Agencja Bezpieczeństwa Wewnętrznego

Raport kwartalny CERT.GOV.PL
lipiec – wrzesień 2009

1. Informacje dotyczące zespołu CERT.GOV.PL

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

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

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

Dane kontaktowe:

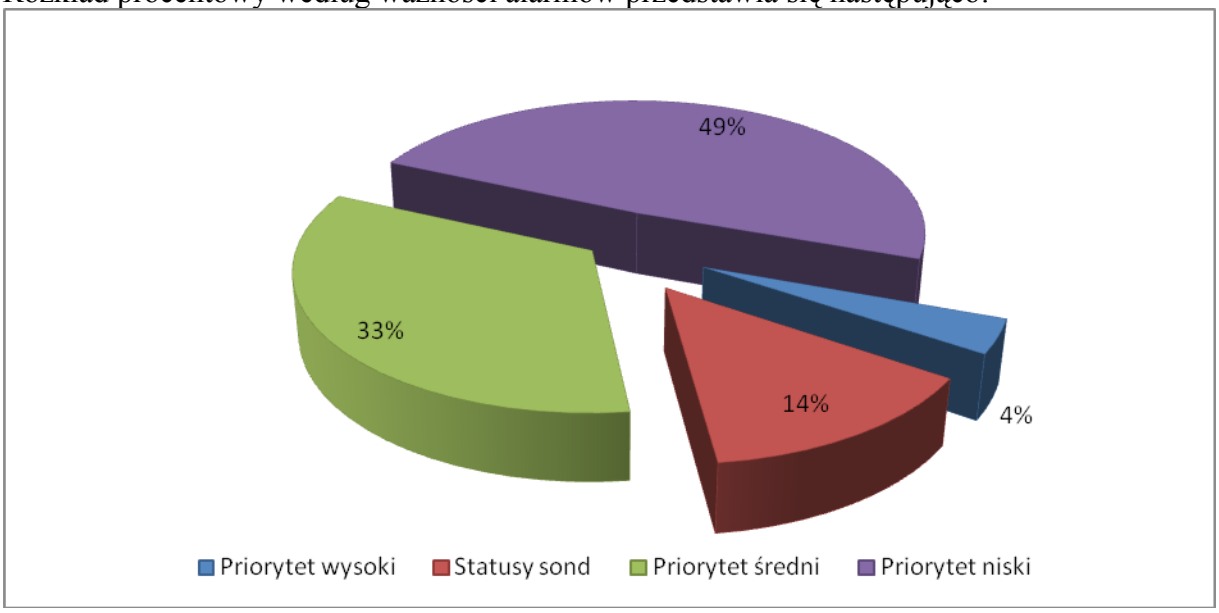
- E-mail: cert@cert.gov.pl
- Telefon: +48 22 58 58 844
- Fax: +48 22 58 58 833

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

2. Statystyki systemu ARAKIS-GOV[1]

W trzecim kwartale 2009 roku system ARAKIS-GOV zgłosił 1463 alarmy, w tym 56 o wysokim priorytecie, 493 o priorytecie średnim, 713 o priorytecie niskim oraz 201 alarmów diagnostycznych.

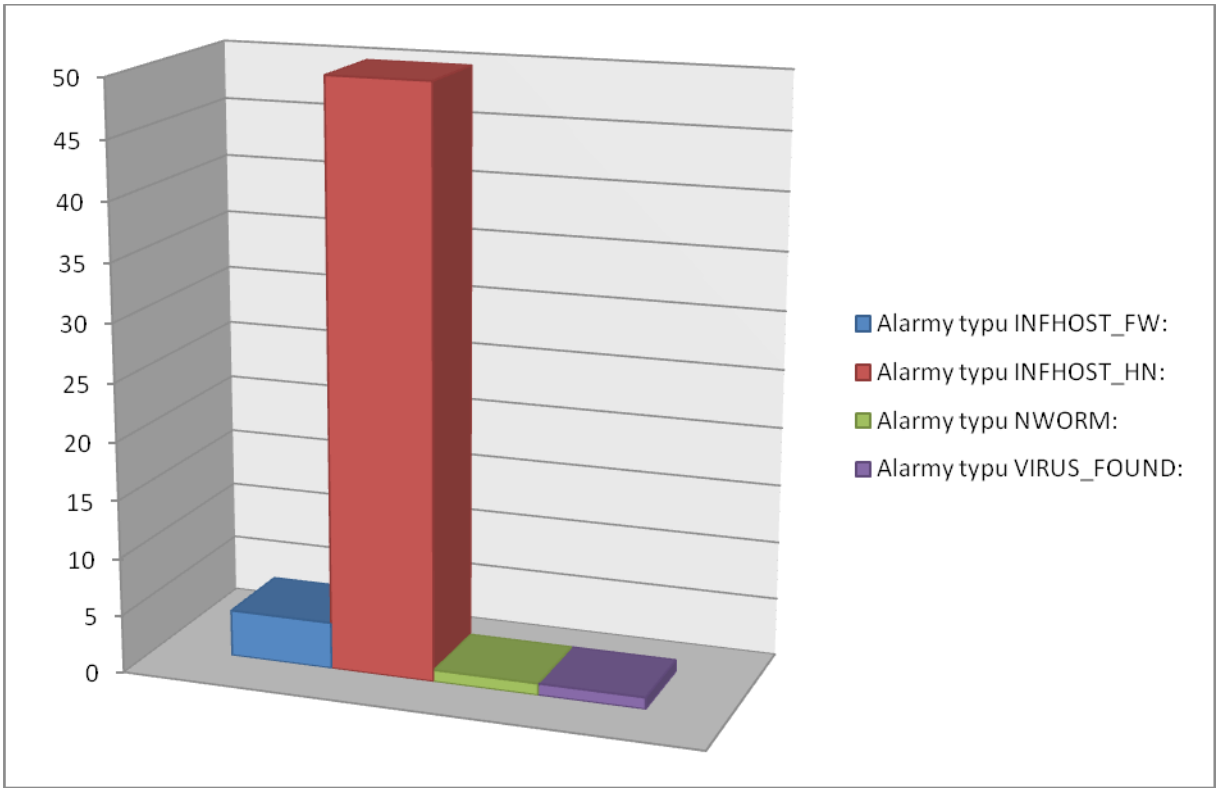
Rozkład procentowy według ważności alarmów przedstawia się następująco:



