Raport o stanie bezpieczeństwa cyberprzestrzeni RP w 2010 roku

Warszawa 2011

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

1. Wprowadzenie

Rządowy Zespół Reagowania na Incydenty Komputerowe CERT.GOV.PL jest podmiotem właściwym w zakresie koordynacji przeciwdziałania cyberzagrożeniom. Funkcjonuje zgodnie z przyjętymi w dniu 9 marca 2009r. przez Komitet Stały Rady Ministrów Założeniami Rządowego Programu Ochrony Cyberprzestrzeni RP na lata 2009-2011 (RPOC). Głównym celem strategicznym programu jest wzrost poziomu bezpieczeństwa cyberprzestrzeni państwa. Szczegółowe zadania zostały określone jako:

a) zwiększenie poziomu bezpieczeństwa krytycznej infrastruktury teleinformatycznej państwa, skutkujące zwiększeniem poziomu odporności państwa na ataki cyberterrorystyczne,
b) stworzenie i realizacja spójnej dla wszystkich, zaangażowanych podmiotów administracji publicznej oraz innych współstanowiących krytyczną infrastrukturę teleinformatyczną państwa, polityki dotyczącej bezpieczeństwa cyberprzestrzeni,
c) zmniejszenie skutków ataków cyberterrorystycznych, a przez to kosztów usuwania ich następstw,
d) stworzenie trwałego systemu koordynacji i wymiany informacji pomiędzy publicznymi i prywatnymi podmiotami odpowiedzialnymi za zapewnianie bezpieczeństwa cyberprzestrzeni państwa oraz władającymi zasobami stanowiącymi krytyczną infrastrukturę teleinformatyczną państwa,
e) zwiększenie kompetencji odnośnie bezpieczeństwa cyberprzestrzeni podmiotów zaangażowanych w ochronę krytycznej infrastruktury teleinformatycznej państwa oraz innych systemów i sieci administracji publicznej,
f) zwiększenie świadomości użytkowników (w tym obywateli) systemów dostępnych elektronicznie i sieci teleinformatycznych w zakresie metod i środków bezpieczeństwa.

Do zadań nałożonych na CERT.GOV.PL i wykonywanych od momentu powstania w lutym 2008 r. należy:

a) kreowanie polityki w zakresie ochrony przed cyberzagrożeniami,
b) koordynowanie przepływu informacji pomiędzy podmiotami w tym zakresie,
c) wykrywanie, rozpoznawanie i przeciwdziałanie cyberzagrożeniom,

d) współpraca z krajowymi instytucjami, organizacjami oraz podmiotami resortowymi w zakresie ochrony cyberprzestrzeni,
e) reprezentacja RP w kontaktach międzynarodowych (w zakresie współpracy wojskowej, w porozumieniu z Centrum Koordynacyjnym Systemu Reagowania na Incydenty Komputerowe resortu obrony narodowej),
f) gromadzenie wiedzy dotyczącej stanu bezpieczeństwa i zagrożeń dla krytycznej infrastruktury teleinformatycznej,
g) reagowanie na incydenty bezpieczeństwa teleinformatycznego ze szczególnym uwzględnieniem krytycznej infrastruktury teleinformatycznej państwa,
h) prowadzenie analiz powłamaniowych,
i) tworzenie polityki ochrony systemów i sieci teleinformatycznych,
j) szkolenia i podnoszenie świadomości odnośnie cyberzagrożeń,
k) przygotowywanie okresowych raportów w zakresie bezpieczeństwa teleinformatycznego państwa,
l) konsulting i doradztwo w zakresie cyberbezpieczeństwa.

W niniejszym raporcie, który stanowi realizację zadań nałożonych przez RPOC, przedstawiono statystyki działań Rządowego Zespołu Reagowania Na Incydenty Komputerowe CERT.GOV.PL, przykłady zarejestrowanych ataków na jednostki administracji państwowej oraz ogólne oszacowanie stanu bezpieczeństwa cyberprzestrzeni RP na tle charakterystyki w tym zakresie w ujęciu światowym.

Rok 2010 pod względem bezpieczeństwa teleinformatycznego przyniósł nowe trendy w zakresie sposobów wykonywania ataków na systemy komputerowe.

Zauważalny jest przede wszystkim bardzo wyraźny wzrost ilości ataków na systemy telefonii VoIP[1]. Skompromitowane systemy VoIP wykorzystywane były zazwyczaj do wykonywania połączeń na numery o podwyższonej płatności lub do wykonywania połączeń międzynarodowych na koszt posiadacza danego systemu. Należy zwrócić uwagę, iż powyższy mechanizm przestępczy przypomina stosowanie w latach dziewięćdziesiątych ubiegłego wieku tzw. dialerów, które także umożliwiały wykonywanie połączeń o podwyższonej opacie bez wiedzy użytkownika.

[1] VoIP (ang. Voice over Internet Protocol) – technologia cyfrowa umożliwiająca przesyłanie dźwięków mowy za pomocą łączy internetowych lub dedykowanych sieci wykorzystujących protokół IP, popularnie nazywana "telefonią internetową". Dane przesyłane są przy użyciu protokołu IP, co pozwala wykluczyć niepotrzebne "połączenie ciągłe" i np. wymianę informacji gdy rozmówcy milczą.

Drugim trendem, który przyczynił się w diametralny sposób do zmiany postrzegania przestępczości komputerowej, było opublikowanie informacji o robaku Stuxnet.

Stuxnet pokazał nowy kierunek w działaniach cyberprzestępców, tj. wykorzystywanie w jednym złośliwym oprogramowaniu (skierowanym przeciwko ściśle określonemu celowi) wielu podatności systemów na raz.

Trzecim zaobserwowanym nurtem, jest przeniesienie środka ciężkości ataków z wykorzystywania podatności w systemach operacyjnych na podatności w oprogramowaniu (zwłaszcza biurowym) uważanym do tej pory za bezpieczne. Typowym przykładem takiego zjawiska jest wykorzystywanie przez cyberprzestępców nowych, niepublikowanych błędów w oprogramowaniu Adobe Acrobat Reader służącym do czytania plików .pdf

Ochrona cyberprzestrzeni RP jest priorytetem w działaniach zespołu CERT.GOV.PL.

Temu celowi służy także rozwijanie współpracy z innymi zespołami CERT. Modelowym przykładem takiego współdziałania jest współpraca z zespołem reagowania na incydenty komputerowe w Wojskowym Biurze Bezpieczeństwa Łączności i Informatyki Ministerstwa Obrony Narodowej, Ministerstwem Spraw Zagranicznych oraz Ośrodkiem Studiów Wschodnich przede wszystkim w obszarze reagowania na ataki ukierunkowane oraz aktywnym uczestnictwem w projekcie ARAKIS-GOV.

Jednocześnie zespół CERT.GOV.PL ściśle współpracuje z różnymi instytucjami państwowymi uczestniczącymi w ARAKIS-GOV.

Pomimo podejmowanych działań w zakresie zmniejszania zagrożeń w cyberprzestrzeni, możliwości ścigania sprawców tego typu przestępstw, są ograniczone. Przeważająca większość spraw, zgodnie z obowiązującym prawodawstwem, jest ścigana na wniosek pokrzywdzonego. Powoduje to, iż w większości przypadków jednostki państwowe, które stały się celem działania cyberprzestępców, nie są w praktyce zainteresowane zgłaszaniem takich spraw do organów ścigania (vide Centralna Komisja Egzaminacyjna, Biuro Ochrony Rządu). Podejście to powoduje, że polscy cyberprzestępcy są praktycznie bezkarni. W ten sposób bezczynność jednostek administracji państwowej w obszarze zgłaszania przestępstw teleinformatycznych powoduje odczuwalne całościowe obniżenie bezpieczeństwa teleinformatycznego dla domeny gov.pl.

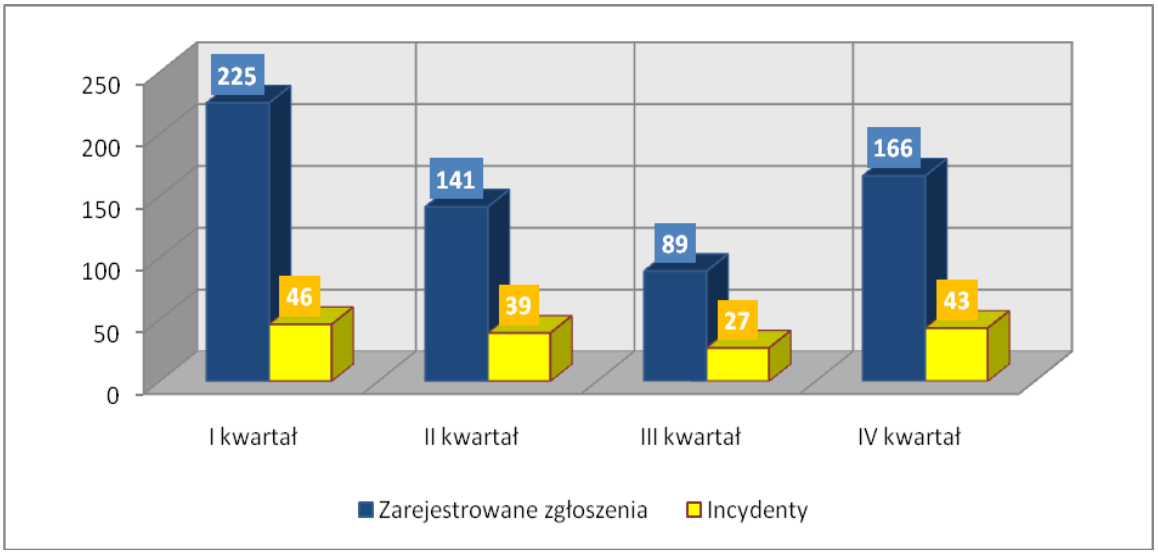
Jednocześnie na przestrzeni ostatnich lat, a szczególnie w roku 2010, zaobserwowano zmianę charakteru cyberzagrożeń, z ataków czysto kryminalnych, na ataki szpiegowskie, lub noszące znamiona cyber - wojny. Oznacza to przesunięcie środka ciężkości problematyki bezpieczeństwa teleinformatycznego z obszaru ochrony bezpieczeństwa i porządku publicznego, na obszar ochrony bezpieczeństwa państwa. Temu zagadnieniu poświęcony został Rozdział 3, traktujący o atakach ukierunkowanych, wykonywanych poprzez przesyłanie złośliwych załączników poczty elektronicznej w formatach oprogramowania biurowego.

W 2010 roku Rządowy Zespół Reagowania na Incydenty Komputerowe CERT.GOV.PL zacieśnił współpracę z zespołem *NATO Computer Incident Response Capability (NCIRC)*, co umożliwiło udział CERT.GOV.PL w ćwiczeniach *NATO Cyber Coallition 2010*.

2. Statystyki incydentów otrzymanych przez zespół CERT.GOV.PL w 2010 roku

2.1. Klasyfikacja zagrożeń

W roku 2010 zespół CERT.GOV.PL odnotował 621 zgłoszeń, z czego 155 zostało zakwalifikowanych jako faktyczne incydenty.

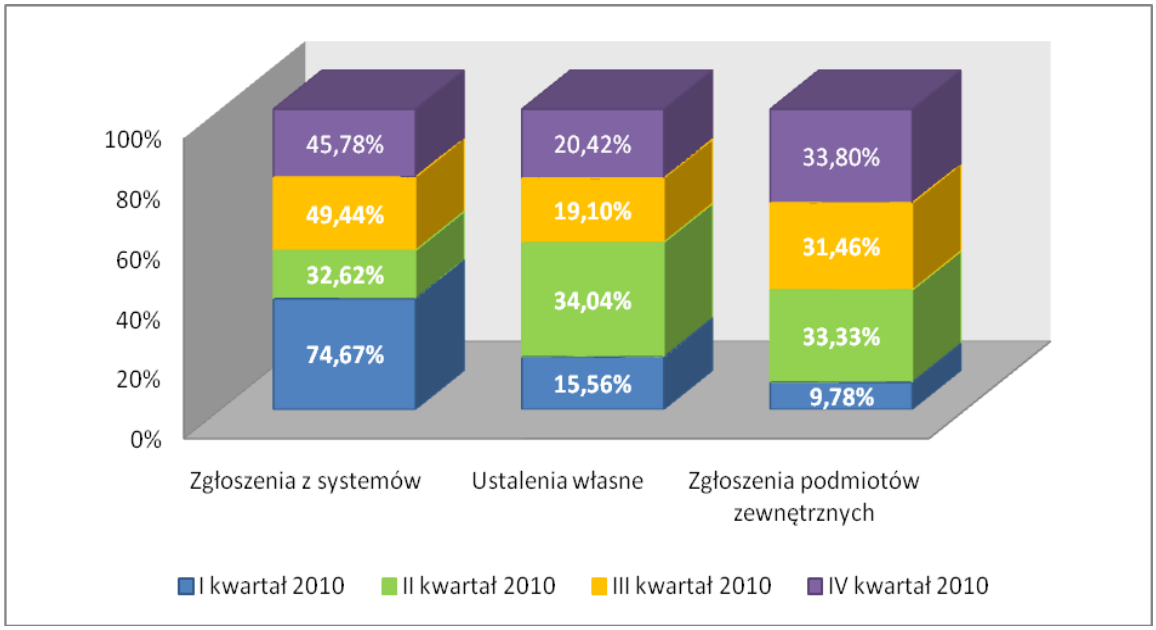


Rysunek 1 – Liczba zarejestrowanych oraz faktycznych incydentów w poszczególnych kwartałach 2010 roku

Znaczna różnica w liczbie zarejestrowanych zgłoszeń w stosunku do liczby faktycznych incydentów wynika z faktu, iż część z nich stanowią zgłoszenia typu. „false-positives", czyli przypadki błędnej interpretacji przez zgłaszającego legalnego ruchu sieciowego.

