Agencja Bezpieczeństwa Wewnętrznego

Raport kwartalny CERT.GOV.PL

styczeń – marzec 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.

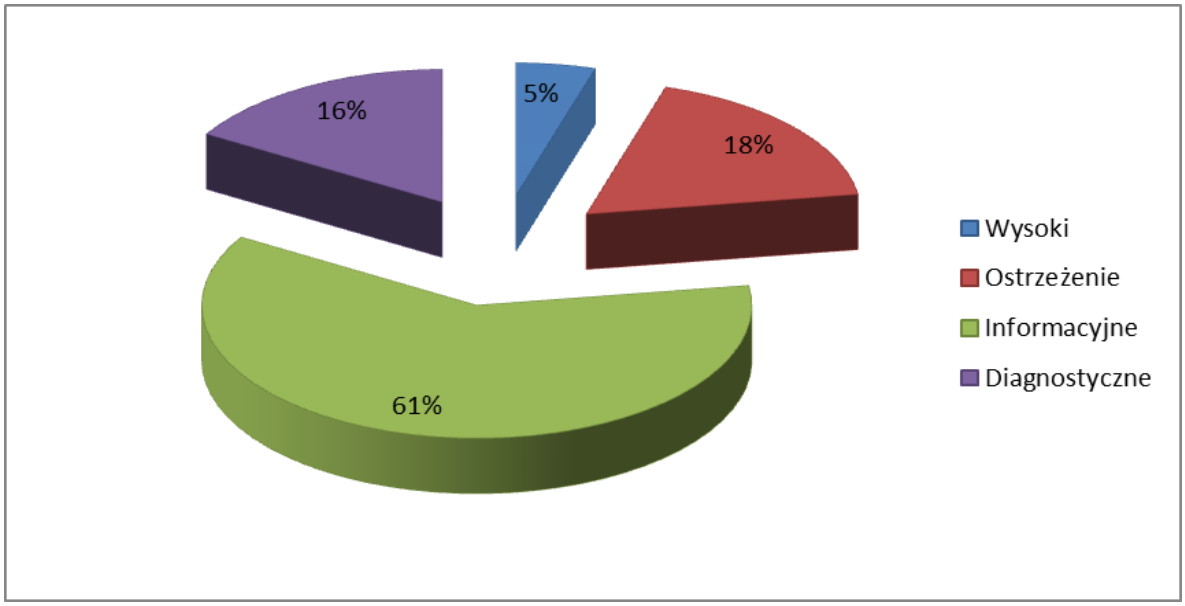
Dane kontaktowe:

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

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

2. Statystyki systemu ARAKIS-GOV[1]

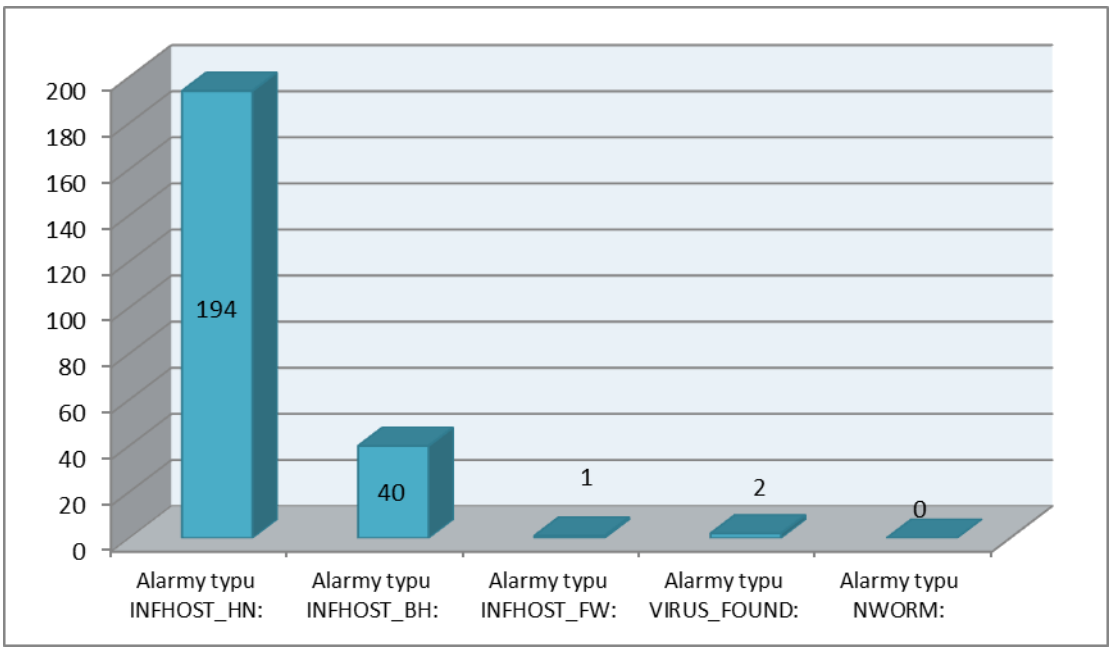
W pierwszym kwartale 2011 roku zdecydowaną większość stanowiły alarmy informacyjne, które stanowiły aż 61 procent wszystkich zarejestrowanych przez system ARAKIS-GOV. Alarmy o priorytecie średnim stanowiły 18%, natomiast alarmy diagnostyczne 16%. System zgłosił najmniej alarmów o priorytecie wysokim – 237 (dwukrotnie więcej alarmów niż w IV kwartale 2010 roku), co stanowiło 5% wszystkich alarmów.



Rysunek 1 – Procentowy rozkład ważności alarmów.

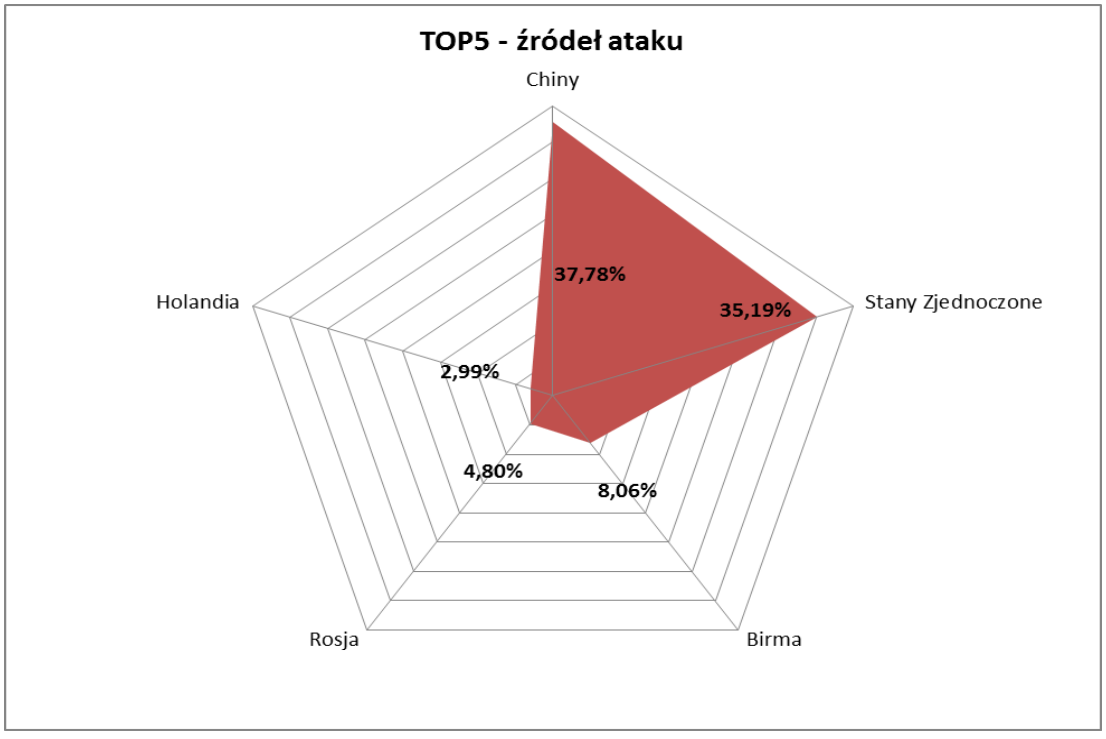
Wśród alarmów o priorytecie wysokim zaobserwowano 194 alarmów typu INFHOST_HN[2], 40 alarmów typu INFHOST_BH[3], 2 alarmy typu VIRUS_FOUND[4], 1 alarm typu INFHOST_FW[5] i brak alarmów typu NWORM[6].

