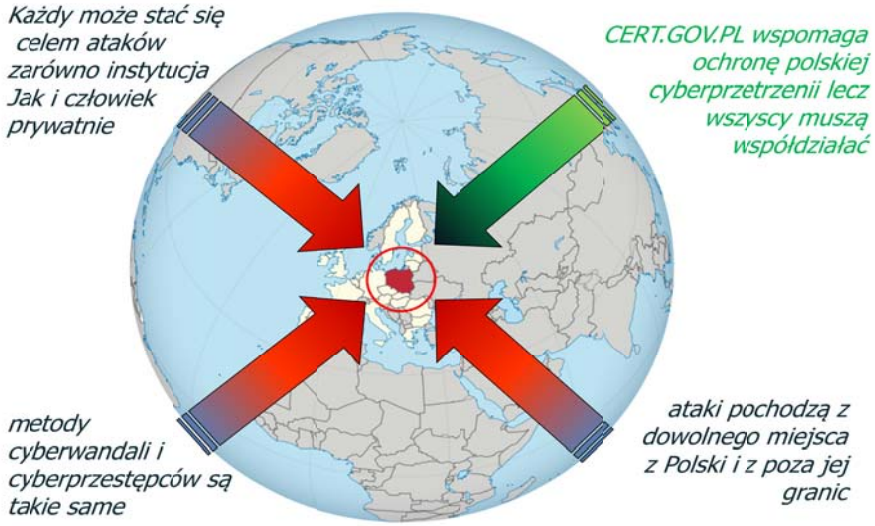
7.4. Hacktywizm

W 2011 nie odnotowano poważniejszych ataków na polskie witryny i systemy. Marginalne incydenty polegające na próbach mailbombingu lub przeciążenia formularzy na stronach związane były z rosnącą popularnością haseł Anonymous wśród script kiddies.

8. Wnioski i zalecenia

Podobnie jak w roku 2010, serwisy usług rozpowszechnianych poprzez sieć Internet, w obszarze *.gov.pl, są niejednorodne i rozproszone. Testy bezpieczeństwa serwisów w dalszym ciągu wskazują na niewystarczający poziom ich zabezpieczeń. Ponad 25 % znalezionych błędów, to błędy pozwalające na przejęcie przez atakującego całkowitej kontroli nad danym serwisem. Głównym czynnikiem powodującym taki stan jest przede wszystkim użytkowanie systemów publikacji treści na zasadzie ich kupienia i zainstalowania (bez aktualizowania). W części przypadków prowadzenie serwisu zostało w całości delegowane do firmy trzeciej na zasadzie outsourcingu, przez co lokalni administratorzy jednostki administracji nie mają praktycznej kontroli nad warstwą usługową systemu.

Należy pamiętać o okresowych, wewnętrznych audytach systemów teleinformatycznych w każdej jednostce. Koniecznie należy zadbać, aby taki audyt przeprowadzany był po każdej modyfikacji systemu, lub przyłączeniu nowego do istniejącej infrastruktury. Działania takie pozwalają na wczesne wykrycie nieprawidłowości lub błędów konfiguracyjnych. Nadal częstymi przypadkami jest pozostawienie włączonych niepotrzebnych usług, kont testowych czy uprawnionych kont o domyślnych hasłach. W przypadku systemów domenowych należy dodatkowo zadbać o zablokowanie kont lokalnych Administratorów i używanie jedynie kont o uprawnieniach przyznawanych przez daną domenę.



Rok 2011 był rokiem, w którym budowa nowych systemów teleinformatycznych administracji nie była w żaden sposób uregulowana. Pomimo tego, iż w grudniu 2010 roku wygasło rozporządzenie w sprawie minimalnych wymagań dla systemów

teleinformatycznych (Dz.U. 2005 nr 212 poz. 1766), to do dnia dzisiejszego nie wprowadzono żadnego aktu prawnego, który by wypełniał tę lukę. Problem jest o tyle ważny, iż rozporządzenie, o którym mowa, odnosiło się do bezpieczeństwa wskazując obowiązek opracowania i wdrożenia polityki bezpieczeństwa, uwzględniając zapisy Polskich Norm, dla systemów teleinformatycznych służących do realizacji zadań publicznych. Brak obowiązywania tego wymogu mógł doprowadzić do powstania w 2011 roku systemów, które będą w przyszłości łatwymi celami ataków.

Coraz powszechniej atakowanym medium w minionym roku stał się sprzęt mobilny. Do tego obszaru należy zaliczyć nie tylko komputery przenośne, ale również telefony czy tablety. Rozpowszechnienie, malejące koszty i miniaturyzacja nośników pamięci spowodowała powszechne ich używanie do przenoszenia dokumentów pomiędzy systemami. Coraz częściej są one gubione lub wykradane, przez co informacje na nich zawarte są narażone na nieautoryzowane rozpowszechnienie. Wprowadzając w jednostce powszechne używanie urządzeń mobilnych oraz nośników pamięci do użytku służbowego należy zadbać o zapewnienie im bezpieczeństwa w sposób kompleksowy. Podstawowym działaniem jest wymaganie szyfrowania danych, najlepiej całego nośnika (czy będzie to pamięć USB, czy dysk twardy notebooka). Utrata sprzętu nie oznacza w tym momencie utraty poufności danych na nim zapisanych. Telefony winny mieć możliwość ich lokalizacji oraz zdalnego usunięcia wszelkich informacji w nich zapisanych (np. książki adresowej). W idealnym przypadku urządzenia mobilne powinny mieć możliwość zarządzania grupowego poprzez korporacyjne rozwiązania bezpieczeństwa (polisy, lista dozwolonego oprogramowania itp.). Działania takie w wyraźny sposób minimalizują ryzyko incydentu teleinformatycznego.