Rysunek 1 - Procentowy rozkład ważności alarmów

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

Spośród alarmów o wysokim priorytecie zanotowano 4 alarmy typu INFHOST_FW[2], 50 alarmów typu INFHOST_HN[3], 1 alarm typu NWORM[4] oraz 1 alarm typu VIRUS_FOUND[5].



Rysunek 2 - Statystyki alarmów o wysokim priorytecie

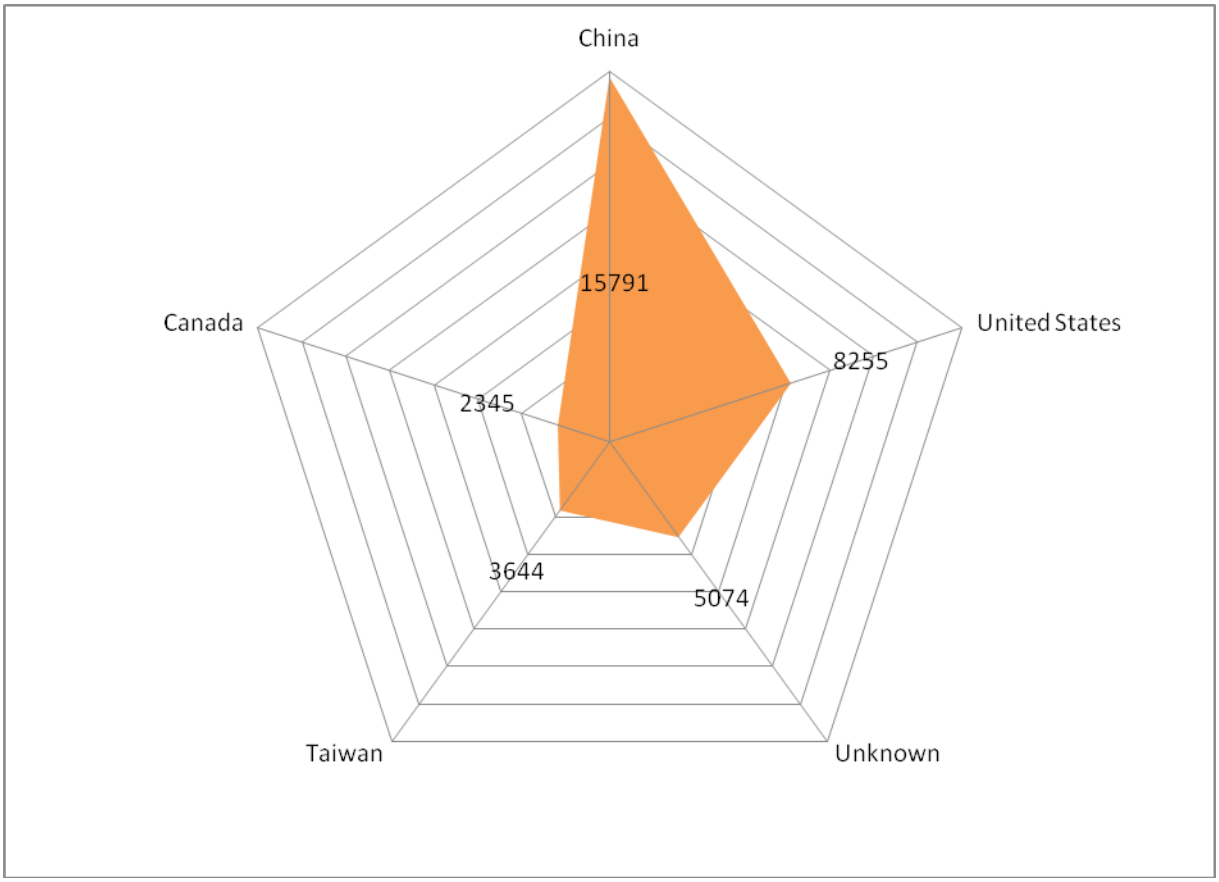
[2] Alarm INFHOST_FW oznacza potencjalne wykrycie zainfekowanego hosta w sieci wewnętrznej instytucji chronionej systemem ARAKIS-GOV. Alarm ten generowany jest na podstawie analizy logów systemów zaporowych.

[3] 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.