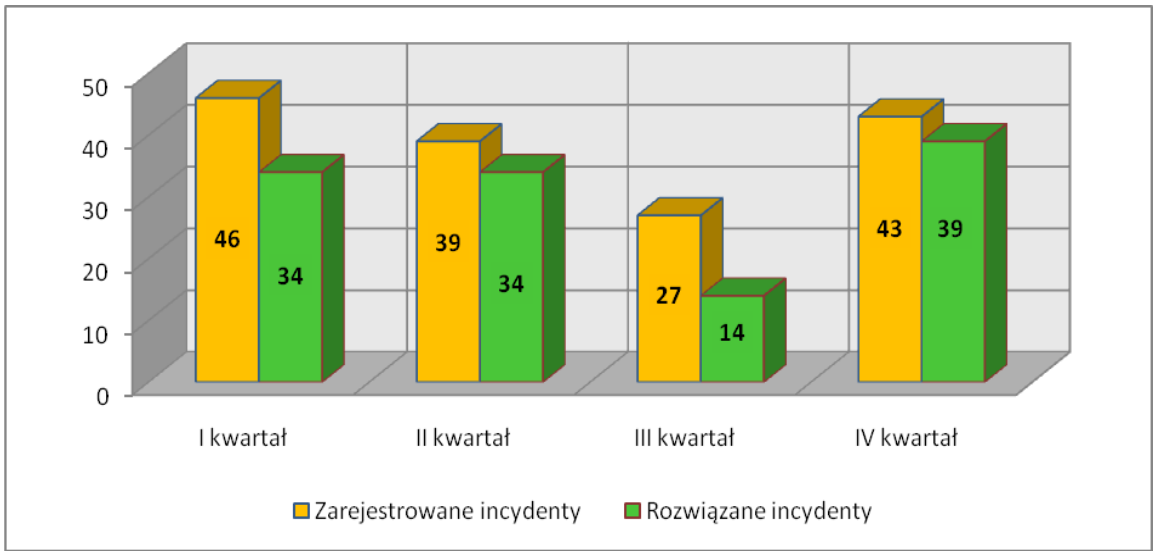
Ponadto należy zwrócić uwagę na fakt, iż większość zgłoszeń pochodzi z systemów autonomicznie raportujących zdarzenia, które w wyniku tego muszą zostać poddane później weryfikacji.

Poniżej przedstawione zostały szczegółowe statystyki źródeł zgłoszeń incydentów trafiających do CERT.GOV.PL.



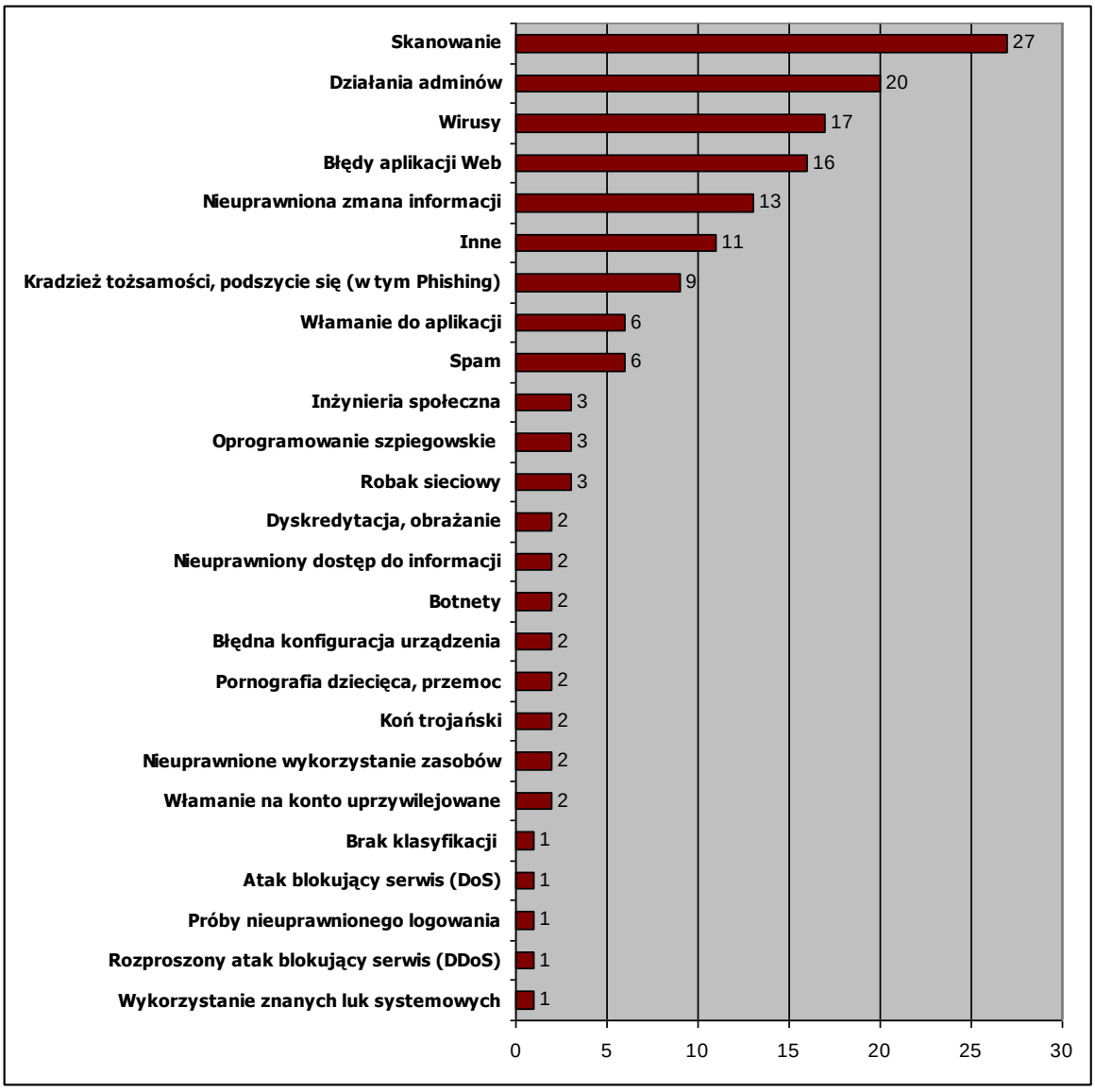
Rysunek 2 – Źródła zgłoszeń incydentów

Porównanie liczby incydentów otwartych i zamkniętych przez zespół CERT.GOV.PL w roku 2010 ilustruje poniższy rysunek.



Rysunek 3 – Porównanie liczby incydentów otwartych i zamkniętych w poszczególnych kwartałach 2010 roku

Podział zarejestrowanych incydentów na poszczególne kategorie przedstawia się następująco:

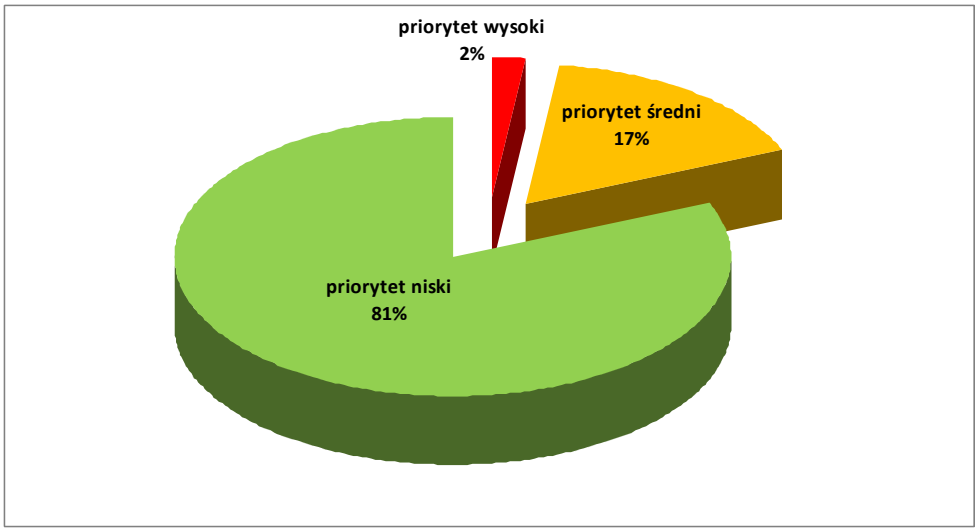


Rysunek 4 – Statystyka incydentów z podziałem na kategorie

Należy zaznaczyć, że dla wyników z IV kwartału 2010 roku uwzględniono dodatkowo zgłoszenia incydentów związane z uczestnictwem zespołu CERT.GOV.PL w ćwiczeniach NATO pod nazwą "Cyber Coalition 2010" (dokładniej opisane w pkt. 6.5). W związku z powyższym, ilość faktycznych incydentów z kwartału IV, jak również z całego 2010 roku, została powiększona o 9 incydentów szkoleniowych, które nie mają wpływu na stan faktyczny bezpieczeństwa teleinformatycznego polskiej przestrzeni adresowej.

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

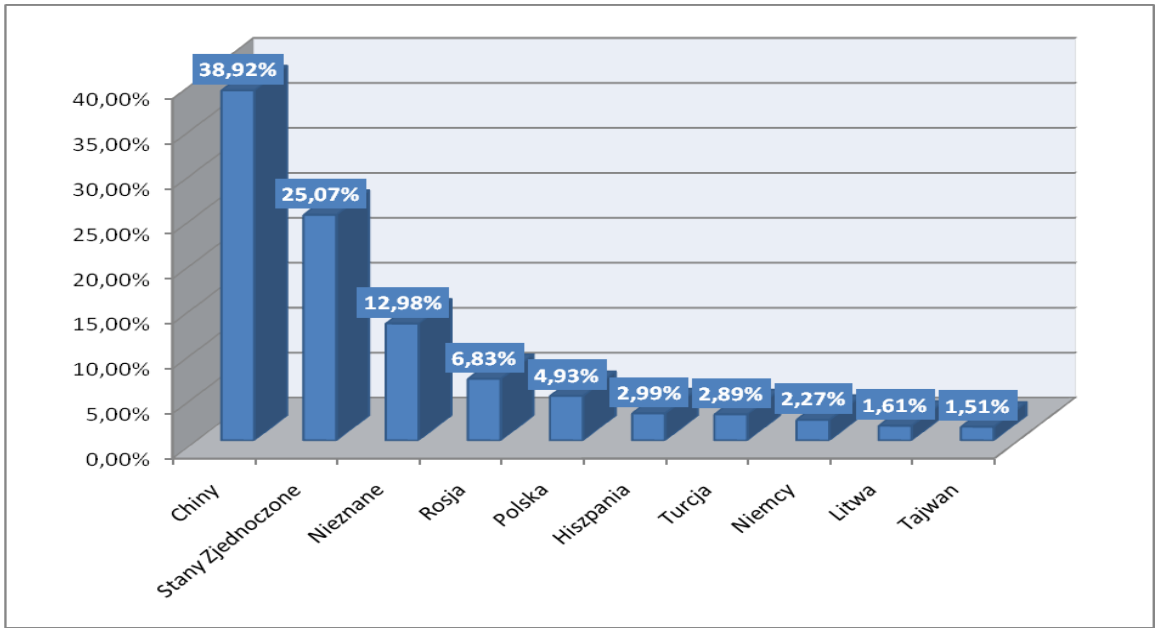
System ARAKIS-GOV[2] w roku 2010 zaraportował 28109 alarmów o różnym priorytecie ważności. Większość alarmów posiadała niski priorytet (69%) – alarmy świadczące o wykryciu pewnej anomalii w ruchu sieciowym. Następne w kolejności były alarmy o priorytecie średnim (14%) – alarmy mówiące o anomalii w ruchu sieciowym, co do których istnieje duże prawdopodobieństwo, iż są to zagrożenia sieciowe. Najmniej było alarmów informujących o wykryciu nowego poważnego zagrożenia w monitorowanych przez system sieciach (2%).