[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 VIRUS_FOUND oznacza wykrycie infekcji wirusowej w sieci wewnętrznej chronionej instytucji. Alarm ten generowany jest na podstawie informacji pochodzących ze skanerów antywirusowych serwerów pocztowych
[5] Alarm INFHOST_FW oznacza potencjalne wykrycie zainfekowanego hosta w sieci wewnętrznej instytucji chronionej systemem ARAKIS-GOV. Alarm ten generowany jest na podstawie analizy logów systemów zaporowych.
[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.

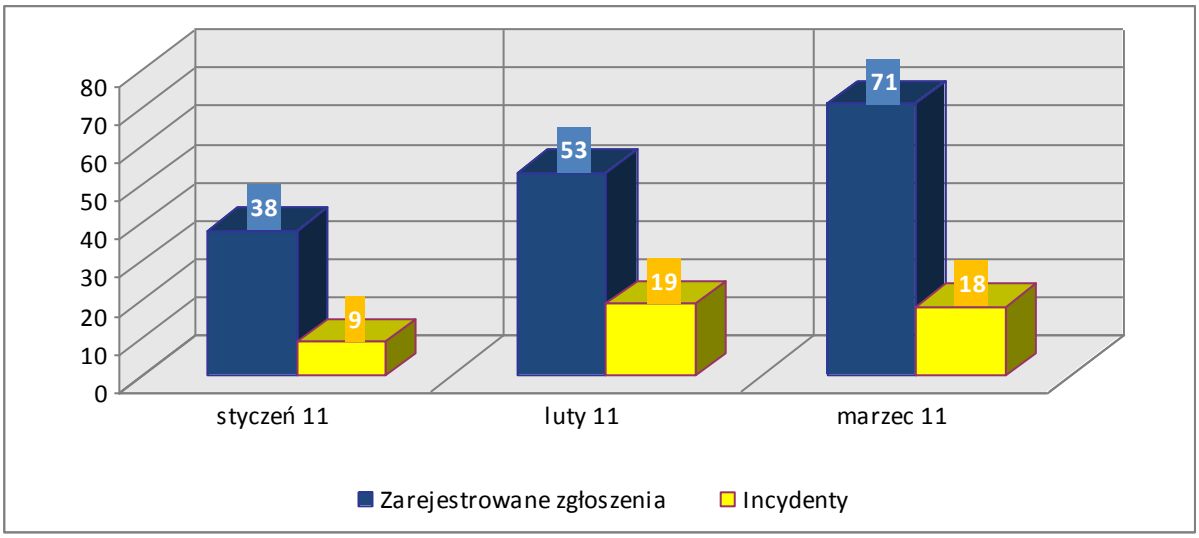
W wyniku analizy zarejestrowanych połączeń stwierdzono, iż w większości źródłem ataku były sieci komputerowe przypisane do Chin, Stanów Zjednoczonych, Birmy, Rosji oraz Holandii. Jednakże mając na uwadze specyfikę protokołu TCP/IP, nie można bezpośrednio łączyć źródła pochodzenia pakietów z faktyczną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

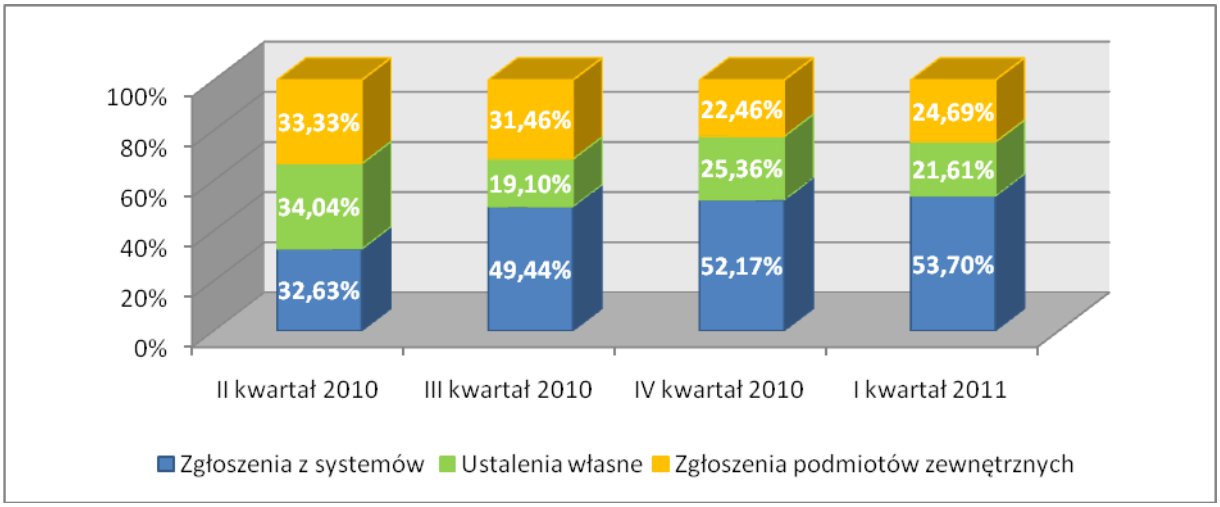
3. Statystyki incydentów

W pierwszym kwartale 2011 roku do zespołu CERT.GOV.PL wpłynęły 162 zgłoszenia, przy czym tylko 46 z nich zostały zakwalifikowane jako faktyczne incydenty.



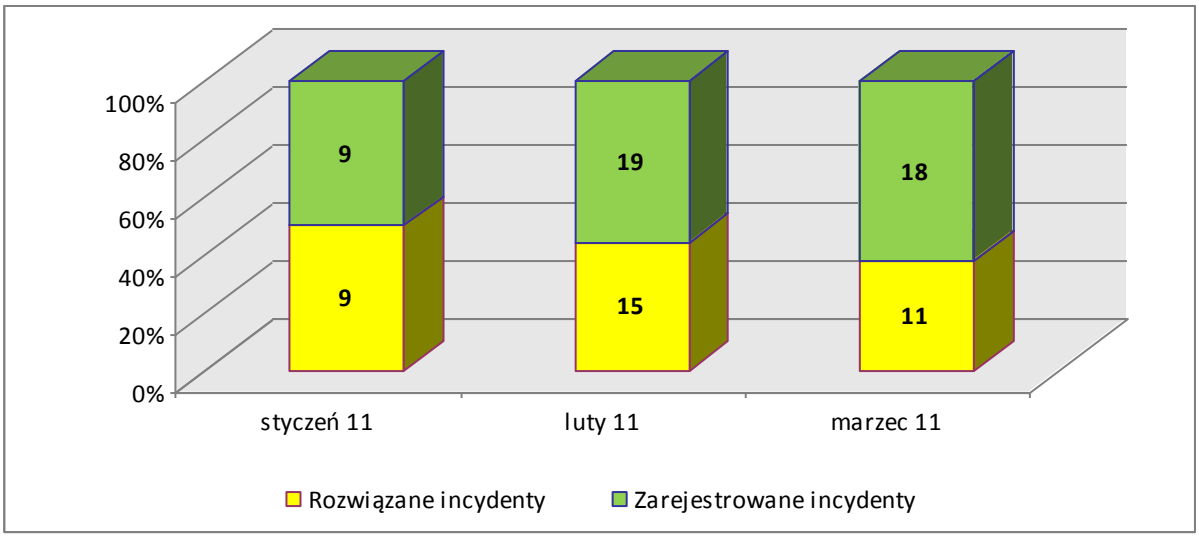
Rysunek 4 - Liczba zgłoszeń oraz faktycznych incydentów w poszczególnych miesiącach pierwszego kwartału 2011