[4] Alarm NWORM oznacza potencjalne wykrycie nowego, szybko rozprzestrzeniającego się zagrożenia sieciowego (robaka sieciowego)

[5] Alarm VIRUS_FOUND oznacza wykrycie infekcji wirusowej w sieci wewnętrznej chronionej instytucji. Alarm ten generowany jest na podstawie informacji pochodzących ze skanerów antywirusowych serwerów pocztowych

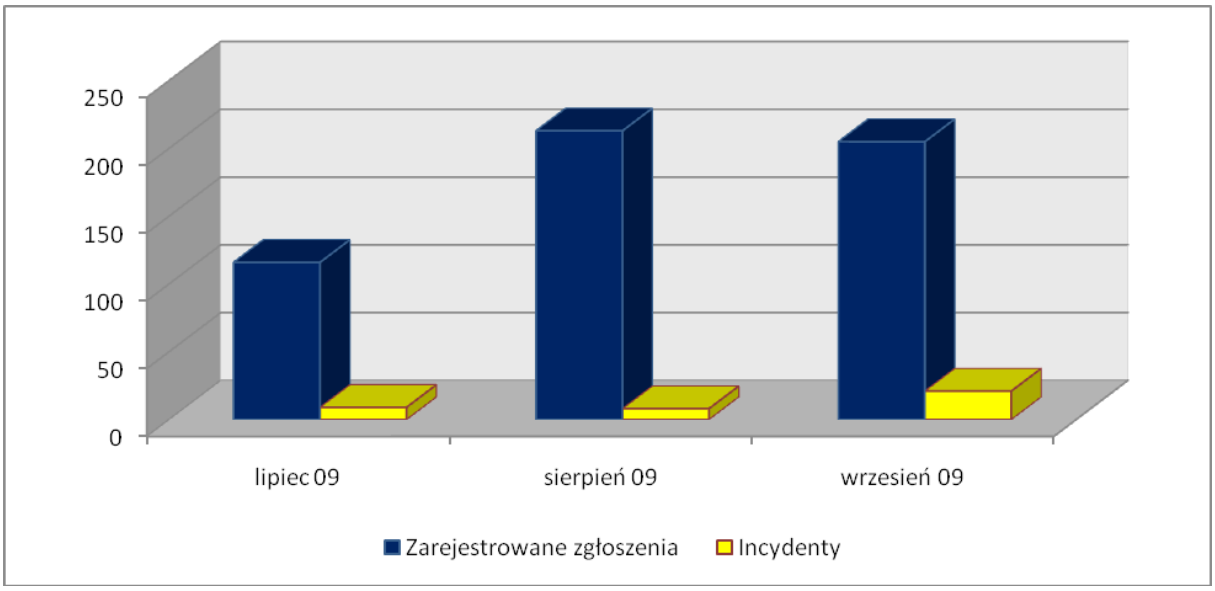
Na podstawie analizy adresu IP nadawcy pakietu stwierdzono, iż źródła ataków zaobserwowanych przez ARAKIS-GOV pochodziły najczęściej z sieci komputerowych Chin, Stanów Zjednoczonych, nieznanego nadawcy, Tajwanu i Kanady. Jednakże ze względu na specyfikę protokołu TCP/IP nie można bezpośrednio łączyć źródła pochodzenia pakietów z faktyczną lokalizacją zleceniodawcy ataku. Wynika to z faktu, iż w celu ukrycia swej tożsamości i fizycznej lokalizacji atakujący wykorzystują serwery pośredniczące (proxy) lub słabo zabezpieczone komputery, nad którymi wcześniej przejmują kontrolę.



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

3. Statystyki incydentów

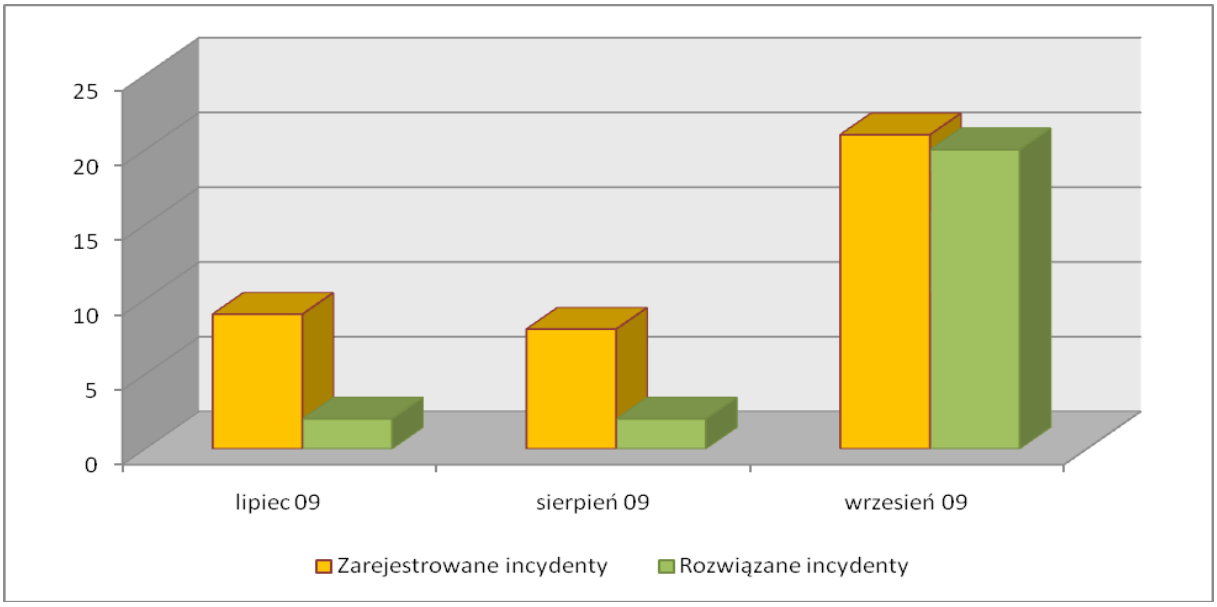
W trzecim kwartale 2009 roku do zespołu CERT.GOV.PL wpłynęły 534 zgłoszenia, przy czym jedynie 38 z nich zostało zakwalifikowane jako faktyczne incydenty.