Rysunek 5: Rozkład procentowy alarmów ze względu na priorytety.

Na podstawie informacji zebranych przez system ARAKIS-GOV w roku 2010 określono lokalizacje geograficzną źródłowych adresów IP, z których wykonywano ataki na polskie sieci rządowe monitorowane przez system. W czołówce napastników znajdują się adresy zlokalizowane w państwach: Chiny (≈39%) i Stany Zjednoczone (≈25%), co nie dobiega od ogólnoświatowych trendów.

[2] 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.

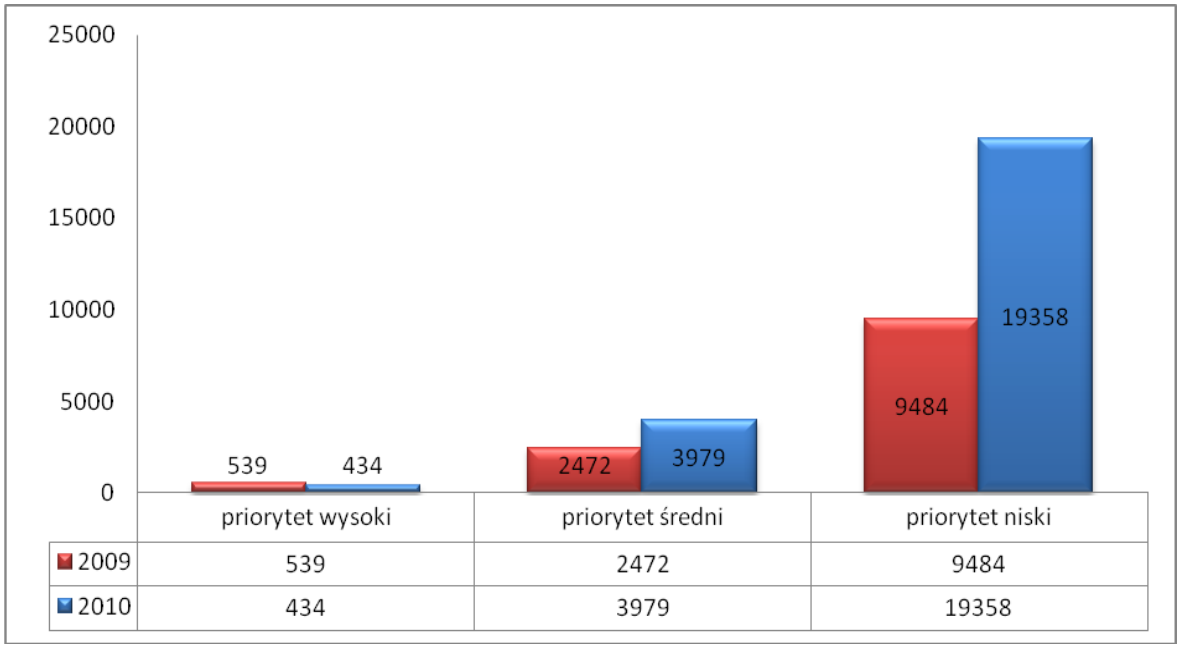


Rysunek 6: Rozkład procentowy źródeł ataków na monitorowane sieci przez system ARAKIS-GOV

W powyższym wykresie dotyczącym statystyk źródeł ataków na monitorowane przez system ARAKIS-GOV sieci na trzecim miejscu znajduje się pozycja „Nieznane". Określenie to dotyczy adresów IP w chwili obecnej nieprzypisanych żadnemu podmiotowi – oznacza to, iż dokonano podszycia się (podmiany adresu źródłowego IP) pod nieistniejący adres IP.

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

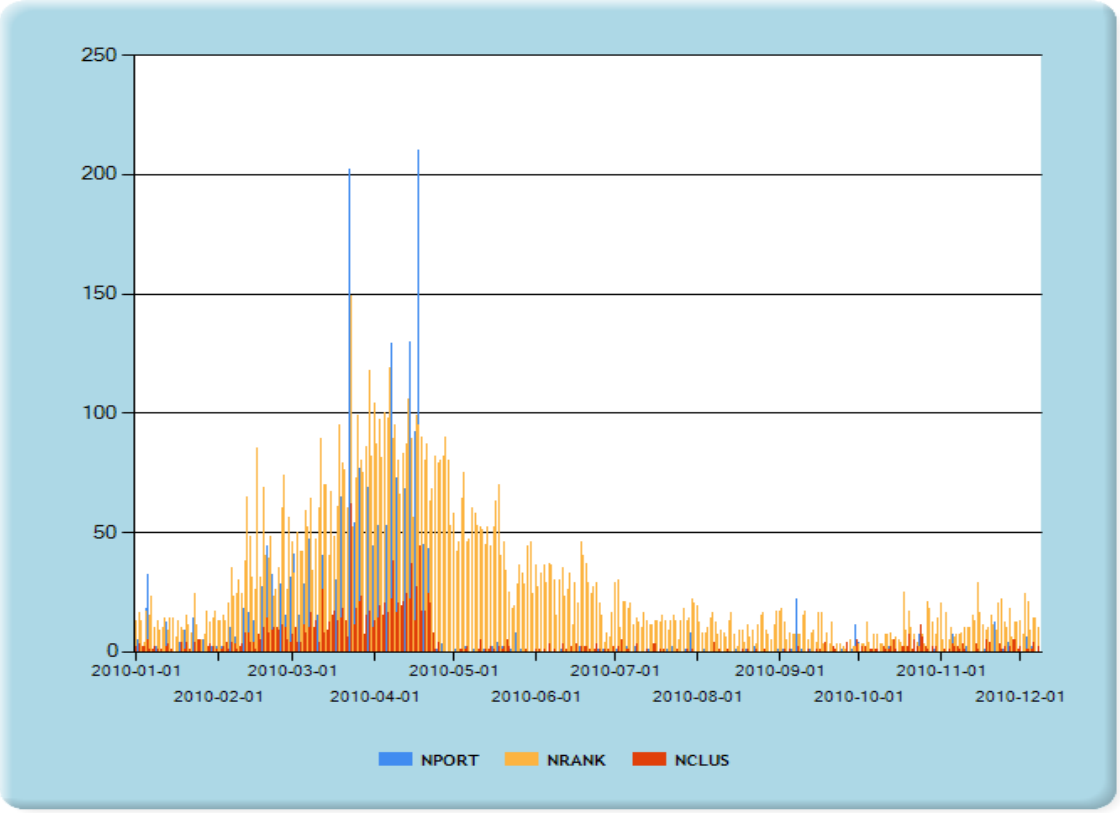
W stosunku do roku poprzedniego w roku 2010 system ARAKIS-GOV odnotował dwa razy większą ilość alarmów (28109), jednakże mniejszą ilość alarmów o priorytecie „wysokim". Zdecydowana przewaga widoczna jest w stosunku do alarmów o priorytecie „niskim".



Rysunek 7: Rozkład alarmów ze względu na priorytety w latach 2009-2010

Tak duża różnica w alarmach o priorytecie „niskim", spowodowana była obserwacją wzrostu ruchu typu BitTorrent[3] na przełomie miesiąca marca i kwietnia 2010 r. Na dalszym etapie obserwacji stwierdzono, że ruch ten zaburza obraz aktualnej sytuacji w monitorowanych sieciach, dlatego też wprowadzono filtry w systemie w celu eliminacji alarmów związanych z uznanym za nieszkodliwy ruch BitTorrent. Poniższy wykres przedstawia odnotowany wzrostu ruchu typu BitTorrent w skali ostatniego roku.

[3] BitTorrent – protokół wymiany i dystrybucji plików przez Internet, którego celem jest odciążenie łączy serwera udostępniającego pliki. Jego największą zaletą w porównaniu do protokołu HTTP jest podział pasma pomiędzy osoby, które w tym samym czasie pobierają dany plik. Oznacza to, że użytkownik w czasie pobierania wysyła fragmenty pliku innym użytkownikom. Ruch sieciowy dotyczący usług współdzielenia plików z zasady nie powinien być obserwowany w systemach administracji publicznej. Sytuacja zaobserwowana przez system ARAKIS-GOV może mieć zarówno charakter przypadkowego skanowania sieci przynależących do administracji publicznej, jak i świadczyć o działających w przeszłości usługach współdzielenia plików w tych sieciach.



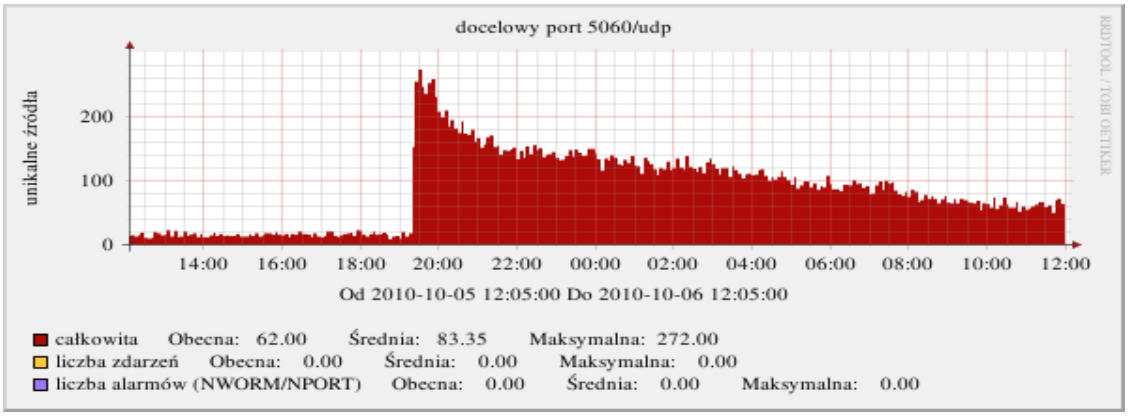
Rysunek 8: Ruch BitTorrent zarejestrowany w 2010 r.

Na wykresie uwzględniono alarmy ARAKIS-GOV typu NPORT, NRANK, NCLUS, świadczące o wykryciu nowego portu w statystykach przez system i wygenerowaniu nowej sygnatury potencjalnego zagrożenia.

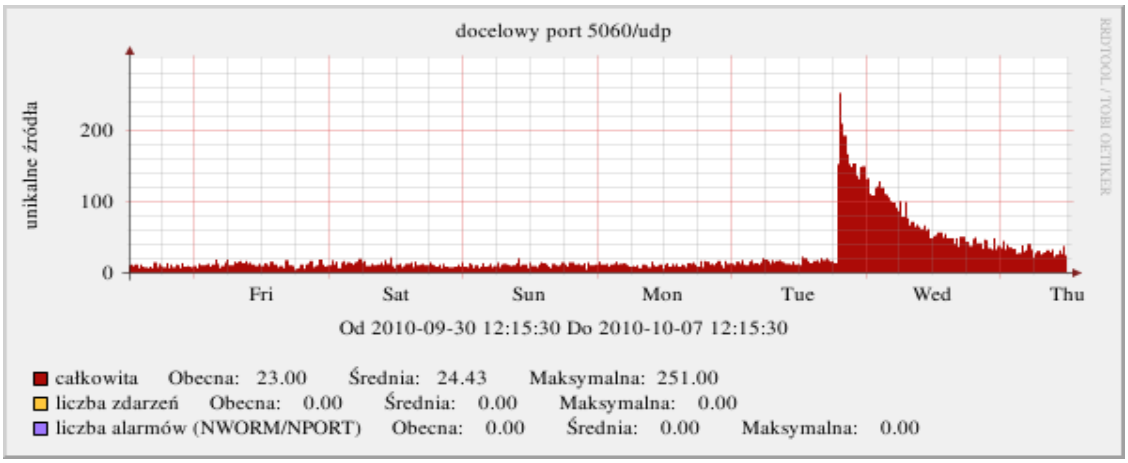
W październiku 2010 roku, system ARAKIS-GOV zaobserwował wzrost ruchu na porcie 5060/UDP (Session Initiation Protocol)[4] – jeden z protokołów w technologii VoIP. Przedmiotowy wzrost widoczny był zarówno w lokalizacjach chronionych systemem jak i w przestrzeniach adresowych Darknetu[5]. Poniżej przedstawione są wykresy obrazujące powyższą sytuację:

[4] Protokół opisany w RFC 3261. Służy on do kontrolowania sesji pomiędzy klientami VoIP, w szczególności do nawiązywania, modyfikowania oraz kończenia połączeń głosowych, a także wideo. Protokół SIP ma zdefiniowany zestaw metod (żądań).