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



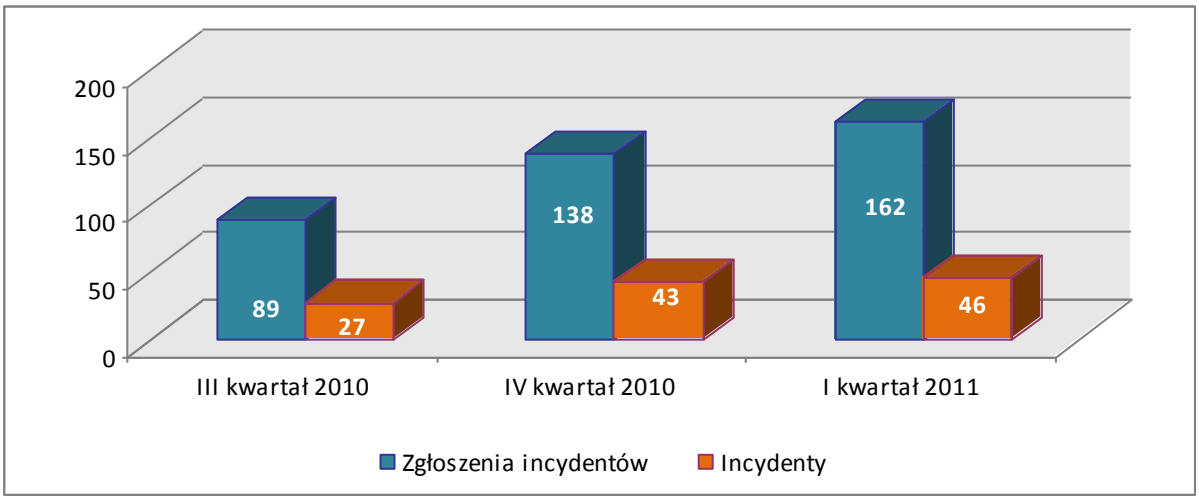
Rysunek 5 - Źródła zgłoszeń incydentów

Rozkład miesięczny incydentów zarejestrowanych i incydentów, które zostały rozwiązane, przedstawia się następująco: w styczniu 2011 zarejestrowano 9 incydentów i wszystkie je rozwiązano, w lutym 2011 odnotowano 19 incydentów, z czego 15 zostało rozwiązanych, natomiast w marcu 2011 przyjęto do realizacji 18 incydentów, z czego 11 jeszcze w tym samym miesiącu zostało zakończonych. Pozostałe incydenty są w trakcie dalszej analizy.



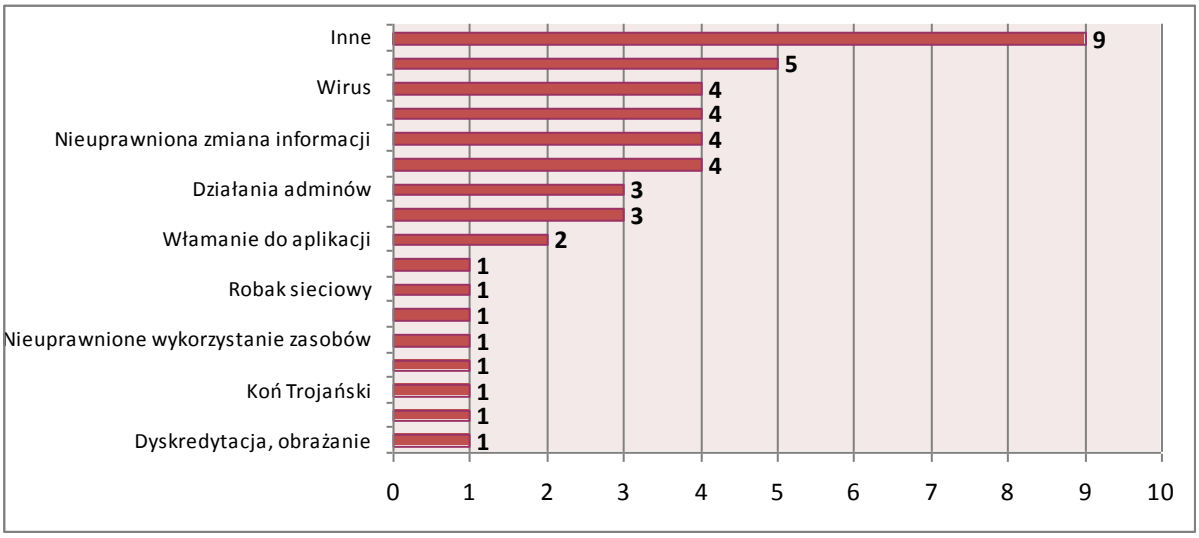
Rysunek 6 - Porównanie liczby incydentów otwartych i zamkniętych w poszczególnych miesiącach drugiego kwartału

Poniższy wykres obrazuje aktualnie utrzymującą się tendencję wzrostową ilości zgłoszeń oraz faktycznych incydentów od III kwartału 2010 roku do I kwartału 2011 roku.



Rysunek 7 – Porównanie ilości zgłoszeń incydentów i incydentów w ostatnich trzech kwartałach

Podział zarejestrowanych incydentów na kategorie przedstawia się następująco:



Rysunek 8 - Statystyka incydentów z podziałem na kategorie

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

- W styczniu do zespołu CERT.GOV.PL wpłynęło zgłoszenie dotyczące próby przełamania zabezpieczeń systemu informatycznego jednej z instytucji administracji państwowej. Szczegółowa analiza powyższego zdarzenia wykazała, że integralność systemu nie została naruszona. Ustalono ponadto, że atak przeprowadzony został z adresu IP zlokalizowanego na terytorium Rumunii. Zalecono zaatakowanemu podmiotowi dokonanie aktualizacji do najnowszej wersji oprogramowania oraz ponowną weryfikacje złożoności haseł.
- W lutym dokonano podmiany zawartości witryny znajdującej się w domenie mil.pl. Obsługa incydentu przekazana została do Wojskowego Biura Bezpieczeństwa Łączności i Informatyki MON, zgodnie z kompetencjami.
- W tym miesiącu zespół CERT.GOV.PL zlokalizował także błędy typu SQL Injection na witrynach w domenie .gov.pl. Mając na uwadze fakt, że wykryte luki umożliwiały nieautoryzowany, bezpośredni dostęp do silnika baz danych, groziło to przejęciem kontroli nad serwerem bazodanowym. Poinformowano administratorów stron, którzy wprowadzili niezbędne zabezpieczenia chroniące przed powyższym zagrożeniem.