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

Duża liczba zgłoszeń w stosunku do liczby faktycznych incydentów wynika z faktu, iż część zgłoszeń stanowią tzw. „false-positives" czyli przypadki błędnej interpretacji, przez zgłaszającego, legalnego ruchu sieciowego. Ponadto część zgłoszeń odnosi się do tego samego incydentu.

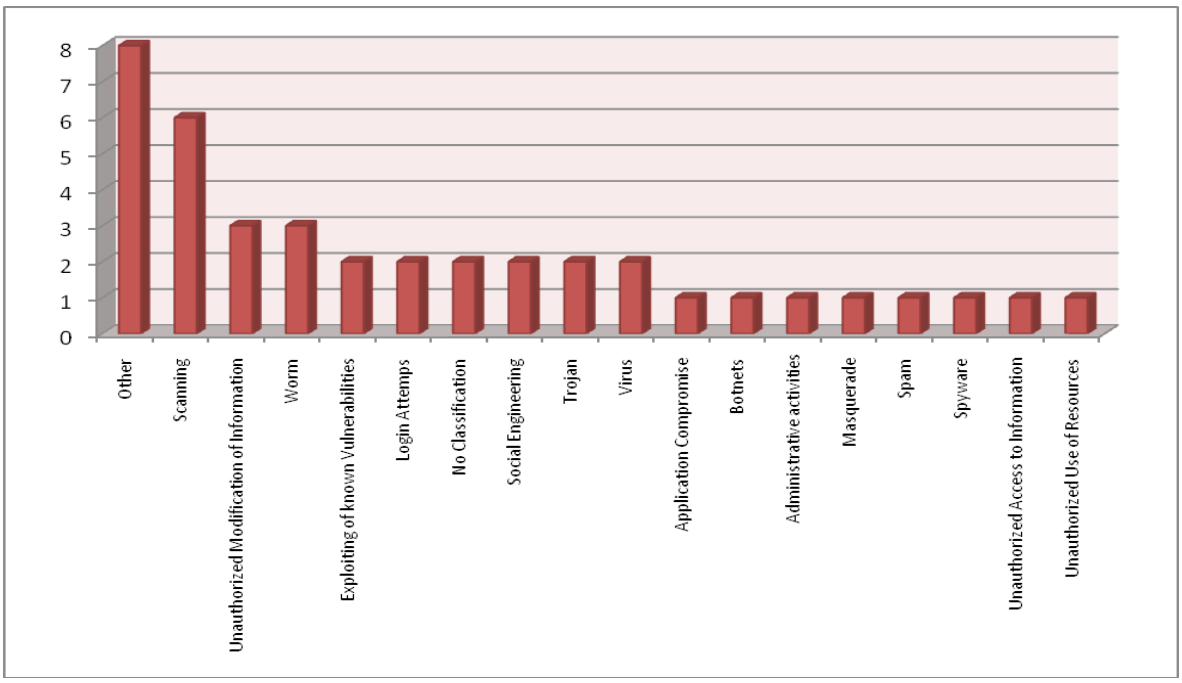
Spośród zarejestrowanych w trzecim kwartale incydentów w lipcu zanotowano 9 incydentów, w sierpniu 8, natomiast we wrześniu 21. W lipcu rozwiązano 2 incydenty, w sierpniu kolejne 2, natomiast we wrześniu 20. Pozostałe incydenty nadal są w trakcie rozwiązywania.



Rysunek 5 - Porównanie liczby incydentów otwartych i zamkniętych w poszczególnych miesiącach trzeciego kwartału

Na podstawie powyższego wykresu wyraźnie widać wpływ zakończenia sezonu wakacyjnego na zwiększenie liczby zarówno faktycznych incydentów jak i możliwości szybszego rozwiązania problemów.

Podział zarejestrowanych incydentów na kategorie przedstawia się następująco:



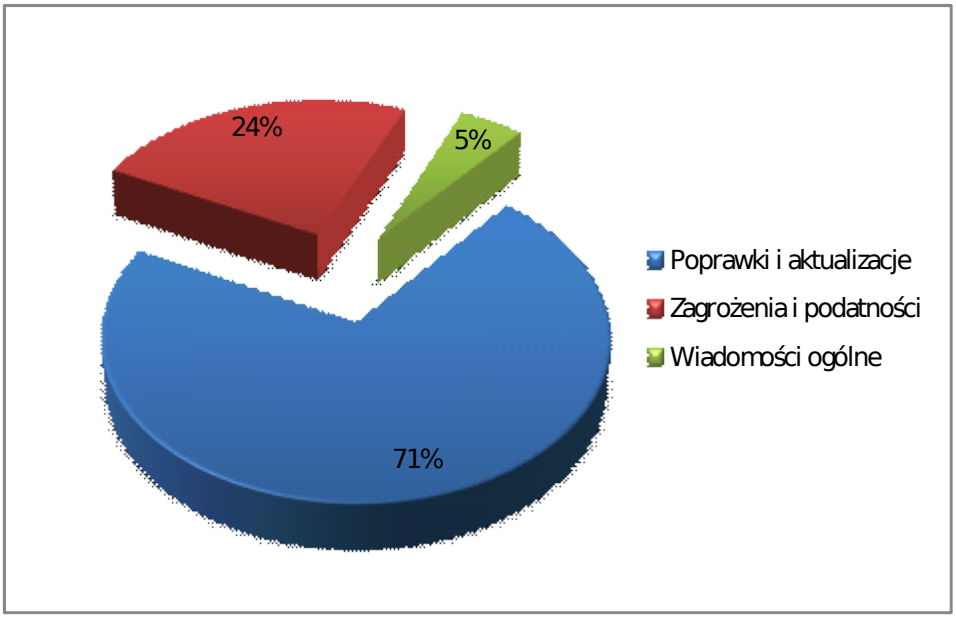
Rysunek 6 - Statystyka incydentów z podziałem na kategorie