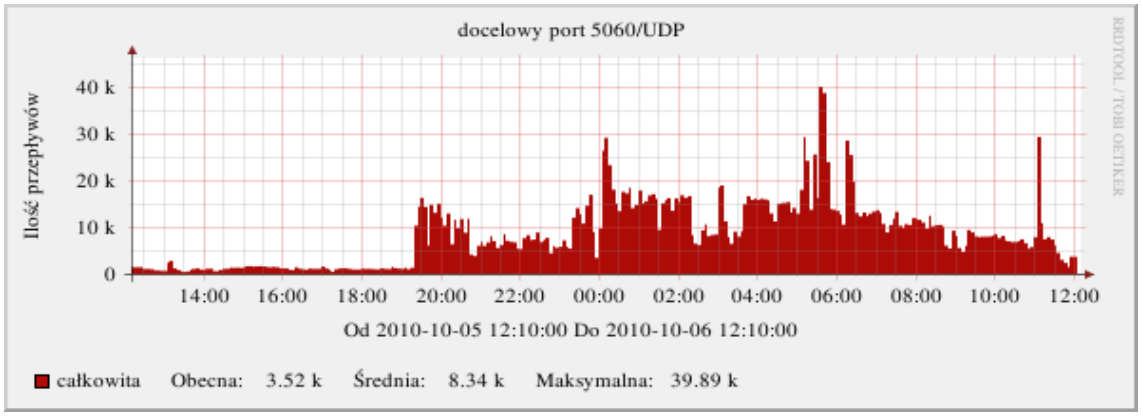
[5] Darknet – duży blok publicznych, niewykorzystywanych adresów IP, które zwykle są w posiadaniu dostawców Internetu (np.: NASK).



Rysunek 9: Rozkład ruchu na porcie 5060/UDP w okresie doby w której nastąpiła anomalia na podstawie danych z lokalizacji chronionych systemem



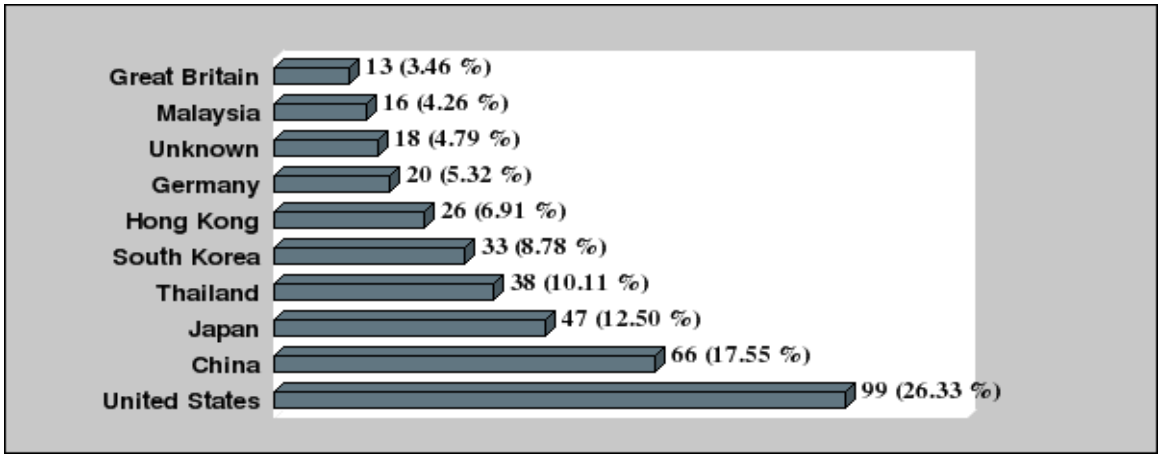
Rysunek 10: Rozkład ruchu na porcie 5060/UDP w okresie 1 tygodnia w którym nastąpiła anomalia na podstawie danych z lokalizacji chronionych systemem



Rysunek 11: Rozkład ruchu na porcie 5060/UDP w okresie doby w której nastąpiła anomalia na podstawie danych z sieci DARKNET

Ruch został zaobserwowany z ponad 400 unikalnych źródłowych adresów IP i kierowany był na ponad 1560 unikalnych adresów docelowych będących monitorowanym przez system ARAKIS-GOV. Na podstawie analizy geolokalizacji źródłowych adresów IP będących inicjatorem powyższego ruchu, stwierdzono, iż

w pierwszej trójce pochodzenia pakietów znalazły się takie państwa jak Stany Zjednoczone około 26% źródłowych adresów IP, Chiny – 18% i Japonia – 12%.



Rysunek 12: Źródło pochodzenia ruchu na porcie 5060/UDP

Istnieje prawdopodobieństwo, iż adresy źródłowe IP mogły być sfałszowane ze względu na specyfikę protokołu UDP (UDP spoofing). Jednakże spoofowanie adresów wydaje się bezużyteczne dla atakującego, ze względu na brak możliwości otrzymania odpowiedzi oraz informacji o opcjach pracy serwera SIP.

Przedmiotowa sytuacja była wynikiem skanowania w poszukiwaniu serwerów SIP. W tym celu wykorzystano żądania OPTION protokołu SIP, które pozwalają w odpowiedzi uzyskać informacje o opcjach pracy serwera. Powyższe dane zbierane były najprawdopodobniej w celu wykorzystania do ataku na serwery SIP (VoIP). Ponadto informacje tego typu dostarczają także wiedzy na temat oprogramowania, w oparciu o które działa serwer SIP.

Skala zaobserwowanego zjawiska była widoczna na całym świecie, o czym świadczyło wiele informacji zawartych w sieci Internet. Pierwsze oznaki wzrostu ruchu związanego z powyższym portem zaobserwowane były już w lipcu w 2010 roku.

Poniżej znajduje się wycinek komunikacji zaobserwowanej przez system ARAKIS-GOV generowany przez narzędzie atakującego:

```
10:07:13.360315 IP 221.130.119.174.5060 > 195.187.xxx.xxx.5060: SIP, length: 411
        0x0000:  4500 01b7 0000 4000 2a11 ca24 dd82 77ae  E.....@.*..$..w.
        0x0010:  c3bb 6c25 13c4 13c4 01a3 199e 4f50 5449  ..l%........OPTI
        0x0020:  4f4e 5320 7369 703a 3130 3040 3139 352e  ONS.sip:100@195.
        0x0030:  3138 372e xxxx xx2e xxxx 2053 4950 2f32  187.xxx.xx.SIP/2
        0x0040:  2e30 0d0a 5669 613a 2053 4950 2f32 2e30  .0..Via:.SIP/2.0
        0x0050:  2f55 4450 2031 3932 2e31 3638 2e31 2e39  /UDP.192.168.1.9
```

```
0x0060:  3a35 3036 303b 6272 616e 6368 3d7a 3968  :5060;branch=z9h
0x0070:  4734 624b 2d36 3832 3333 3437 333b 7270  G4bK-68233473;rp
0x0080:  6f72 740d 0a43 6f6e 7465 6e74 2d4c 656e  ort..Content-Len
0x0090:  6774 683a 2030 0d0a 4672 6f6d 3a20 2273  gth:.0..From:."s
0x00a0:  6970 7373 6375 7365 7222 3c73 6970 3a31  ipsscuser"<sip:1
0x00b0:  3030 4031 3932 2e31 3638 2e31 2e39 3e3b  00@192.168.1.9>;
0x00c0:  2074 6167 3d35 3833 3235 3134 3330 3330  .tag=58325143030
0x00d0:  3136 3234 3135 3634 3734 3433 3938 3339  1624156474439839
0x00e0:  3336 3530 3237 3236 3832 3630 3931 3830  3650272682609180
0x00f0:  3039 3532 0d0a 4163 6365 7074 3a20 6170  0952..Accept:.ap
0x0100:  706c 6963 6174 696f 6e2f 7364 700d 0a55  plication/sdp..U
0x0110:  7365 722d 4167 656e 743a 2073 756e 6461  ser-Agent:.sunda
0x0120:  7964 6472 0d0a 546f 3a20 2273 6970 7373  yddr..To:."sipss
0x0130:  6322 3c73 6970 3a31 3030 4031 3932 2e31  c"<sip:100@192.1
0x0140:  3638 2e31 2e39 3e0d 0a43 6f6e 7461 6374  68.1.9>..Contact
0x0150:  3a20 7369 703a 3130 3040 3139 322e 3136  :.sip:100@192.16
0x0160:  382e 312e 393a 3530 3630 0d0a 4353 6571  8.1.9:5060..CSeq
0x0170:  3a20 3120 4f50 5449 4f4e 530d 0a43 616c  :.1.OPTIONS..Cal
0x0180:  6c2d 4944 3a20 3036 3237 3838 3239 3437  l-ID:.0627882947
0x0190:  3939 3736 3639 3930 3635 3435 3136 3134  9976699065451614
0x01a0:  390d 0a4d 6178 2d46 6f72 7761 7264 733a  9..Max-Forwards:
0x01b0:  2037 300d 0a0d 0a                        .70....
```

```
Session Initiation Protocol
  Request-Line: OPTIONS sip:100@195.187.      SIP/2.0
    Method: OPTIONS
    Request-URI: sip:100@195.187
      Request-URI User Part: 100
      Request-URI Host Part: 195.187.
    [Resent Packet: False]
  Message Header
    Via: SIP/2.0/UDP 192.168.1.9:5060;branch=z9hG4bK-68233473;rport
    Content-Length: 0
    From: "sipsscuser"<sip:100@192.168.1.9>; tag=583251430301624156474439839365027268260918009 52
      SIP Display info: "sipsscuser"
      SIP from address: sip:100@192.168.1.9
        SIP from address User Part: 100
        SIP from address Host Part: 192.168.1.9
      SIP tag: 583251430301624156474439839365027268260918009 52
    Accept: application/sdp
    User-Agent: sundayddr
    To: "sipssc"<sip:100@192.168.1.9>
      SIP Display info: "sipssc"
      SIP to address: sip:100@192.168.1.9
        SIP to address User Part: 100
        SIP to address Host Part: 192.168.1.9
    Contact: sip:100@192.168.1.9:5060
      Contact-URI: sip:100@192.168.1.9:5060
        Contactt-URI User Part: 100
        Contact-URI Host Part: 192.168.1.9
        Contact-URI Host Port: 5060
    CSeq: 1 OPTIONS
      Sequence Number: 1
      Method: OPTIONS
    Call-ID: 06278829479976690654516149
    Max-Forwards: 70
```

Rysunek 13: Przykładowy pakiet SIP na porcie 5060/

Charakterystyczną cechą zaobserwowanej komunikacji były następujące elementy:

- numer sekwencyjny żądania (CSeq) = 1
- User-Agent = sundayddr – świadczący o wykorzystaniu popularnego narzędzia do audytu urządzeń VoIP.

Warto zauważyć, iż pod koniec lipca 2010 roku, zespół CERT.GOV.PL został poinformowany o incydencie mającym miejsce w jednym z Urzędów Miasta polegającym na kradzieży impulsów telekomunikacyjnych. Na podstawie danych uzyskanych od administratora sieci lokalnej UM wynikało, iż kradzieży dokonano poprzez włamanie na konto uprzywilejowane, które zabezpieczone było słabym hasłem. Konsekwencją powyższego incydentu było wykonanie połączeń na koszt UM o łącznym czasie 740280 sekund (206 godzin = 8,5 dni). Oszacowane przez Urząd Miasta straty z tytułu nieautoryzowanych połączeń telefonicznych wynosiły około 60000 PLN. Ataki tego typu w opinii CERT.GOV.PL będą przeprowadzane coraz częściej, wykorzystując niewiedzę administratorów dokonujących wdrożeń telefonii internetowej VoIP. Bezpieczeństwu implementacji rozwiązań VoIP poświęcony jest punkt 6.4 niniejszego raportu. Przedstawiono w nim rekomendacje dotyczące dobrych praktyk przy wdrażaniu tego typu technologii.

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.

Ważniejsze ministerstwa, których witryny zostały przebadane przez zespół CERT.GOV.PL to:

1. Ministerstwo Spraw Wewnętrznych i Administracji
2. Kancelaria Prezydenta RP
3. Centrum Obsługi Kancelarii Prezesa RM
4. Ministerstwo Spraw Zagranicznych
5. Ministerstwo Infrastruktury
6. Ministerstwo Finansów
7. Ministerstwo Edukacji Narodowej

8. Ministerstwo Pracy i Polityki Społecznej
9. Ministerstwo Sprawiedliwości

Ponadto testom zostały poddane strony WWW innych ważnych instytucji takich jak:

1. Centralne Biuro Antykorupcyjne
2. Ministerstwo Obrony Narodowej
3. Komenda Główna Policji
4. Kancelaria Polskiej Akademii Nauk
5. Prokuratura Okręgowa w Bydgoszczy
6. Państwowa Komisja Wyborcza
7. strony WWW należące do Ministerstwa Finansów (Izby Celne i Urzędy Skarbowe)

W trakcie skanowania witryn stwierdzono, że 75% 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.