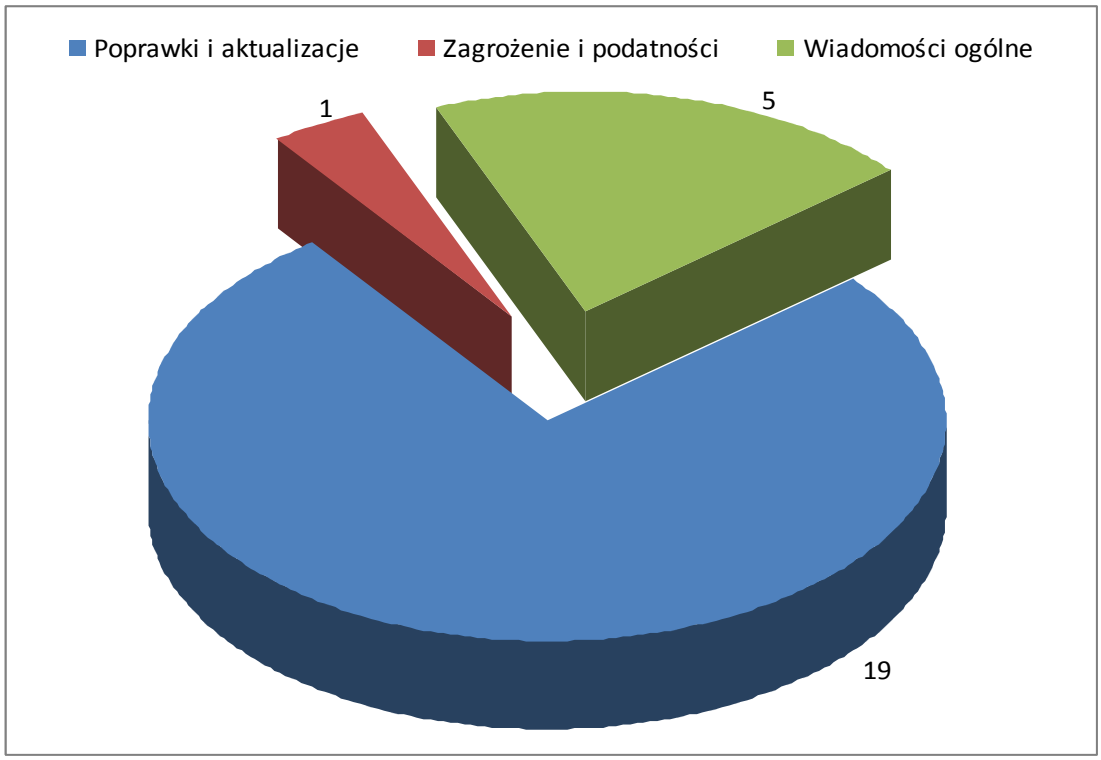
- W drugiej połowie lutego zespół CERT.GOV.PL otrzymał informację o kompromitacji komputera w jednej z instytucji administracji państwowej. Doszło do infekcji, w której wyniku nastąpiła masowa próba nieautoryzowanego logowania na inne konta w sieci wewnętrznej. Zainfekowana maszyna inicjująca połączenia została odpowiednio zabezpieczona, a następnie ponownie przyłączona do sieci urzędu. Zespół CERT.GOV.PL w celach poprawy bezpieczeństwa zalecił zmianę haseł dostępowych.
- W marcu zespół CERT.GOV.PL uzyskał informacje o włamaniu na stronę jednego z Urzędów Wojewódzkich. Atak dotyczył podmiany strony w części, na której umieszczane są relacje z aktualnych wydarzeń. Administratorzy o zaistniałym zdarzeniu zostali niezwłocznie poinformowani.
- W marcu doszło także do podmiany strony jednej z Komend Powiatowych Policji. Tak jak w powyższym przypadku poinformowano administratorów o zaistniałym fakcie w celu zabezpieczenia witryny.

4. Istotne podatności, zagrożenia i biuletyny zabezpieczeń

Witryna http://www.cert.gov.pl jest źródłem specjalistycznych danych związanych z bezpieczeństwem teleinformatycznym. Publikowane są tam między innymi aktualne informacje o istotnych zagrożeń, 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 pierwszym kwartale 2011 roku na witrynie www.cert.gov.pl dodano:

- 19 publikacji w kategorii „Poprawki i aktualizacje”,
- 1 publikację w kategorii „Zagrożenia i podatności”,
- 5 publikacji w kategorii „Wiadomości ogólne”.



Rysunek 9 - Procentowy rozkład publikacji na witrynie www.cert.gov.pl

Najistotniejsze publikacje dotyczące zagrożeń w pierwszym kwartale 2011 roku dotyczyły:

- **Comiesięcznych biuletynów bezpieczeństwa firmy Microsoft**

Styczniowy Biuletyn Bezpieczeństwa:

Styczniowy Biuletyn Bezpieczeństwa informował o usunięciu dwóch błędów. Otrzymały one status „krytyczny" i „ważny"

1. MS11-002 – biuletyn dotyczący luki w zabezpieczeniach składników Microsoft Data Access Components - krytyczny
2. MS11-001 – biuletyn dotyczący podatności aplikacji Windows Backup Manager – ważny

Lutowy Biuletyn Bezpieczeństwa:

Lutowy Biuletyn Bezpieczeństwa informował o wydaniu dwunastu aktualizacji. Trzy oznaczono jako „krytyczne", pozostałe zostały sklasyfikowane jako „ważne".

1. MS11-003 - biuletyn dotyczący podatności w programie Internet Explorer- krytyczny
2. MS11-006 - biuletyn dotyczący podatności w zabezpieczeniach jądra systemu Windows Graphics Processing - krytyczny
3. MS11-007 – biuletyn dotyczący aktualizacji zabezpieczeń sterownika OpenType Compact Font Format (CFF) w systemie Windows - krytyczny
4. MS11-004 – biuletyn dotyczący luki w zabezpieczeniach programu Microsoft Internet Information Services (IIS) – ważny
5. MS11-005 – biuletyn dotyczący luki w usłudze Active Direktory - ważny
6. MS11-008 – biuletyn dotyczący podatności w programie Microsoft Office Visio - ważny
7. MS11-009 – biuletyn dotyczący luki w JScript i VBScript - ważny
8. MS11-010 – biuletyn dotyczący podatności w Windows XP i Windows Server 2003 - ważny
9. MS11-011 –biuletyn dotyczący luki w zabezpieczeniach sterowników trybu jądra systemu Windows – ważny

10. MS11-012 – biuletyn dotyczący luki w zabezpieczeniach sterowników trybu jądra systemu Windows - ważny
11. MS11-013 - biuletyn dotyczący luki w zabezpieczeniach protokołu Kerberos – ważny
12. MS11-014 –biuletyn dotyczący podatności w zabezpieczeniach usługi podsystemu lokalnego uwierzytelniania zabezpieczeń (LSAS) - ważny

Marcowy Biuletyn Bezpieczeństwa:

Marcowy biuletyn bezpieczeństwa informował o wykryciu oraz usunięciu trzech błędów występujących w produktach Microsoft. Jedna otrzymała status „krytyczny", pozostałe dwie zostały sklasyfikowane jako „ważne".

1. MS11-015 - biuletyn dotyczący luki w pakiecie filtrów DirectShow oraz podatności w Windows Media Player i Windows Media Center - krytyczny
2. MS11-016 – biuletyn dotyczący luki w zabezpieczeniach Microsoft Groove - ważny
3. MS11-017 – biuletyn dotyczący luki w zabezpieczeniach klienta pulpitu zdalnego – ważny

- **Biuletynów bezpieczeństwa dla produktów Adobe**

Rządowy Zespół Reagowania na Incydenty Komputerowe informował o:

1. Biuletynie bezpieczeństwa Adobe APSA11-01 dotyczącym wykrycia poważnych luk w programach Adobe Flash Player, Reader i Acrobat. Wykryte podatności mogą być przyczyną awarii i umożliwić atakującemu przejęcie kontroli nad zaatakowanym systemem. Możliwe jest, iż luka ta może być wykorzystywana w atakach ukierunkowanych za pomocą Flash wbudowanego w Microsoft Excel dostarczonego jako załącznik e-mail.
2. Biuletynie bezpieczeństwa Adobe Security Advisory APSB11-05 dotyczącym wykrycia w programie Flash Player wielu luk w zabezpieczeniach. Wykorzystanie tych podatności może pozwolić atakującemu na przeprowadzenie ataku typu odmowa usługi (denial-of-service) lub wykonanie dowolnego kodu.
3. Biuletynie bezpieczeństwa Adobe APSB11-06dotyczącym wykrytej podatności w bibliotece authplay.dll. Wykorzystanie luki może pozwolić atakującemu na wykonanie dowolnego kodu.

- **Poprawek do oprogramowania zarządzającego sieciami komputerowymi CISCO**

Zespół CERT.GOV.PL informował na swojej stronie m.in. o podatnościach w następujących produktach firmy CISCO.