4. Istotne podatności, zagrożenia i biuletyny zabezpieczeń

Witryna http://www.cert.gov.pl jest źródłem specjalistycznych informacji związanych z bezpieczeństwem teleinformatycznym. Publikowane są tam między innymi aktualne informacje dotyczące istotnych zagrożeń, nowych podatności w popularnych systemach i aplikacjach, najczęstszych form ataków sieciowych oraz sposobów ochrony przed zagrożeniami. Dodatkowo, na powyższej witrynie umieszczane są biuletyny bezpieczeństwa udostępniane przez producentów sprzętu i oprogramowania.

W trzecim kwartale 2009 roku na witrynie www.cert.gov.pl dodano:

- 30 publikacji w kategorii „Poprawki i aktualizacje”,
- 10 publikacji w kategorii „Zagrożenia i podatności”,
- 2 publikacje w kategorii „Wiadomości ogólne”.



Rysunek 7 - Procentowy rozkład publikacji na witrynie www.cert.gov.pl

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

- **Ataków ukierunkowanych na instytucje administracji publicznej**

Ataki ukierunkowane przeprowadzane są zwykle poprzez, zawierające złośliwe oprogramowanie, załączniki poczty elektronicznej, których otwarcie skutkuje instalacją w systemie oprogramowania typu „koń trojański”. Istotą ataku jest jego „ukierunkowanie”, tzn. indywidualny, spersonalizowany, charakter przesłanej wiadomości, udający np. korespondencję służbową.

- **Krytycznego błędu w nowej wersji protokołu SMB2 zaimplementowanego w niektórych wersjach systemów operacyjnych Windows**

Zespół CERT.GOV.PL jako pierwszy w Polsce poinformował na swojej witrynie o błędzie dotyczącym nowej wersji protokołu SMB2 zaimplementowanego w systemach operacyjnych Windows. Na stronie została również umieszczona informacja jak tymczasowo zabezpieczyć system do czasu pojawienia się odpowiedniej aktualizacji.

- **Luki w serwerze DNS-BIND (podatność na atak DoS[6])**

W oprogramowaniu ISC BIND9 wykryto lukę, która pozwala na wykonanie zdalnego ataku typu odmowa usługi (DoS). Przesłanie specjalnie spreparowanego pakietu dynamicznej aktualizacji do serwera mogło zatrzymać pracę serwera DNS.
Administratorzy instytucji rządowych zostali poinformowani o poprawkach dostępnych w Internecie i poproszeni o jak najszybsze zaktualizowanie oprogramowania zgodnie z używaną wersją systemu operacyjnego.

- **Poprawek dla jądra systemu Linux**

Opublikowana została krytyczna poprawka do jądra systemu Linux. Poprawka usuwała błąd, który umożliwiał zwykłemu użytkownikowi uzyskać prawa roota (superużytkownika).
Problem ten dotyczył jądra systemu w wersjach:
Linux 2.4: od 2.4.4 do wersji 2.4.37.4 włącznie
Linux 2.6: do 2.6.0 do wersji 2.6.30.4 włącznie

- **Podatności w jądrze systemu Linux w środowisku maszyny wirtualnej**

Opublikowano informacje na temat błędów jądra systemu Linux stanowiących podatności na atak typu *Local DoS*[7] oraz uzyskanie dostępu do pamięci jądra systemu operacyjnego zainstalowanego na wirtualnej maszynie.

- **Comiesięcznych biuletynów bezpieczeństwa firmy Microsoft**

Lipcowy biuletyn bezpieczeństwa:

Biuletyn dotyczył usunięcia sześciu poważnych błędów. Trzy otrzymało status „krytyczny", pozostałe „ważny". Luki o statusie "krytyczny" pozwalały na zdalne wykonanie kodu.

1. MS09-028 - Biuletyn dotyczący oprogramowania Microsoft DirectShow - krytyczny
2. MS09-029 - Biuletyn dotyczący komponentu Embedded OpenType (EOT) Font Engine - krytyczny

[6] DoS (Denial of Service) – atak typu odmowa usługi, polegający na uniemożliwieniu uprawnionym użytkownikm na dostęp do systemu np. poprzez całkowite obciążenie łącza lub wyczerpanie zasobów systemowych
[7] Local DoS - odmiana ataku typu odmowa usługi, możliwa do przeprowadzenia wyłącznie z poziomu lokalnego dostępu do systemu.

3. MS09-032 - Biuletyn dotyczący oprogramowania Microsoft Video ActiveX Control - krytyczny
4. MS09-030 - Biuletyn dotyczy oprogramowania Microsoft Office Publisher - ważny
5. MS09-031 - Biuletyn dotyczy oprogramowania Microsoft Internet Security and Acceleration (ISA) Server 2006 - ważny
6. MS09-033 - biuletyn dotyczący oprogramowania Virtual PC and Virtual Server - ważny

Firma Microsoft poza normalnym trybem wydawania poprawek opublikowała dodatkowo w lipcu dwa biuletyny bezpieczeństwa:

1. MS09-034 - Zbiorcza aktualizacja zabezpieczeń dla programu Internet Explorer -krytyczny
2. MS09-035 - Luki w zabezpieczeniach biblioteki Active Template Library programu Visual Studio - umiarkowany

Sierpniowy biuletyn bezpieczeństwa:

Sierpniowy biuletyn bezpieczeństwa informował o usunięciu dziewięciu poważnych błędów w swoich produktach. Pięć otrzymało status „krytyczny", pozostałe „ważny". Luki o statusie "krytyczny" pozwalały na zdalne wykonanie kodu.