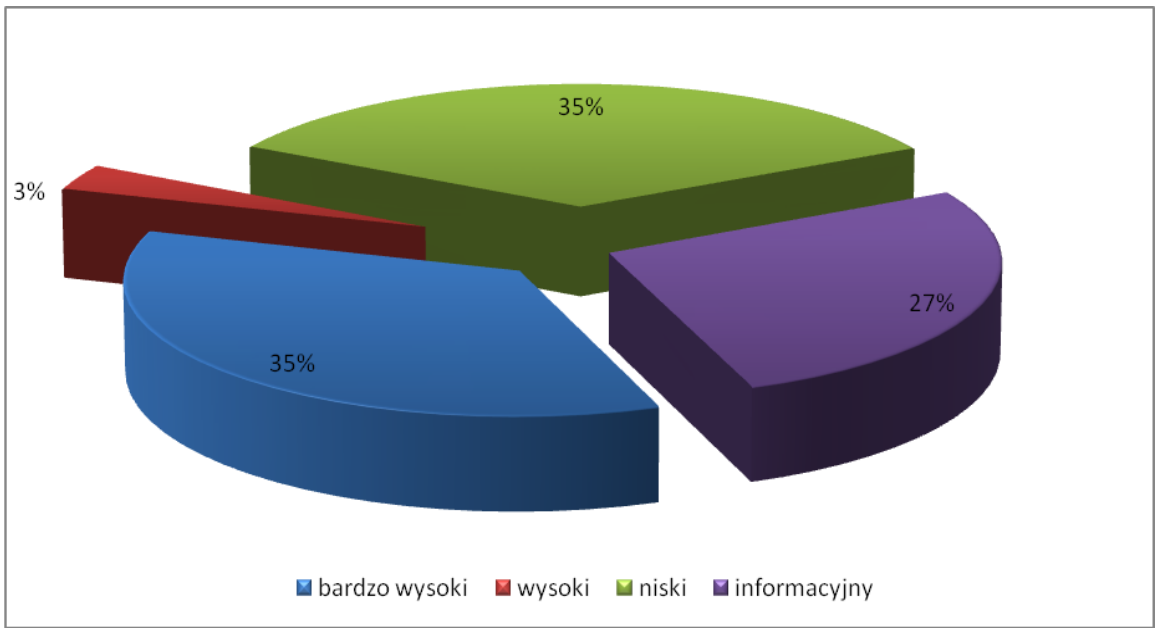
Na podstawie dotychczasowych badań można wskazać następujące przyczyny słabego zabezpieczenia stron WWW polskich instytucji państwowych:

- Niska świadomość administratorów oraz twórców witryn zagrożeń istniejących w Internecie.
- Małe doświadczenie i wiedza osób odpowiadających za administrowanie systemami.
- Brak zrozumienia dla konieczności bezwzględnej ochrony systemów wśród osób decyzyjnych oraz braku wsparcia dla administratorów systemów przez kadrę kierowniczą instytucji.
- Kierowanie się wyłącznie kryterium ceny podczas wyboru firmy wynajmowanej do stworzenia witryny i/lub późniejszego jej utrzymania bez odpowiedniego doświadczenia w tym zakresie.

Rekomendacje do sformułowanej powyżej diagnozy zawarto w punkcie 6.1.

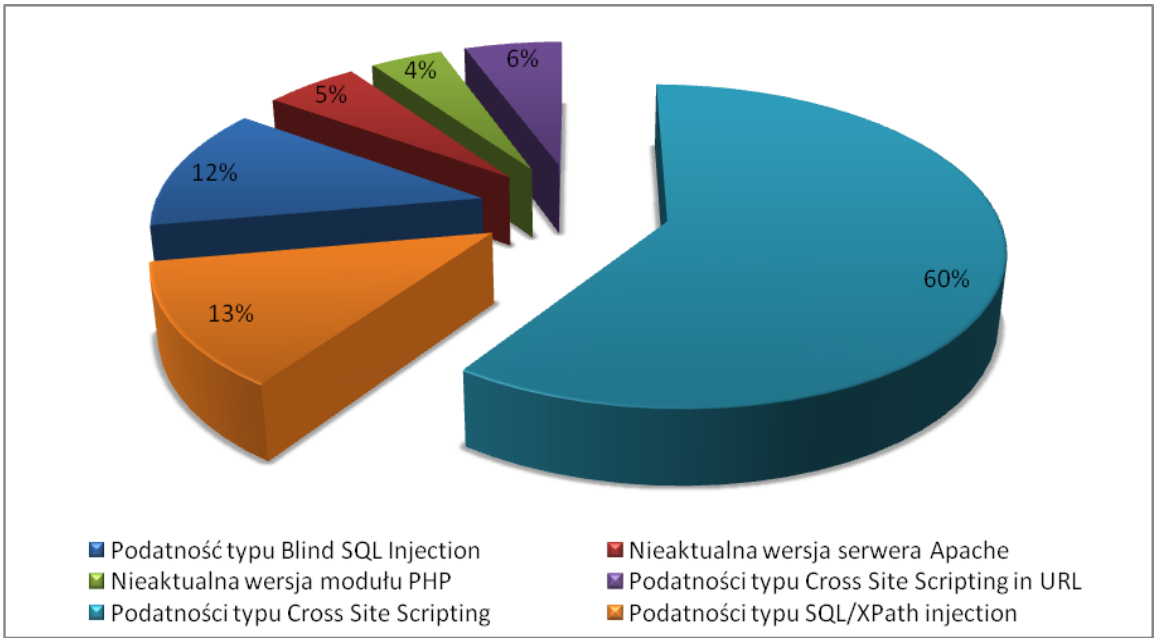
Bardzo niski poziom zabezpieczeń przebadanych witryn pozwala przypuszczać, że znacząca większość systemów instytucji administracji publicznej w Polsce może być źle chroniona lub może zawierać informacje podatne na zagrożenie dla bezpieczeństwa publikowanych treści. Świadczy to o konieczności dalszego prowadzenia audytów bezpieczeństwa witryn internetowych instytucji publicznych, jak również opracowania i wdrożenia spójnej polityki bezpieczeństwa dla witryn administracji publicznej.

W 2010 roku przebadano 93 witryny należące do 63 instytucji państwowych. Stwierdzono ogółem 1277 błędów w tym: 451 błędów o bardzo wysokim poziomie zagrożenia, 40 błędów o wysokim poziomie zagrożenia, 440 błędy o niskim poziomie zagrożenia i 346 błędów oznaczonych jako informacyjne.



Rysunek 14: 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, Blind SQL Injection oraz SQL/XPath Injection. Istotnym problemem jest również wykorzystywanie w serwerach produkcyjnych nieaktualnych wersji oprogramowania.



Rysunek 15: 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: Przykłady przebadanych witryn instytucji pod względem ilości krytycznych błędów.

Stan bezpieczeństwa przebadanych witryn	Instytucja
Bardzo dobry poziom bezpieczeństwa	Centrum Obsługi Kancelarii Prezesa RM
	Prokuratura Okręgowa w Bydgoszczy
	Urząd Kontroli Skarbowej w Białymstoku
	Urząd Kontroli Skarbowej w Katowicach
	Urząd Kontroli Skarbowej w Olsztynie
	Urząd Kontroli Skarbowej w Poznaniu
Średni poziom bezpieczeństwa	Krajowa Rada Radiofonii i Telewizji
	Izba Skarbowa w Gdańsku
	Ministerstwo Sprawiedliwości
	Państwowy Instytut Geologiczny
	Urząd Komunikacji Elektronicznej
Niski poziom bezpieczeństwa	Izba Skarbowa w Krakowie
	Rządowe Centrum Legislacji
	Polska Agencja Rozwoju Przedsiębiorczości
	Centralny Ośrodek Geodezji i Kartografii
	Izba Skarbowa w Katowicach

Niski poziom bezpieczeństwa powyższych witryn wynika z wykrytych podatności:

PODATNOŚCI TYPU SQL/XPATH INJECTION

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

Kod aplikacji powinien filtrować dane wprowadzane przez użytkownika strony, eliminując znaki specjalne takie jak znaki końca polecenia SQL „;", znaki komentarza „--" itp. Warto również upewnić się, że moduł mod_security jest uruchomiony na serwerze PHPi zasymulować próbę

PODATNOŚĆ TYPU BLIND SQL INJECTION

Blind SQL injection jest podatnością pozwalająca atakującemu podmienić strukturę logiczną zapytania SQL kierowanego do produkcyjnej bazy danych, z której korzysta witryna WWW. Zagrożenie występuje, gdy aplikacja dane otrzymane od użytkownika strony dołącza do zapytania SQL bez filtrowania go z niedozwolonych znaków. Podatność nie pozwala w bezpośredni sposób uzyskać informacji z bazy danych, jednakże metodą prób i błędów w skrajnych wypadkach można uzyskać nazwy tabel lub pól, typ danych w wybranej kolumnie i innych informacji o bazie danych co może bardzo ułatwić złośliwemu użytkownikowi przygotowanie ekstremalnie groźnego ataku na bazę danych witryny.

Kod aplikacji powinien filtrować dane wprowadzane przez użytkownika strony, eliminując znaki specjalne takie jak znaki końca polecenia SQL „;", znaki komentarza „--" itp. Warto również upewnić się, że moduł mod_security jest uruchomiony na serwerze PHP i zasymulować próbę ataku, aby zaobserwować reakcję mechanizmu obronnego na ten atak.

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.

Należy filtrować dane przesłane przez użytkownika z ewentualne występujących znaków CR(0x13) i LF(0x10) (%0d%0a).

PODATNOŚĆ TYPU FILE INCLUSION

Skrypt witryny próbuje dołączyć plik używając nazwy pobranej od użytkownika. Dana pobrana od użytkownika nie jest właściwie filtrowana przed wstawieniem jej do funkcji typu include. Podatność ta umożliwia złośliwemu użytkownikowi dołączenie lokalnego lub zdalnego pliku co w efekcie może zaowocować wykonaniem złośliwego kodu na prawach usługi serwera WWW.

Należy bardzo dokładnie filtrować dane pobrane w celu określenia nazwy pliku do dołączenia. Jeżeli to możliwe należy stworzyć listę plików, która weryfikuje poprawność podanej przez użytkownika nazwy i odrzucać żądania dołączenia plików z poza tej listy. Należy również zwrócić uwagę czy serwer WWW umożliwia otwieranie zdalnych plików (Apache - allow_url_fopen). Zalecane jest by możliwość taka była zablokowana w pliku konfiguracyjnym serwera WWW (Apache - php.ini).

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 ta występuje w sytuacji, gdy programista stosuje dynamiczne dołączanie plików w zależności od akcji podjętej przez użytkownika. Jest to bardzo ryzykowny sposób pisania aplikacji i jeżeli nie ma innego wyjścia niż skorzystania z niego, należy filtrować dane pobierane od użytkownika na obecność niedozwolonych znaków. Dobrym rozwiązaniem jest również utworzenie listy dozwolonych plików do dołączenia (stosowanie białych list) i odrzucanie żądań do plików z poza tej listy.

3. Ataki ukierunkowane

Jednostki administracji publicznej, w odróżnieniu od indywidualnych użytkowników cyberprzestrzeni, są szczególnie narażone na jeden z typów wrogich działań tj. na ataki ukierunkowane. Ten typ ataków polega najczęściej na próbie nakłonienia użytkownika do otwarcia złośliwego załącznika w poczcie e-mail, bądź odwiedzenia lokalizacji z umieszczonego w treści odnośnika i w efekcie infekcji złośliwym oprogramowaniem (tzw. „*drive-by-download*").

W roku 2010 coraz częściej rejestrowano ataki ukierunkowane wykorzystujące także metody socjotechniczne, takie jak spersonalizowana przesyłka wysłana z adresu, do którego odbiorca ma zaufanie (przy czym adres nadawcy jest sfałszowany), zawartość zawierająca interesujące treści z punktu widzenia odbiorcy. Trend ten znacznie się nasilił po Tragedii Smoleńskiej. CERT.GOV.PL uzyskał informacje o wielu przypadkach otrzymania fałszywych wiadomości email z informacjami dotyczącymi katastrofy, bądź prowadzonego dochodzenia.

Efektem udanych ataków tego typu jest często masowa infekcja maszyn, która może bardzo skutecznie pozyskiwać dane wrażliwe użytkowników (*Gh0stRat*, *Zbot/Zeus*), czy destabilizować pracę systemów i sieci teleinformatycznych (*Stuxnet*).