1. Poradnik bezpieczeństwa cisco-sa-20110223-asa - opisuje podatności w Cisco ASA 5500 Series Adaptive Security Appliances, które pozwalają atakującemu na wykonanie ataku denial-of-service oraz umożliwiają nieautoryzowany dostęp do systemu plików.
2. Poradnik bezpieczeństwa cisco-sa-20110223-fwsm - dotyczy urządzenia Cisco Firewall Services Module dla przełączników Cisco Catalyst 6500 i routerów serii Cisco 7600. Wykorzystywanie podatności przez atakującego pozwala na wykonanie ataku denial-of-service.
3. Poradnik bezpieczeństwa cisco-sa-20110223-telepresence-cts - opisuje podatności w urządzeniu Cisco TelePresence Endpoint Devices. Wykorzystanie luk pozwala na wykonanie ataku denial-of-service oraz przejęcia kontroli nad podatnym urządzeniem.
4. Poradnik bezpieczeństwa cisco-sa-20110223-telepresence-ctrs - dotyczy podatności w urządzeniu Cisco TelePresence Recording Server. Wykorzystanie luk może pozwolić atakującemu na zdalne wykonanie kodu w celu przejęcia kontroli nad zaatakowanym urządzeniem.
5. Poradnik bezpieczeństwa cisco-sa-20110223-telepresence-ctsman - opisuje luki w oprogramowaniu Cisco TelePresence Manager. Wykorzystanie tych błędów może pozwolić na ominięcie ograniczeń bezpieczeństwa oraz przejęcie kontroli nad podatnym urządzeniem.
6. Poradnik bezpieczeństwa cisco-sa-20110223-telepresence-ctms - opisuje wiele podatności w przełączniku Cisco TelePresence Multipoint Switch. Błędy mogą pozwolić na zdalne wykonanie kodu, przejęcie kontroli nad systemem lub urządzeniem oraz przeprowadzenie ataku denial-of-service.

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

Zespół CERT.GOV.PL zamieścił na stronie informacje na temat pakietu aktualizacyjnego dla systemu operacyjnego Mac OS X v10.6.7 łatającego wiele luk

w zabezpieczeniach. Wykorzystanie tych podatności może pozwolić atakującemu na wykonanie dowolnego kodu, możliwe jest przeprowadzenie ataku typu odmowa usługi (denial-of-service) lub uzyskanie dostępu do poufnych informacji użytkownika.

- **Wykrytych podatnościach i poprawkach dla produktów VMware**

Na stronie http://www.cert.gov.pl opublikowano informacje na temat wypuszczenia przez VMware aktualizacji dotyczącej klienta VMware instalowanego na Windows 7. Błąd uniemożliwiał połączenia pomiędzy klientem View Client a View Connection Server po dokonaniu aktualizacji systemu Windows 7 poprawkami numer 2467023 lub 2482017.

- **Poprawkach dla użytkowników przeglądarki Chrome**

Zespół CERT.GOV.PL zamieścił na stronie informacje dotyczące wydania przez Google nowej wersji przeglądarki internetowej Chrome. Naprawiono w niej 19 luk występujących w zabezpieczeniach.

- **Krytycznych poprawkach dla produktów Oracle**

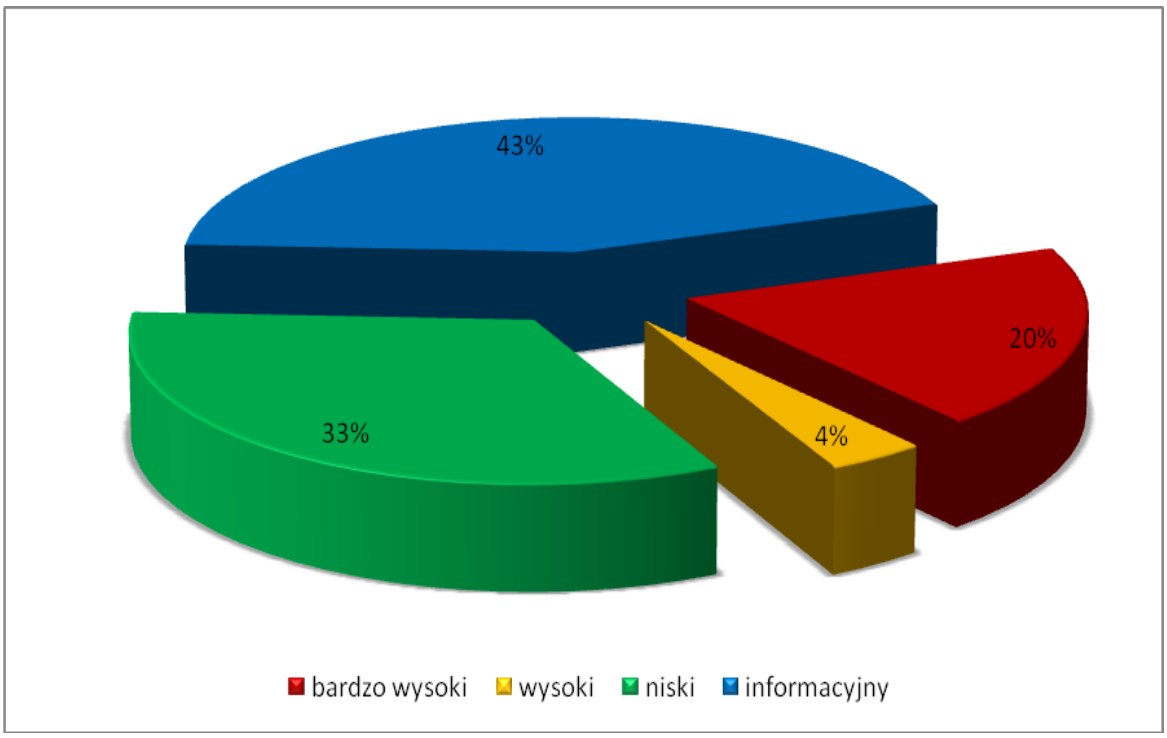
Opublikowany został biuletyn bezpieczeństwa łatający 88 krytycznych luk w produktach Oracle opublikowanych pod nazwą Critical Patch for January 2011. Poprawki usuwały błędy w niżej wymienionych programach:

1. Oracle Database Server – 7 poprawek bezpieczeństwa
2. Oracle Fusion Middleware – 16 poprawek bezpieczeństwa
3. Oracle Enterprise Manager Grid Control – 2 poprawki bezpieczeństwa
4. Oracle E-Business Suite – 6 poprawek bezpieczeństwa
5. Oracle Applications– 16 poprawek bezpieczeństwa
6. Oracle Supply Chain Products Suite – 3 poprawki bezpieczeństwa
7. Oracle PeopleSoft and JDEdwards Suite – 11 poprawek bezpieczeństwa
8. Oracle Industry Applications – 2 poprawki bezpieczeństwa
9. Oracle Sun Products Suite – 23 poprawki bezpieczeństwa
10. Oracle Open Office Suite – 2 poprawki bezpieczeństwa