1. MS09-037 - dotyczy usterki w bibliotece Microsoft Active Template Library (ATL) - krytyczny
2. MS09-038 – poświęcony został usterce w przetwarzaniu plików Windows Media - krytyczny
3. MS09-039 – opisuje luki w zabezpieczeniach protokołu WINS - krytyczny
4. MS09-043 – rozwiązuje problem w produktach wykorzystujących Microsoft Office Web Components - krytyczny
5. MS09-044 – dotyczy luki w zabezpieczeniach usługi Remote Desktop - krytyczny
6. MS09-036 - dotyczy usterki w Microsoft .NET Framework - ważny
7. MS09-040 – opisuje lukę w usłudze kolejkowania wiadomości systemu Windows (MSMQ) - ważny
8. MS09-041 - rozwiązuje problem w usłudze Windows Workstation Service - ważny
9. MS09-042 – poświęcony został usłudze Microsoft Telnet - ważny

Wrześniowy biuletyn bezpieczeństwa:

Firma Microsoft opublikowała sierpniowy biuletyn bezpieczeństwa informujący o usunięciu pięciu poważnych błędów w swoich produktach. Wszystkie otrzymały status „krytyczny".

1. MS09-045 – dotyczy podatności w silniku Jscript - krytczny
2. MS09-046 – dotyczy podatności w edytowanym komponencie sterującym ActiveX DHTML - krytyczny
3. MS09-047 – dotyczy podatności w Windows Media Format - krytyczny
4. MS09-048 – dotyczy podatności w Windows TCP/IP - krytyczny
5. MS09-049 – dotyczy podatności w usłudze AutoConfig dla bezprzewodowych sieci LAN - krytyczny

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

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

1. Firewall Services Module (FWSM) - Błąd pozwalał na przeprowadzenie ataku typu DoS podczas przesyłania przez atakującego specjalnie spreparowanych pakietów ICMP do urządzenia.
2. Unified Communications Manager - posiadał wiele podatności umożliwiających przeprowadzenie ataku typu denial of service (DoS), co mogło doprowadzić do zatrzymania usług SIP (Session Initiation Protocol) i SCCP (Skinny Client Control Protocol).
3. Błędy w implementacji protokołu TCP w produktach Cisco IOS, IOS-XE, CatOS, ASA, PIX, NX-OS i urządzeń z serii Linksys pozwalały na przeprowadzenie ataków typu DoS.
4. Cisco IOS - Wykryto wiele podatności w systemie Cisco IOS, za pomocą których możliwe było przeprowadzenie ataku typu DoS (Denial-of-Service), obejście zabezpieczeń systemowych i dostęp do chronionych informacji

- **Biuletynów bezpieczeństwa dla produktów firmy Adobe**

Rządowy Zespół Reagowania na Incydenty Komputerowe informował o:

1. Krytycznych lukach w Shockwave Player, które pojawiały się dwukrotnie w ostatnim kwartale i mogły doprowadzić do przejęcia kontroli nad komputerem.
2. Poprawkach dla aplikacji internetowej ColdFusion przeznaczonej do tworzenia dynamicznie generowanych stron internetowych oraz narzędzia administracyjnego JRun.
3. Biuletynie bezpieczeństwa Adobe APSB09-14 dotyczącym likwidacji podatności w produkcie RoboHelp Server 8. Wykorzystanie podatności umożliwiało zdalne wykonanie kodu na komputerze ofiary.

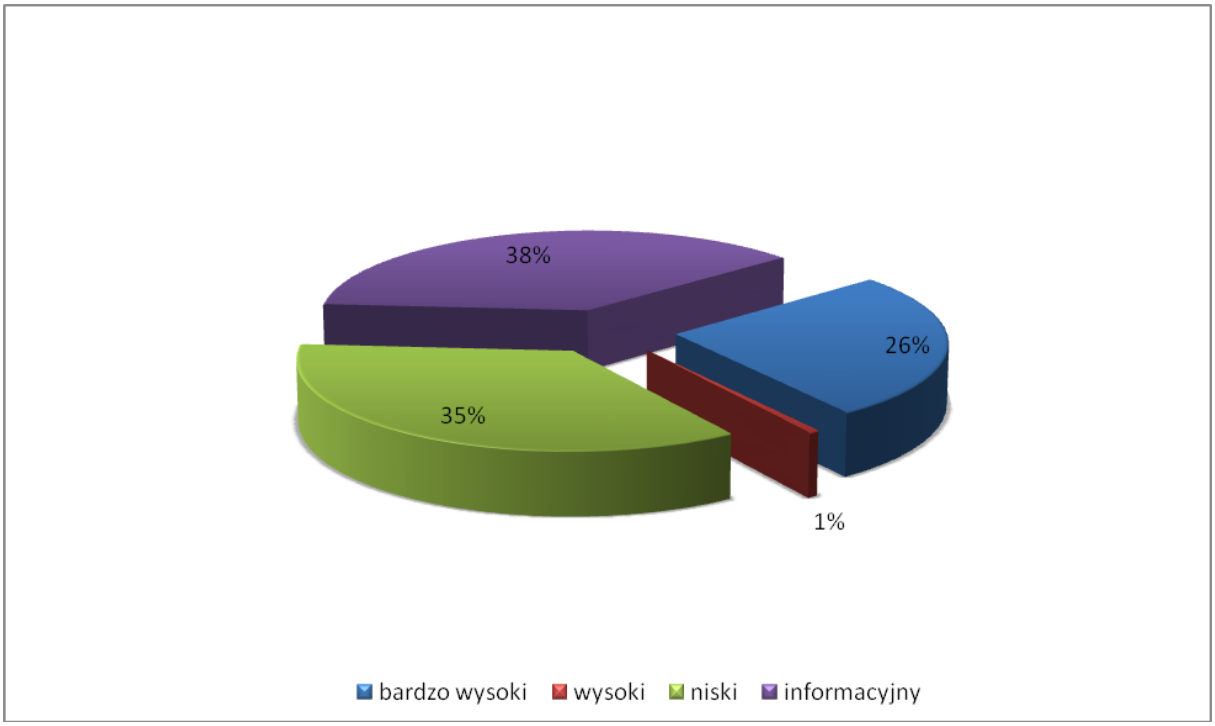
- **Podatności i poprawki dla użytkowników systemu Mac OS**