3.1. Złośliwe załączniki PDF

2010 rok to znaczny wzrost masowej wysyłki wiadomości mailowych z załącznikami zawierającymi złośliwe oprogramowanie. Załącznikami najczęściej były pliki .pdf, bądź pliki pakietu MS Office – głównie MS Word i MS Excel. Należy zauważyć, że często zawarty złośliwy kod był wykrywany jedynie przez nieliczne systemy antywirusowe co powodowało, iż moment infekcji mógł pozostać niezauważony.

W maju 2010 roku miał miejsce atak ukierunkowany na Ministerstwo Spraw Zagranicznych. Opierał się na masowej wysyłce wiadomości mailowych do pracowników MSZ. Wiadomość tego typu została wysłana na 192 adresy pracowników zarówno centrali jak i placówek zagranicznych. Wiadomość stanowiła próbę podszycia się pod pracownika pomocy technicznej i zawierała prośbę o podanie nazwy użytkownika, adresu email, hasła oraz numeru telefonu. Wiadomość wysyłano z maszyny przypisanej do Danii. Według otrzymanych informacji z duńskiego zespołu CERT, wspomniany host został przejęty przez cyberprzestępców.

We wrześniu 2010 do pracowników MSZ przesyłano wiadomości email zawierające załącznik „Military Operation of the EU – EU NAVFOR Somalia.pdf". Załączony plik zawierał złośliwe oprogramowanie. Wspomniana wiadomość została wysłana również do innych pracowników zagranicznych agencji rządowych. Wiadomość wysłano z bezpłatnej skrzynki pocztowej, a adres IP wskazywał na Chiny.

W listopadzie 2010 r. miał miejsce atak ukierunkowany również na MSZ. Wiadomości zawierały załączony zainfekowany złośliwym oprogramowaniem plik .pdf. Wiadomość również była adresowana do użytkowników MSZ, natomiast sfałszowanym nadawcą był członek Komitetu Unii Europejskiej. Według nagłówków pocztowych prawdziwym źródłem wiadomości była maszyna przypisana do terenów Federacji Rosyjskiej.

Listopad 2010 r. to także atak mailowy ukierunkowany na MON. Sfałszowany adres nadawcy należał do Ministerstwa Ochrony Środowiska i zawierał plik o nazwie „NATO ma już gotowe nowe plany obrony Polski i krajów nadbałtyckich". Analiza wykazała, iż oryginalnym źródłem ataku była maszyna przypisana do Bułgarii. Dalsze czynności wykazały także, iż pod wzmiankowanym adresem IP podłączony był najprawdopodobniej jedynie przejęty przez cyberprzestepców host wykorzystywany do tego typu ataków. Dalsza analiza wykazała, iż zawarty w załączniku złośliwy kod wykorzystywał lukę „0-day" w aplikacji Adobe Reader ponadto, wykorzystane złośliwe oprogramowanie wykorzystywało bibliotekę, pozwalającą na ukrycie się w systemie. Co warte podkreślenia to fakt, że w momencie ataku złośliwy kod był rozpoznawany jedynie przez trzy silniki antywirusowe.

W grudniu 2010 r. odnotowano także masowe rozsyłanie wiadomości mailowych mających swoje źródło w Federacji Rosyjskiej, a adresowane do kilku instytucji administracji publicznej, m.in.: MSZ i ABW. Wiadomości zawierały zainfekowane załączniki w postaci plików .pdf, bądź pakietu MS Office, a w tytule omawiały sytuację m.in. wojsk NATO: „Rogozin Condemns secret NATO Pact" lub informacje dotyczące portalu WikiLeaks i szczegółów aresztowania jego założyciela – Juliana Assange.

3.2. Socjotechnika w atakach ukierunkowanych.

W roku 2010 coraz częściej rejestrowano ataki ukierunkowane wykorzystujące metody socjotechniczne. Wektor ataku to najczęściej masowa wysyłka wiadomości mailowych do dokładnie określonych odbiorców. Nadawcy natomiast to sfałszowane

adresy mailowe należące do użytkowników polskiej administracji publicznej, bądź wojskowej. Wiadomości - temat, treść, jak i zawartość samego załącznika - były odpowiednio spreparowane, a merytorycznie zawierały informacje kierowane dokładnie pod wybrany „cel". Dla przykładu wiadomości kierowane do sektora wojskowego mogły w treści omawiać np. sytuację NATO i jej najbliższe plany związane z modernizacją wojsk Sojuszu, natomiast wiadomości kierowane do Ministerstwa Spraw Zagranicznych zawierały komentarze, analizy oraz wnioski związane z ostatnimi wydarzeniami na arenie geopolitycznej. Wykorzystywane były zarówno wydarzenia społeczne (jak katastrofa w Smoleńsku) jak i lokalne (konferencja bezpieczeństwa w Tallinie).

Drugą, ale również bardzo ważną stroną wspomnianych ataków, są techniki już „czysto" informatyczne. W zaobserwowanych atakach używano złośliwego oprogramowania również wykorzystujące podatności typu „*0-day*" na popularne aplikacje, a sam złośliwy kod w momencie ataku jest wykrywany jedynie przez nieliczne systemy antywirusowe.

Jeden z analizowanych przez zespół CERT.GOV.PL incydentów tego typu wykazał, iż oryginalnym źródłem ataku była maszyna przypisana do Bułgarii, a nie jak wynikałoby z adresów email nadawcy, host należący do polskiej administracji publicznej. Dalsze czynności wykazały także, iż pod wzmiankowanym adresem IP podłączony był najprawdopodobniej jedynie przejęty przez cyberprzestepców host wykorzystywany do tego typu ataków. Dodatkowo ustalono, iż zawarty w załączniku złośliwy kod wykorzystywał lukę „*0-day*[6]" na aplikację Adobe Reader (CVE-2010-3654) oraz plik wykonywalny, zawierający zaobfuskowany skrypt *Java*. Wspomniany skrypt otwierał połączenie *http* metodą POST na adres przypisany do USA ponadto, malware wykorzystywał bibliotekę, pozwalającą na ukrycie się w systemie. Co warte podkreślenia to fakt, iż w momencie ataku złośliwy kod był rozpoznawany jedynie przez trzy silniki antywirusowe.

Te wszystkie techniki socjotechniczne sprawiają, iż odbiorca często wbrew szkoleniom, akcjom uświadamiającym i wdrażanej przez piony bezpieczeństwa pragmatyce, często otwiera podejrzaną wiadomość i uruchamia załączony plik. Aktualizacje systemów antywirusowych, jak również aplikacji biurowych często trwają kilka, bądź kilkanaście dni, co powoduje, że jedyną ochroną przed tego typu zagrożeniami jest zachowawczość i zdrowy rozsądek użytkownika.

[6] 0-day – atak na system komputerowy, który nastepuje bezpośrednio po ujawnieniu, bądź wykryciu podatności jakiegoś miejsca na atak, a przed opracowaniem i opublikowaniem odpowiedniej poprawki.

3.3. Wykorzystanie socjotechniki przez cyberprzestępców w obliczu katastrofy samolotu rządowego pod Smoleńskiem.

W kwietniu 2010 roku - zespół CERT.GOV.PL uzyskał informację dotyczącą ataku ukierunkowanego na niektóre instytucje administracji publicznej związane z Tragedią Smoleńską. W niecałe dwa dni po tragedii w Smoleńsku, z konta Bill Murray bbc.news@wp.pl rozsyłana była poczta e-mail zatytułowana „Looking beyond Poland's 'unprecedented disaster'"

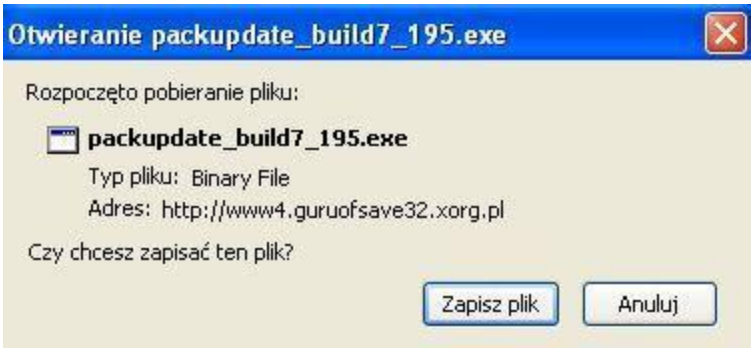
Treść rozsyłanej wiadomości bezpośrednio dotyczyła wydarzeń z dnia 10 kwietnia 2010 roku. Jednocześnie do wiadomości dołączone zostały dwa pliki „Page1.pdf oraz Draft.doc", których otwarcie mogło doprowadzić do zainfekowania sytemu.

Kilka dni później tj. 16 kwietnia 2010 roku, odnotowano kolejny przypadek wykorzystywania tragedii narodowej do celów rozsyłania poczty internetowej zawierającej złośliwe oprogramowanie. Wiadomość *„Dear colleagues! Kazakhstan head of state sends official condolences to Seym of Poland. Official text is attached. Condolences are also posted on official site, http://www.kazakhstan.org.sg/content/intro.php?act=news&c_id=726"* rozsyłana z konta kazakstan.embass@mail.ru o tytule "*Kazakhstan head of state sends official condolences* również zawierała złośliwy załącznik o nazwie „Official_condolences.pdf", którego otwarcie mogło prowadzić do utraty istotnych informacji lub nawet do przejęcia komputera użytkownika.

Dodatkowo cyberprzestępcy wykorzystali fakt, że najczęściej wyszukiwanymi w tym czasie informacjami w sieci były informacje dotyczące katastrofy. Dlatego wyszukując w wyszukiwarkach internetowych informacji na temat śmierci prezydenta wiele stron nie zawierało żadnych informacji o tragedii, lecz infekowało po wejściu na stronę komputer użytkownika szkodliwym oprogramowaniem. W pierwszych dniach po tragedii po wyszukaniu frazy „*Lech Kaczyński nie żyje*" w wyszukiwarce *Google* większość pojawiających się stron serwowało złośliwy kod. Użytkownik, który wszedł na zainfekowaną stronę zostawał przekierowany na witrynę, gdzie pojawiał się komunikat informujący, że komputer stał się obiektem ataku.

Rysunek 16: Przykładowy komunikat pojawiający się po wejściu na zainfekowaną stronę

Pojawiało się ostrzeżenie o wykryciu infekcji w systemie operacyjnym komputera. W celu jej usunięcia program zachęcał użytkownika do pobrania i instalacji pliku z rozszerzeniem .exe.

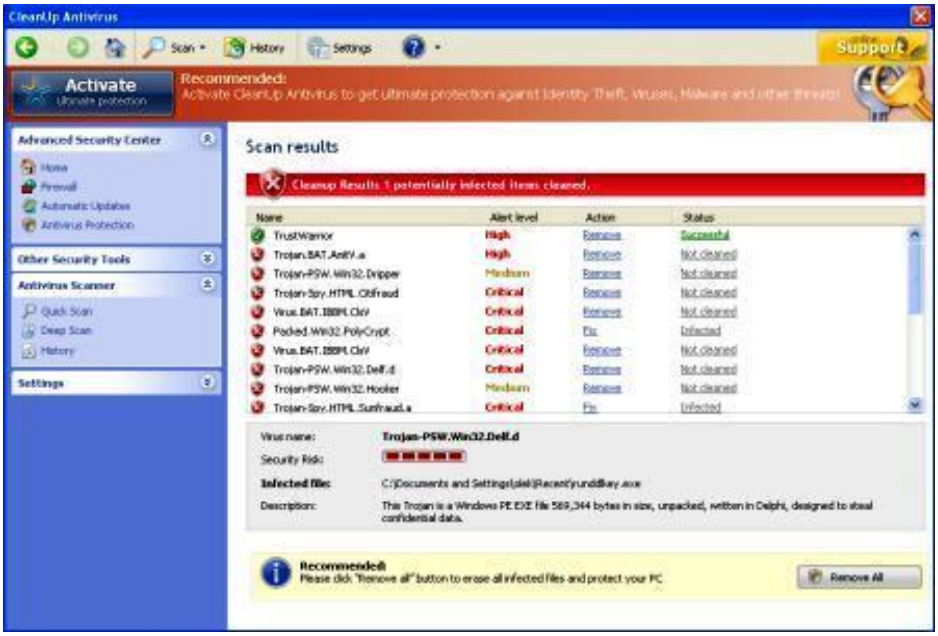


Rysunek 17: Komunikat zachęcający do instalacji rozszerzenia

Po jego pobraniu i uruchomieniu, instalowany był fałszywy program antywirusowy, który udawał automatyczne skanowanie komputera w poszukiwaniu błędów.