5. Testy bezpieczeństwa witryn WWW instytucji państwowych

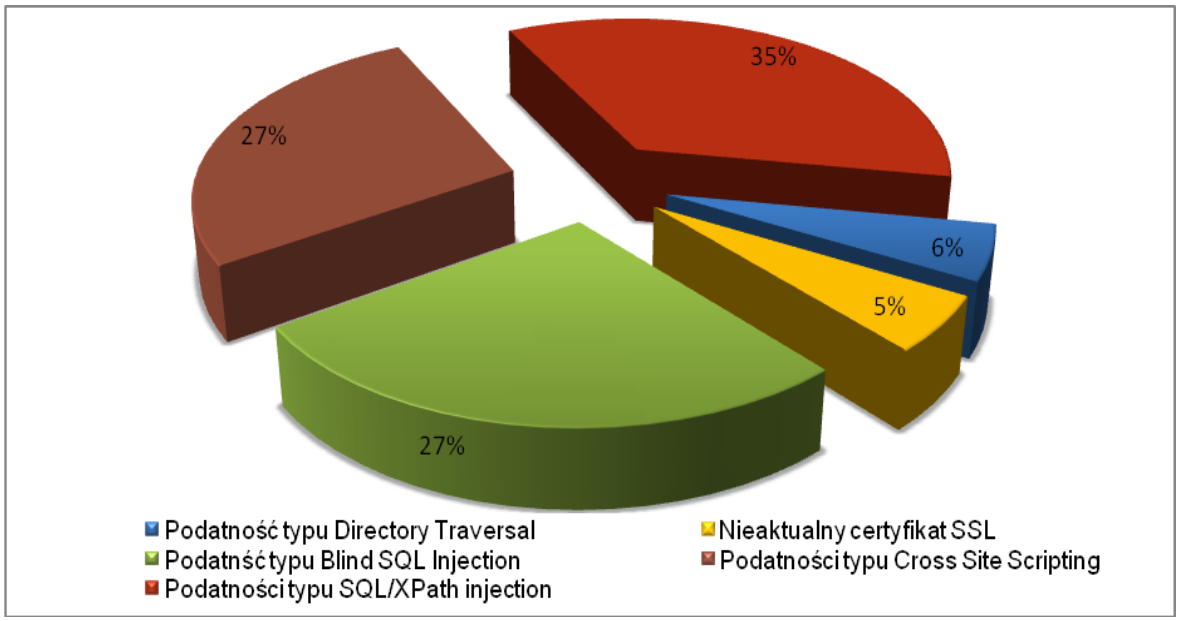
Zespół CERT.GOV.PL kontynuował testy bezpieczeństwa witryn WWW należących do instytucji państwowych.

W I kwartale 2011 roku przebadano 21 witryn należących do 19 instytucji państwowych. Stwierdzono ogółem 188 błędów w tym: 37 błędów o bardzo wysokim poziomie zagrożenia, 7 błędów o wysokim poziomie zagrożenia, 62 błędy o niskim poziomie zagrożenia i 82 błędy oznaczone jako informacyjne.



Rysunek 10 - Statystyka wykrytych podatności w rządowych witrynach WWW według poziomu zagrożenia

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



Rysunek 11 - Procentowy rozkład najpoważniejszych błędów

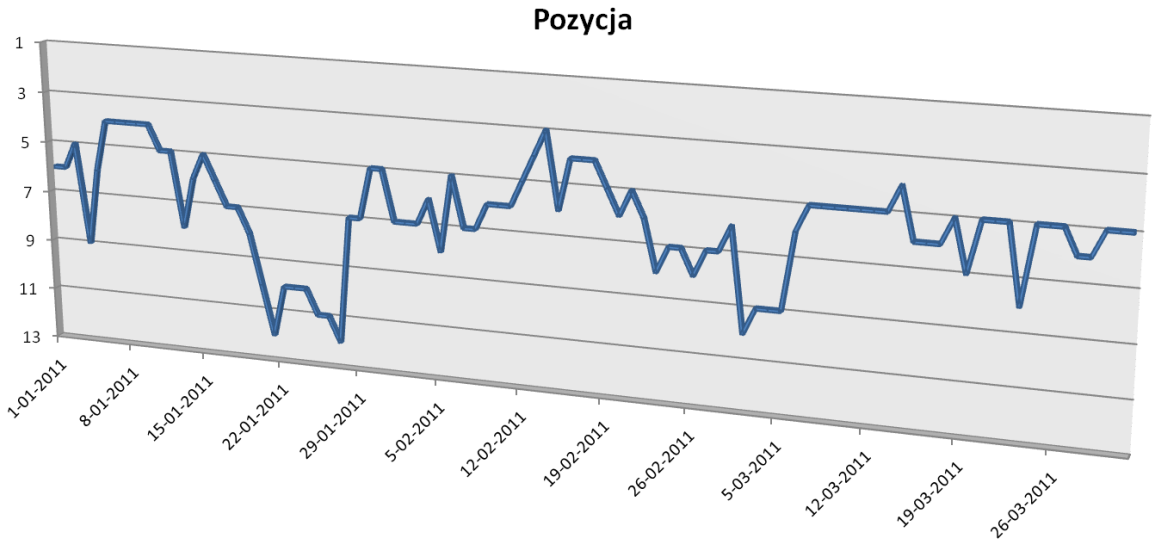
Należy zwrócić uwagę, iż podatności krytyczne najczęściej znajdują się w warstwie usługowej systemu (np. serwerze http czy frontendzie do bazy danych), a nie w warstwie systemu operacyjnego. Jak widać, obecnie największe zagrożenie dla bezpieczeństwa stanowią błędy w aplikacjach, które są budowane, konfigurowane i utrzymywane poza lokalną infrastrukturą instytucji państwowej.

6. Informacje z systemów zewnętrznych

6.1. System ATLAS

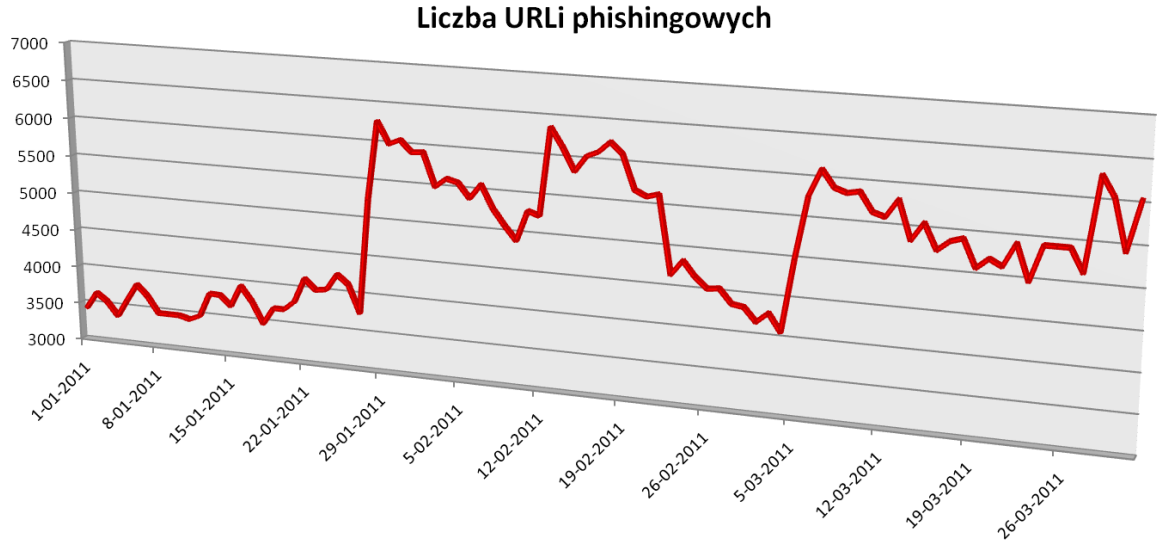
System ATLAS[7] gromadzi istotne informacje na temat zagrożeń teleinformatycznych w sieci Internet i agreguje je pod względem m.in. klas adresowych poszczególnych państw oraz poszczególnych typów niebezpieczeństw. Na podstawie tych danych każdemu z krajów przydzielane jest miejsce w statystyce pokazującej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

Polska w dalszym ciągu utrzymuje się pomiędzy 5 a 7 miejscem rankingu krajów stwarzających zagrożenie dla bezpieczeństwa Internetu. Ciągłe działanie zespołów bezpieczeństwa poprzez likwidowanie stron służących do wyłudzania danych, przekłada się bezpośrednio pozycję Polski. Widać to w szczególny sposób w okresie pomiędzy 12 lutego a 5 marca.