Zespół CERT.GOV.PL zamieścił na stronie szczegółowe informacje na temat pakietu aktualizacyjnego dla systemu operacyjnego Mac Os X.

5. Testy bezpieczeństwa witryn WWW instytucji państwowych

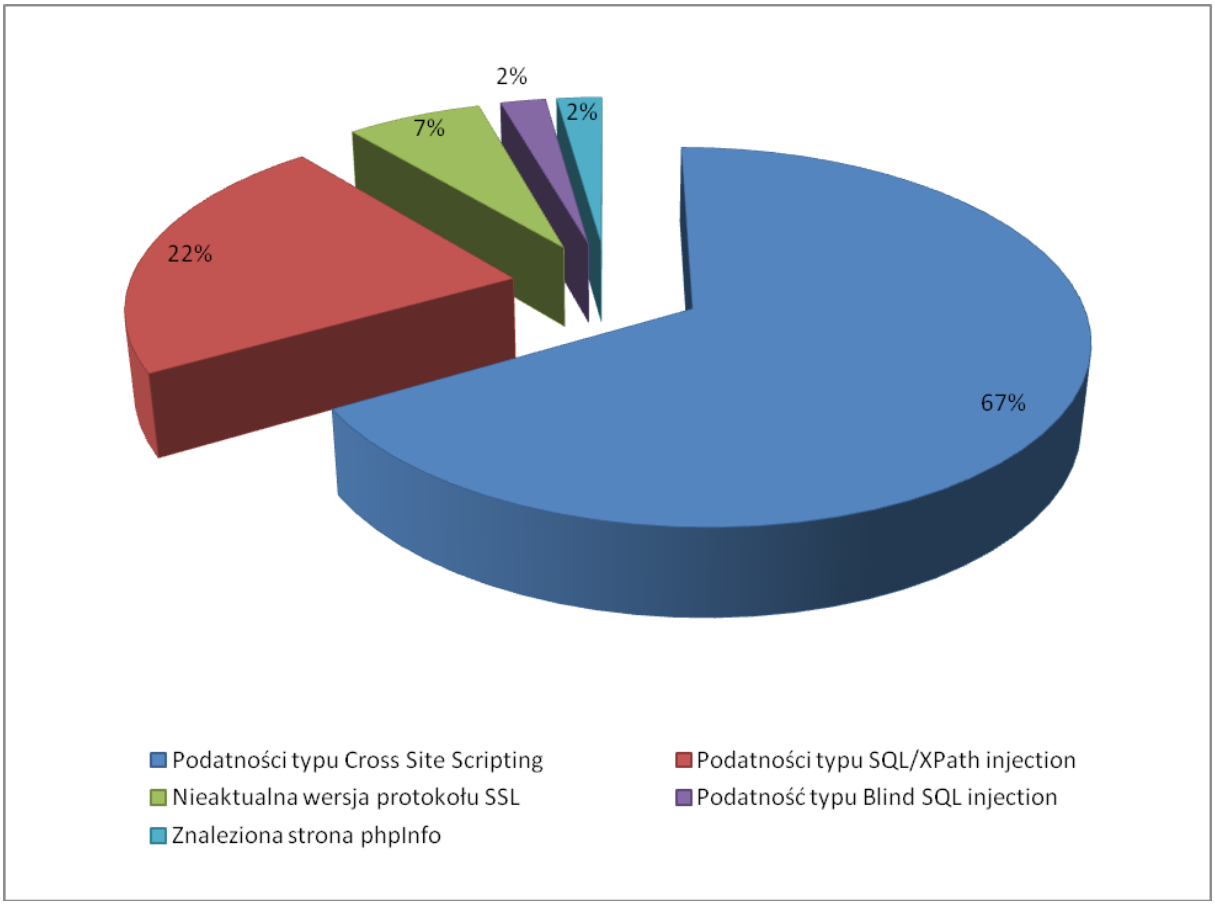
W związku z ujawnianiem coraz większej liczby podatności na witrynach internetowych, CERT.GOV.PL rozpoczął proces sukcesywnego testowania poziomu bezpieczeństwa witryn należących do instytucji państwowych. Usługa ta wykonywana jest nieodpłatnie dla instytucji państwowych i cieszy się dużym zainteresowaniem.

W trzecim kwartale 2009 roku przebadano 15 witryn należących do 8 instytucji państwowych. Stwierdzono ogółem 167 błędów w tym: 44 błędy o bardzo wysokim poziomie zagrożenia, 1 błąd o wysokim poziomie zagrożenia, 59 błędów o niskim poziomie zagrożenia i 63 błędy oznaczone jako informacyjne.