Rysunek 18: Instalacja rozszerzenia w toku

Następnie pojawiało się ostrzeżenie o wykryciu infekcji w zagrażających bezpieczeństwu danych i wyświetlany był komunikat podkreślający powagę zagrożenia i znalezieniu wielu infekcji komputera.



Rysunek 19: Przykładowy komunikat pojawiający się podczas rzekomego skanowania komputera

Po wybraniu opcji skasowania wirusów, pojawiał się komunikat zachęcający do wykupienia płatnej wersji programu, co oznacza zazwyczaj podanie numeru konta bankowego, hasła lub po prostu dokonania przelewu pieniędzy na wskazane konto.

Rysunek 20: Przykładowy komunikat zachęcający użytkownika do wykupienia pełnej wersji systemu antywirusowego

Wykradzione w ten sposób dane generalnie są sprzedawane innym przestępcom i mogą służyć do wyłudzeń, tworzenia nowych tożsamości lub bezpośredniej kradzieży pieniędzy z konta osoby pokrzywdzonej.

Złośliwe oprogramowanie zainstalowane w systemie modyfikowało również rejestr wyłączając w nim powiadomienia o nieaktywności firewalla oraz antywirusa. Użytkownik nie mógł uruchamiać programów antywirusowych. Infekcja mogła zainstalować również inne złośliwe dodatki takie jak programy do przechwytywania haseł czy kolejne narzędzia do kradzieży danych.

3.4. Ghostnet

Ghostnet to nazwa nadana wielkoskalowej operacji cyberszpiegowskiej wykrytej w marcu 2009 r. Zarażone komputery zlokalizowano w 103 krajach. Zarażone systemy znajdowały się m.in. w ambasadach czy ministerstwach spraw zagranicznych. Atak przebiegał dwuetapowo. W pierwszym etapie na konto ofiary wysyłana była odpowiednio spreparowana przesyłka e-mail, która powodowała zainstalowanie złośliwego oprogramowania. W etapie drugim oprogramowanie nawiązywało połączenie z serwerem zarządzającym, a następnie ściągało i instalowało konia trojańskiego znanego jako Ghost Rat służącego do szpiegowania wszelkich działań prowadzonych na danym komputerze oraz pozwalającego na przejęcie nad nim całkowitej kontroli (łącznie z możliwością podglądania użytkownika przez kamerkę internetową).

W 2010 roku, podczas prowadzenia analiz poincydentowych zespół CERT.GOV.PL natrafił w kilku przypadkach na ślady wskazujące na to, iż zaatakowane systemy mogły służyć również do działań związanych z działaniem Ghostnetu.

3.5. Stuxnet

Stuxnet jest wirusem ukierunkowanym na przemysłowe systemy produkcyjne SCADA (Supervisory Control And Data Acquisition) firmy Siemens, które nadzorują przebieg procesów technologicznych i produkcyjnych oraz sterują tymi procesami. Jest on pierwszym programem wykorzystującym jednocześnie cztery luki w systemach Windows sklasyfikowane jako „0-day" czyli takie, które nie zostały jeszcze usunięte przez twórców oprogramowania w procesie aktualizacji. To sprawiało, że skuteczność infekcji była bardzo wysoka. Ponadto Stuxnet wykorzystywał w procesie infekcji certyfikaty podpisywane przez firmy – Realtek oraz JMicron.

Jak wynika z przeprowadzonych przez specjalistów analiz, infekcja wirusem przebiega w dwóch fazach:

1. Faza pierwsza rozprzestrzeniania odbywa się poprzez:
   - dyski wymienne (wykorzystanie luki: Microsoft Windows Shortcut 'LNK/PIF' Files Automatic File Execution Vulnerability),
   - sieci LAN przy wykorzystaniu luki w usłudze Windows Print Spooler (Microsoft Windows Print Spooler Service Remote Code Execution Vulnerability),
   - System Message Block (SMB), wykorzystując usługę RPC (Microsoft Windows Server Service RPC Handling Remote Code Execution Vulnerability),
   - wykonanie kopii i uruchomienie swojego kodu na komputerach zdalnych poprzez udziały sieciowe,
   - wykonanie kopii i uruchomienie swojego kodu na komputerach zdalnych pracujących pod kontrolą serwera bazy danych WinCC.

2. Faza druga - znalezienie stacji roboczej, która działa w oparciu o programowalny sterownik logiczny (PLC) firmy Siemens oraz ukrycie swojej obecności oraz wprowadzonych zmian.

Po infekcji systemu komputerowego, oprócz działań związanych z atakowaniem urządzeń SCADA, wirus zbiera informacje o systemie zawierające:

- dane o wersji systemu Windows
- nazwie komputera
- nazwie grupy roboczej w sieci komputerowej
- informacje czy oprogramowanie SCADA jest zainstalowane w systemie
- adresy IP wszystkich interfejsów sieciowych

Następnie program łączy się poprzez port 80 z serwerami C&C (command-and-control), z którymi następuje wymiana informacji oraz pobieranie ewentualnych uaktualnień.

Komunikacja odbywa się z wykorzystaniem szyfrowania XOR (szyfrowanie podstawieniowe) z wykorzystaniem 31 bitowego klucza innego zarówno dla komunikacji inicjującej jak i zwrotnej.

Na podstawie analizy złośliwego oprogramowania stwierdzono, iż używa ono dwóch serwerów C&C:

- www(.)mypremierfutbol(.)com
- www(.)todaysfutbol(.)com

Należy pamiętać, iż możliwe jest istnienie innych tego typu serwerów kontrolujących inne szczepy wirusa Stuxnet.

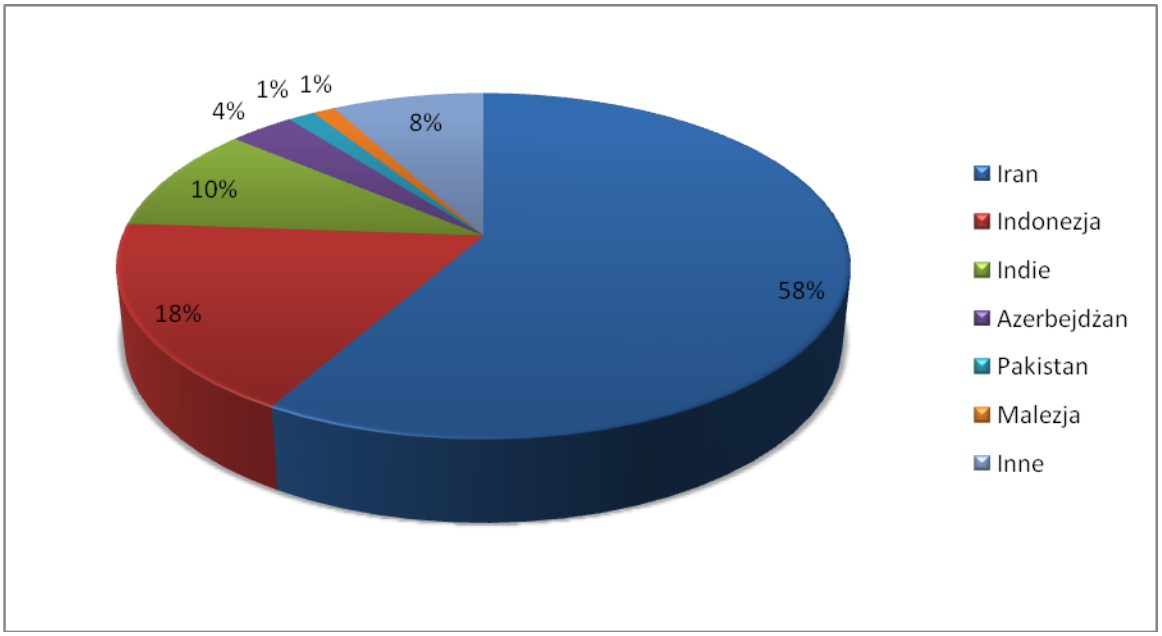
Najistotniejsze pliki tworzone w systemie podczas infekcji:

%Windir%\inf\mdmcpq3.PNF – plik związany z konfiguracją oraz aktualizacja wirusa
~WTR4141.tmp – zawiera funkcje wykorzystywane głównie do uruchomienia właściwego kodu oraz jest wykorzystywany w procesie zarażania nośników wymiennych.
~WTR4132.tmp – przeprowadza właściwy proces infekcji oraz zawiera w sobie zakodowane biblioteki wirusa instalowane w systemie jak również przechwytuje wywołania systemowe atakując biblioteki Kernel32.dll oraz Ntdll.dll.

Podczas infekcji kody wirusa zostają również wstrzyknięte w procesy Lsass.exe (Local Security Authority Subsystem Service – zawiązany z bezpieczeństwem i systemem uwierzytelniania) oraz przeglądarki Internet Explorer,

Pierwszy raz na wirusa natrafili w połowie czerwca 2010r. specjaliści z białoruskiej firmy VirusBlokAda, badając komputery jednego z ich irańskich klientów. Później, w trakcie konferencji Virus Bulletin 2010 w Vancouver, ekspert laboratorium firmy Symantec Liam O'Murchu zaprezentował możliwości wirusa przeprogramowując przy jego wykorzystaniu czas pracy urządzenia podłączonego do kontrolera firmy Siemens. W ten sposób udowodnił, że może on również doprowadzać do fizycznych awarii sprzętu, co w przypadku np. instalacji nuklearnych może mieć katastrofalne skutki.

Dokładna liczba zarażonych komputerów i systemów jest trudna do oszacowania, jednakże z publikowanych danych wynika, że według analiz na dzień 29 września 2010 roku zarażonych było ok. 100 000 komputerów. Najwięcej infekcji odkryto w Iranie – 58,31% zarażonych komputerów, Indonezji – 17,83%, Indiach – 9,96% i Azerbejdżanie - 3,4%.



Rysunek 21: Rozkład procentowy ujawnionych miejsc infekcji wirusem Stuxnet

W Polsce dotychczas nie zgłoszono przypadków zakłócenia pracy systemów produkcyjnych związanych z infekcją wirusem Stuxnet.

3.6. Zbot/ZeuS.

Ataki ukierunkowane to również doskonała metoda na wyłudzenie informacji od użytkowników prywatnych, skupiona na odpowiednim celu. W 2010 roku wzrosło znaczenie wspomnianej techniki propagowania różnego rodzaju trojanów tzw. bankowych – mających za zadanie wykradanie danych koniecznych do logowania i wykonywania przelewów bankowych bez wiedzy użytkownika.

Masowa wysyłka odpowiednio spreparowanych wiadomości mailowych zawierających złośliwe oprogramowanie stanowi według cyberprzestępców znakomitą metodę do dotarcia do użytkowników bankowych. Według szacunków, jednym z najpopularniejszych jest *Zbot/Zeus* – trojan atakujący klientów wielu banków, w tym również działających w Polsce.

W związku z prowadzonym przez Agencję Bezpieczeństwa Wewnętrznego śledztwem, Rządowy Zespół Reagowania na Incydenty Komputerowe CERT.GOV.PL podjął szereg czynności zmierzających do wyeliminowania procederu phishingowego, opartego na kradzieży danych oraz środków finansowych klientów polskiego banku z wykorzystaniem botnetu Zbot\Zeus. W ramach tych czynności wykonano co następuje:

- błyskawicznie ustalono fizyczną lokalizację szeregu adresów IP związanych z grupą przestępczą celem ich wykorzystania w realizacjach procesowych,
- udzielono wsparcia związanego z informacjami na temat przestępczego wykorzystania przez RBN[7] serwera zlokalizowanego na Ukrainie,
- dokonano zabezpieczenia procesowego danych zgromadzonych w złożonych systemach teleinformatycznych (serwery zlokalizowane w firmach hostingowych),
- Laboratorium Elektronicznych Nośników Informacji wykonało analizę na potrzeby przyszłych czynności procesowych oraz w celu wytypowania potencjalnie zagrożonych klientów banku i neutralizacji ryzyka (adres IP),
- ujawniono kontakty internetowe (Skype) osoby stojącej wysoko w hierarchii przestępców,
- analiza informacji ujawnionych z konta Skype doprowadziła do wskazania potencjalnych członków międzynarodowej grupy zarządzającej procederem przestępczym.

3.7. Wykorzystanie metod socjotechnicznych oraz phisingowych do ataku na użytkowników systemów handlu uprawnieniami do emisji CO2.

W styczniu 2010 roku właściciele kont krajowych systemów handlu uprawnieniami do emisji gazów cieplarnianych otrzymali e-maile, w których zostali poinformowani, iż w związku z powtarzającymi się atakami na systemy handlu, Komisja Europejska zadecydowała o podniesieniu poziomu zabezpieczeń. Treść E-maila informowała, iż Komisja Europejska wskazała firmę do realizacji tego zadania, przekazując jej konieczne informacje o użytkownikach. W związku z tym, należy wpisać adres wskazanej strony internetowej i potwierdzić na niej poprawność informacji. Następnie użytkownikom zostanie przekazany klucz USB, dzięki któremu można będzie bezpiecznie logować się do systemu.