Rysunek 12 - Pozycja Polski w rankingu ATLAS

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



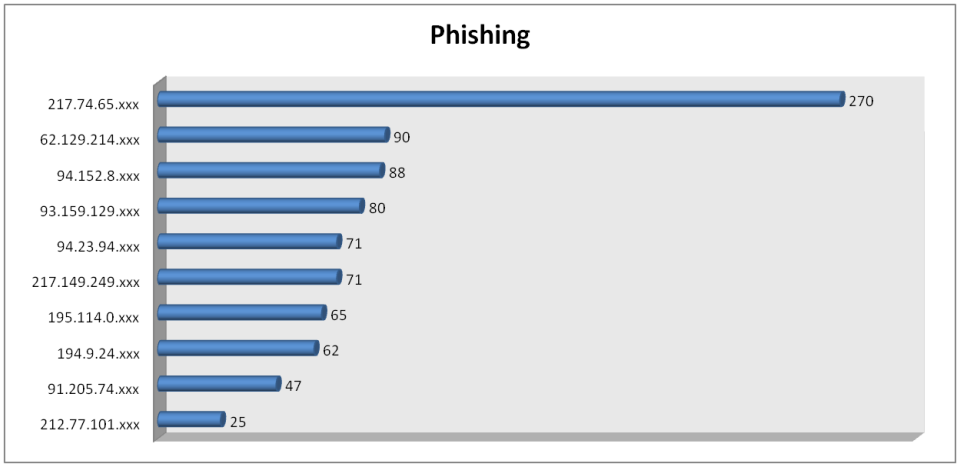
Rysunek 13 – Liczba URLi phishingowych wg ATLAS

Skoki w ilości adresów URL służących do phishingu są bezpośrednio powiązane z powstaniem exploitów na systemy zarządzania treścią Joomla i Wordpress

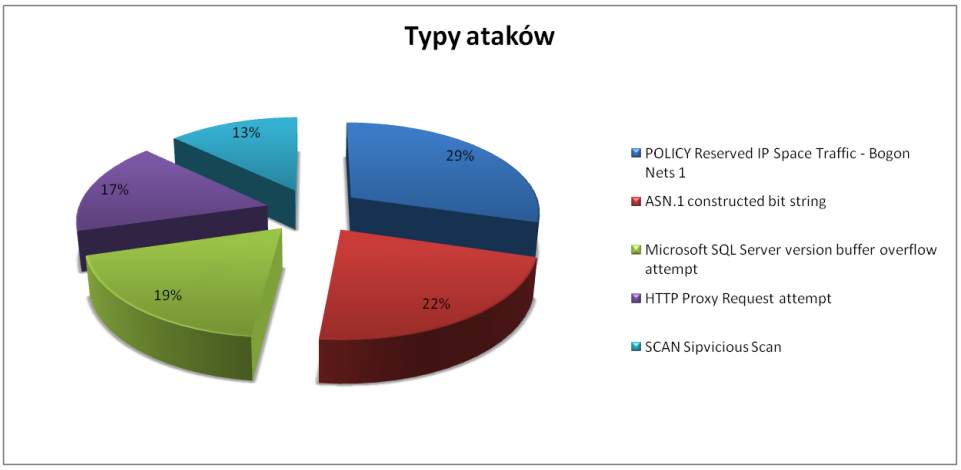
Sytuacja ta, po raz kolejny potwierdza opinię zespołu CERT.GOV.PL, iż liczba stron phishingowych w polskiej przestrzeni adresowej wynika z dużej ilości słabo zabezpieczonych witryn WWW (na których po przełamaniu zabezpieczeń włamywacze umieszczają nieautoryzowane treści), a nie z działalności w Polsce firm oferujących tzw. „kuloodporny hosting”[8].

W dalszym ciągu strony służące do wyłudzania informacji znajdują się w przeważającej ilości przypadków w prywatnych zasobach WWW. Zazwyczaj ich właściciele nie wiedzą o włamaniu, ponieważ treść phishingowa jest jedynie dodawana, bez zmiany dotychczasowej zawartości stron w danej witrynie, co pozwala ukryć przed właścicielem dodanie nielegalnych treści.

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

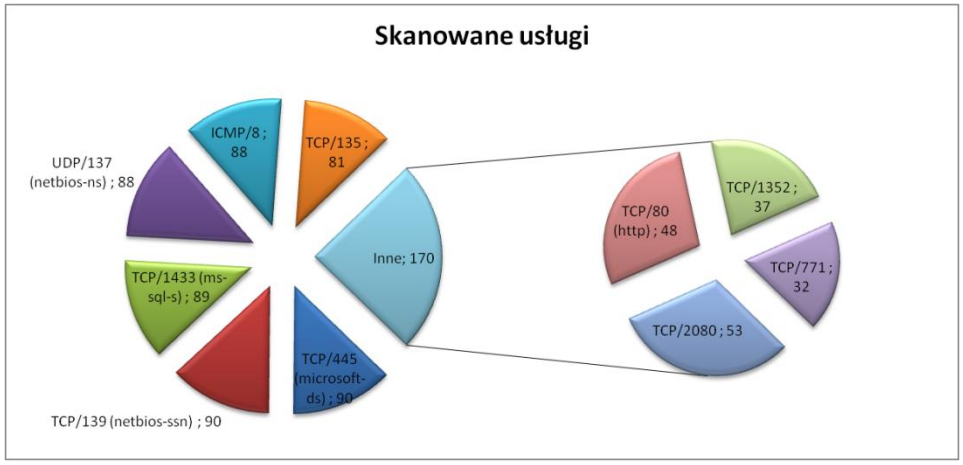


Rysunek 14 Statystyki phishingu wg systemu Atlas
(najwyższe odnotowane udziały, najbardziej aktywnych hostów w drugim kwartale 2010r.)

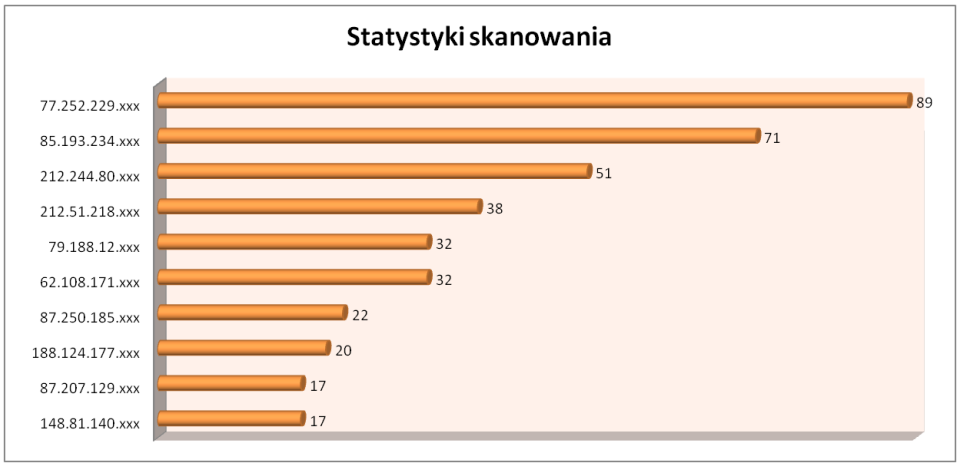


Rysunek 15 Statystyki ataków wg systemu Atlas (II kwartał 2010r.)
Pięć najczęściej występujących typów ataków wg systemu ATLAS – w drugim kwartale 2010r.
(udział procentowy liczony tylko dla tych usług)

Rysunek 16 Najbardziej aktywne hosty w Polsce wg systemu ATLAS – w drugim kwartale 2010r.
(najwyższe odnotowane udziały procentowe w stosunku do pozostałych)