Rysunek 8 - Statystyka wykrytych podatności w rządowych witrynach WWW według poziomu zagrożenia

Wśród podatności o wysokim lub bardzo wysokim poziomie zagrożenia dominują błędy typu Cross Site Scripting, SQL/XPath Injection, Blind SQL Injection, korzystanie z przestarzałych wersji protokołu SSL czy też ujawnianie istotnych informacji poprzez publikację strony zawierającej instrukcje PHP phpinfo.

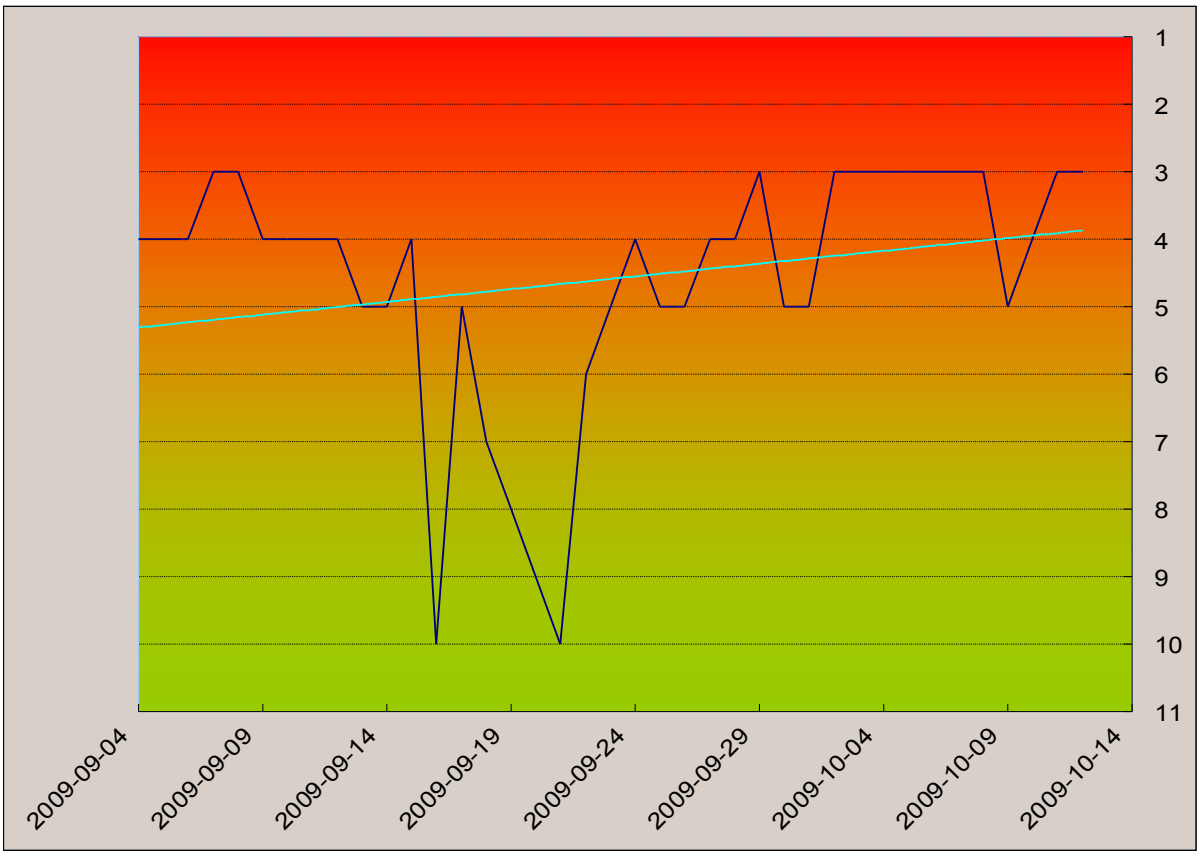


Rysunek 9 - Procentowy rozkład najpoważniejszych błędów

Należy zwrócić uwagę, iż podatności krytyczne najczęściej znajdują się w warstwie usługowej systemu (np. serwerze http czy frontendzie do bazy danych) a nie w warstwie systemu operacyjnego. Jak widać, obecnie największe zagrożenie dla bezpieczeństwa stanowią błędy w aplikacjach, do których ma dostęp użytkownik zewnętrzny i które bardzo często, nie są budowane, konfigurowane i utrzymywane przez lokalnych administratorów w instytucjach.

6. Informacje z systemu ATLAS[8]

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



Rysunek 10 - Pozycja Polski w "rankingu" ATLAS

Wysokie miejsce Polski (oraz rosnący w dalszym ciągu trend) jest spowodowane bardzo dużą liczbą stron służących do phishingu (ponad 4000). Ponad 40% tych stron hostowanych jest w systemie autonomicznym AS16138[9] , natomiast ponad 35% w AS16276.
W pozostałych kategoriach (ilość wykrytych botnetów, ilość skanów w przeliczeniu na podsieć, ilość ataków w przeliczeniu na podsieć, ataki DoS) Polska znajduje się poza pierwszą dziesiątką krajów stanowiących największe zagrożenie.

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

[9] AS – Autonomus System – zakres lub grupa zakresów podsieci, przyporządkowanych do jednej jednostki i jako taki stanowiący wpis w bazie RIPE NCC lub innego odpowiedniego RIR (Regional Internet Registry) w przypadku gdy lokalizacja sieci znajduje się poza obszarem Europy, Bliskiego Wschodu lub części Azji. Numer AS jest jednoznacznym identyfikatorem przyporządkowania sieci do danej organizacji (np. dostawcy usług)