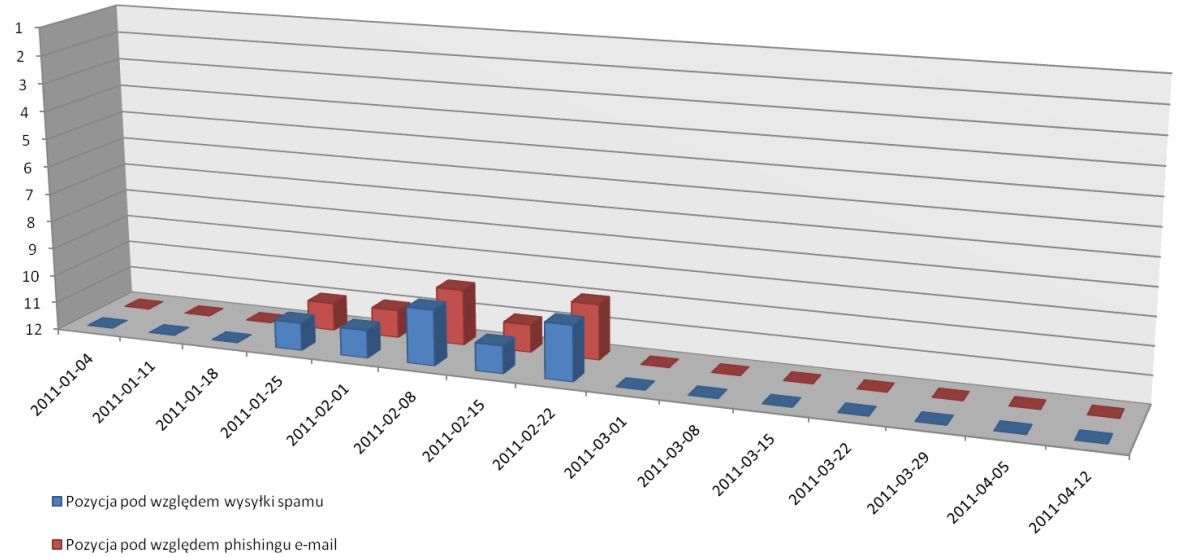
Rysunek 17 Statystyki skanowania wg systemu Atlas (II kwartał 2010r.)
Najczęściej skanowane porty/usługi wg systemu ATLAS – w drugim kwartale 2010r.



Rysunek 18 Najbardziej aktywne hosty w Polsce wg systemu ATLAS – w drugim kwartale 2010r. (najwyższe odnotowane udziały procentowe w stosunku do pozostałych)

6.2. Inne systemy zewnętrzne

Od początku 2010 r. zbierane są informacje na temat udziału Polski pod względem zawartości niechcianych przesyłek e-mailowych[9]



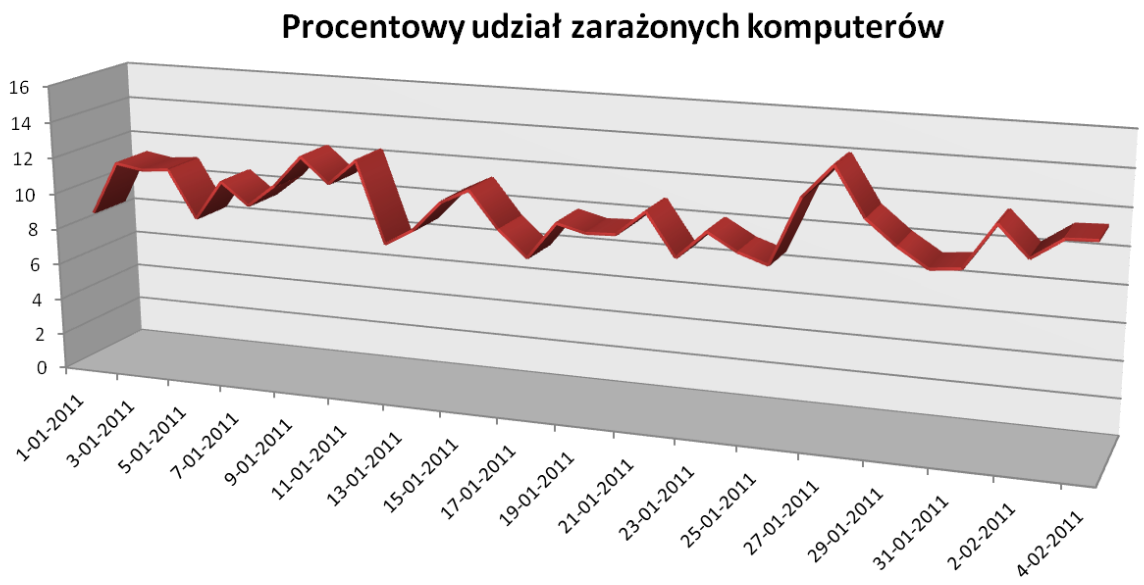
Rysunek 19 – Ranking Polski pod względem wysyłanych e-maili typu „spam" oraz phishingowych (pozycje poniżej miejsca 12-go nie są raportowane)

Pomimo skoku w połowie kwartału, Polska w dalszym ciągu plasuje się w dolnych częściach statystyki krajów, zarówno pod względem przesyłek phishingowych jak i ilości wysyłanego spamu.

Kontynuowana była również analiza (na podstawie informacji zewnętrznych) ilości komputerów zainfekowanych złośliwym oprogramowaniem znajdujących się w obszarze polskiej cyberprzestrzeni. Komputer zainfekowany rozumiany jest jako pojedyncza maszyna, na której znajduje się przynajmniej jeden program należący do jednego z poniższych typów:

- Trojan;
- Worm;
- Wirus;
- Backdoor;
- Adware.

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



Rysunek 20 – Procentowy poziom zawirusowanych komputerów w okresie II-go kwartału 2010r.[10]

Poziom ilości zawirusowanych komputerów można uznać za w miarę stały, utrzymujący się prawie cały czas pomiędzy 8 a 12%. Należy pamiętać, iż statystyka odnosi się do komputerów włączonych w danym okresie (dane zbierane są co 15 minut a następnie uśredniane na poziomie dziennym). Ze względów technicznych, statystyka obejmuje jedynie komputery pracujące pod kontrolą systemu operacyjnego Windows.

Analiza posiadanych informacji wskazuje na utrzymywanie się niskiego miejsca Polski pod względem stanowienia potencjalnego zagrożenia dla użytkowników Internetu. Aktualnie najbardziej newralgicznym obszarem, jest utrzymywanie dużej ilości stron pshisingowych w polskiej przestrzeni adresowej. Wysyłka spamu utrzymana jest na niskim poziomie, lecz nadal Polska występuje pod tym względem w rankingach. Pod względem zagrożeń aktywnych (ataki, rozsyłanie wirusów, skanowania, próby wywołania odmowy dostępu /DDoS/) Polska w dalszym ciągu znajduje się poza przedziałem klasyfikowanym.

[10] Na podstawie informacji otrzymywanych od f-my Panda Security (http://www.pandasecurity.com).
Z dniem 4 lutego f-ma Panda zaprzestała publikacji informacji źródłowych.

7. Inne działania CERT.GOV.PL

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

Uczestnikom szkolenia przedstawione zostały najnowsze trendy zagrożeń dla sieci teleinformatycznych oraz ich użytkowników. Zaprezentowane zostały najczęściej występujące formy ataków, a także sposoby ochrony przed nimi.

W dniu 15 marca 2011 roku miało miejsce kolejne spotkanie z cyklu ABUSE-FORUM (grupa zrzeszająca przedstawicieli zespołów reagujących na incydenty komputerowe, zespołów bezpieczeństwa operatorów telekomunikacyjnych oraz dostawców treści internetowych), którego członkiem jest między innymi Rządowy Zespół Reagowania na Incydenty Komputerowe CERT.GOV.PL.

W trakcie spotkania omówione zostały problemy związane z nielegalnym dostępem do sieci GSM oraz możliwości zakłócania jej prawidłowej pracy. Poruszona została również tematyka klonowania kart GSM, w wyniku stosowania nieefektywnego algorytmu COMP-1.

Ponadto, dużą uwagę poświęcono kwestii związanej z pojawieniem się nowej wersji trojana bankowego o nazwie „ZeuS". Zaimplementowany w nim dodatkowy moduł obsługujący komunikację banku z klientem za pomocą wiadomości SMS infekował podatne systemy telefonów komórkowych (Windows Mobile, BlackBerry oraz Symbian).

Jednocześnie dyskutowano na temat konieczności tworzenia i rozbudowy lokalnych zespołów bezpieczeństwa w firmach komercyjnych.