E-maile takie zostały przesłane do użytkowników z wielu krajów, w tym Polski. Na uwagę zasługuje kilka szczegółów – tekst wiadomości napisany był w odpowiednim języku, w zależności od narodowości odbiorcy, na wskazaną stronę można było się dostać zarówno klikając link umieszczony w treści, jak również wpisując ręcznie adres samej domeny. Przestępcy stworzyli całą stronę internetową fałszywej firmy i umieścili na niej

[7] The Russian Business Network – rozproszona cyberprzestępcza organizacja działająca, specjalizująca się w wielu aspektach nielegalnej działalności w Internecie, m.in. kradzież i handel danymi wrażliwymi, publikacja nielegalnych treści, kierowanie botnetem i wykorzystywanie do cyber ataków.

odpowiednie wersje językowe, wraz z całym portfolio (fałszywym). Proces „potwierdzania" informacji składał się z kilku podstron, na których znajdowały się różne pytania. Na jednej z nich było pytanie o login do systemu, na innej o hasło. Jako, że nie były one umieszczone obok siebie, lecz obok innych typu: nazwa firmy, ulica, numer budynku, kod pocztowy, miasto, numer kierunkowy itp. zapytanie mogło nie wzbudzić podejrzeń. Dodatkowo, każda przesyłka e-mail była kierowana osobiście do każdej z atakowanych osób. Zawierała jej imię, nazwisko, numer telefonu służbowego jak i nazwę reprezentowanej firmy. W dużym stopniu podwyższało to zaufanie odbiorcy co do prawdziwości treści zawartych w e-mailu. Wielu użytkowników w różnych krajach (w tym w Polsce) podało dane, o które chodziło atakującym. Natychmiast zostały one wykorzystane do wykradzenia tym użytkownikom posiadanych przez nich uprawnień do emisji. Szkody powstałe w Niemczech szacowane są na 3 miliony Euro. Dzięki szybkiej reakcji polskiego Krajowego Administratora Systemu Handlu Uprawnieniami, Polska nie poniosła strat.

Należy zauważyć, iż przestępcy wykorzystali metody zarówno socjotechniczne (e-mail w odpowiednim języku zawierający dane odbiorcy oraz odpowiednia forma fałszywej strony internetowej) jak i phishingowe (skupienie się na wyłudzeniu haseł i natychmiastowe ich wykorzystanie, podszycie się pod legalną stronę, duża skala ataku). Sądząc po stratach tylko jednego kraju należy sądzić, iż osiągnęli sukces. Spowodowane to zostało tym, iż dane użytkowników rejestrów są publicznie dostępne (wymóg prawny), posiadacze kont nie byli świadomi zagrożeń a także niskim stopniem zabezpieczenia samych rejestrów (dostęp i użytkowanie chronione wyłącznie za pomocą hasła).

4. Ataki na witryny internetowe w domenie gov.pl

Rok 2010 cechował się znaczną ilością ataków na witryny WWW. 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 gromadzeniu danych wrażliwych. Pomimo prowadzonych przez zespół CERT.GOV.PL działań pro aktywnych takich jak testy bezpieczeństwa witryn oraz akcje uświadamiające, sektor polskiej administracji publicznej również nie ustrzegł się tego typu ataków.

4.1. Rada ds. Uchodźców

Pierwszym poważniejszym atakiem była podmiana zawartości witryny Rady ds. Uchodźców, która miała miejsce na przełomie lat 2009 i 2010. Ataku dokonała osoba, która prawdopodobnie jest odpowiedzialna za wiele innych włamań na serwery – w tym również administracji publicznej. Włamywacz umieścił na stronie groźbę kolejnych ataków na serwery, których nazwa symboliczna znajduje się w domenie .gov.pl. Analiza incydentu oraz logów dostarczonych przez administratorów pozwoliła na ustalenie podejrzanych. Sprawa została przekazana na policję, aktualnie toczy się postępowanie przygotowawcze.

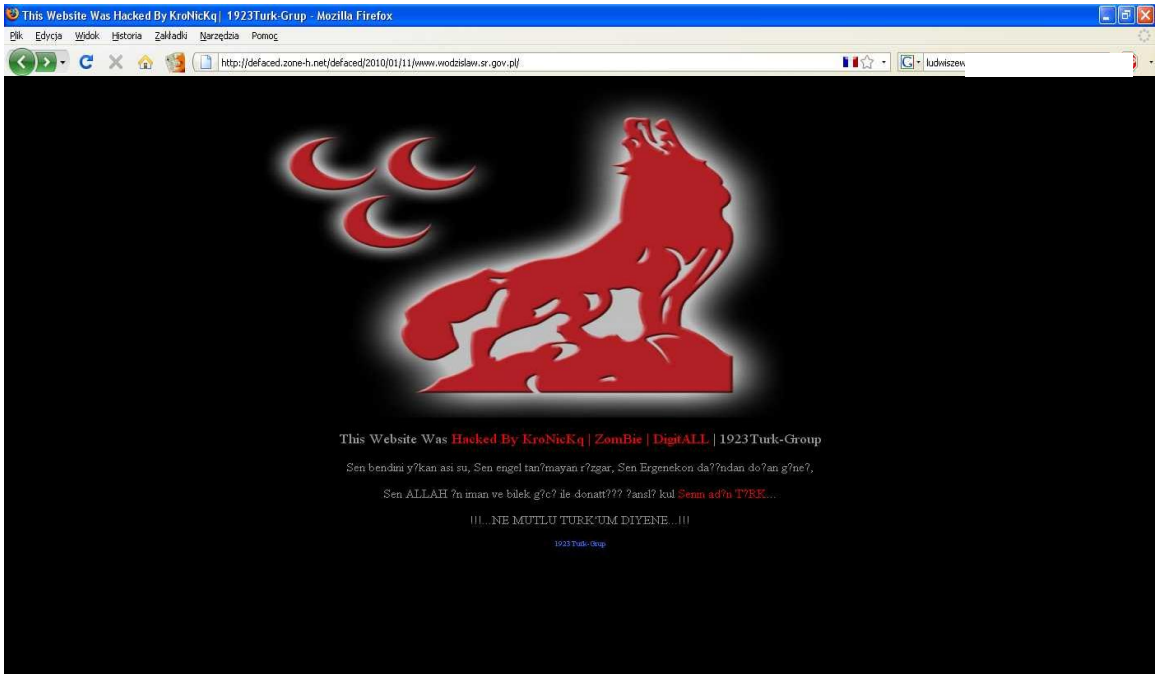
Rysunek 22: Wygląd witryny „rada-ds.-uchodzcow.gov.pl”

Rysunek 23: Wygląd witryny „rada-ds.-uchodzcow.gov.pl" po ataku

4.2. Witryny Sądów Rejonowych

Kolejny udany atak miał miejsce 11 stycznia 2010 roku. Ofiarą padło pięć witryn Sądów Rejonowych. Wszystkie one znajdowały się na jednym serwerze. Sprawcami okazali się najprawdopodobniej członkowie tureckiej grupy. Niestety, brak współpracy ze strony właścicieli portali, w celu dokładnego wyjaśnienia sprawy i ustalenia sposobu przełamania zabezpieczeń serwera, nie pozwolił na ustalenie sprawców.

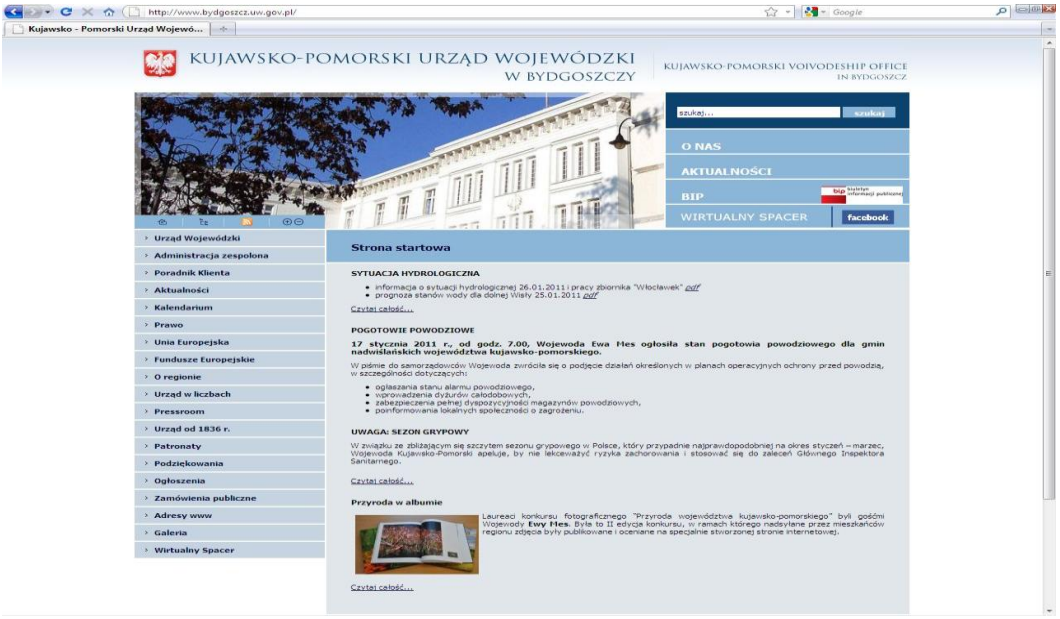
Rysunek 24: Wygląd witryny Sadu Rejonowego w Wodzisławiu Śląskim



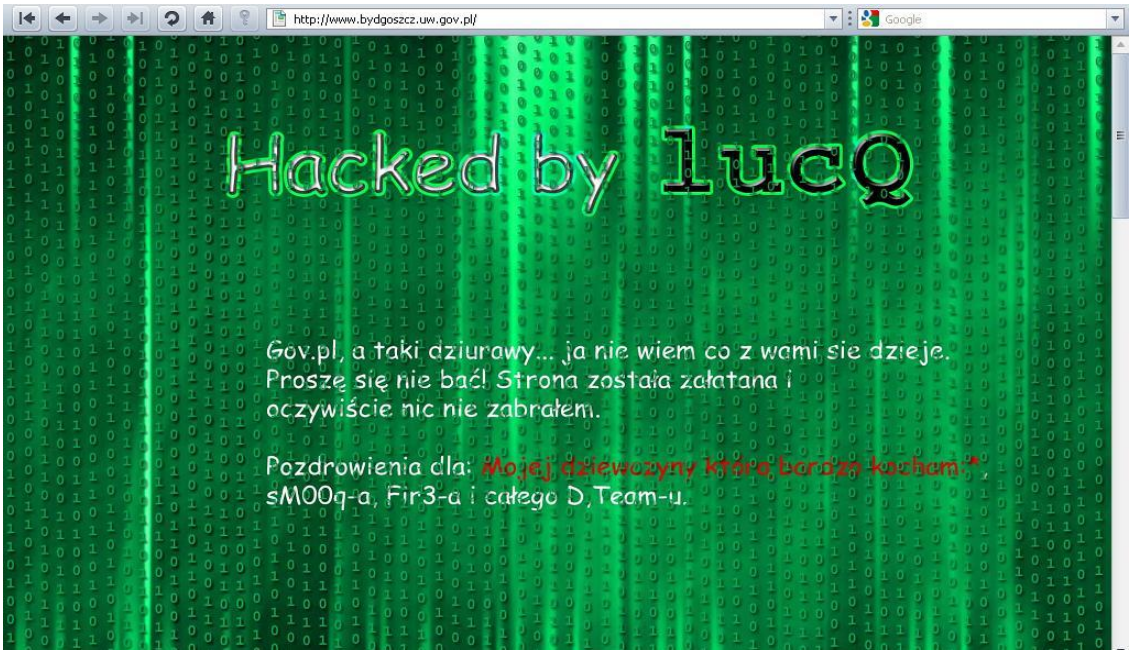
Rysunek 25: Przykład podmienionej zawartości ataku z 11 stycznia 2010 r.

4.3. Urząd Wojewódzki w Bydgoszczy

W marcu 2010 dokonano włamania na witrynę Urzędu Wojewódzkiego w Bydgoszczy. Napastnik umieścił napis świadczący o bardzo słabych zabezpieczeniach serwerów administracji publicznej. Co ciekawe, sprawca przesłał wiadomość elektroniczną do Wojewody z przeprosinami. Zgodnie z posiadaną wiedzą sprawa została przekazana do odpowiedniej jednostki policji, gdzie toczy się postępowanie.



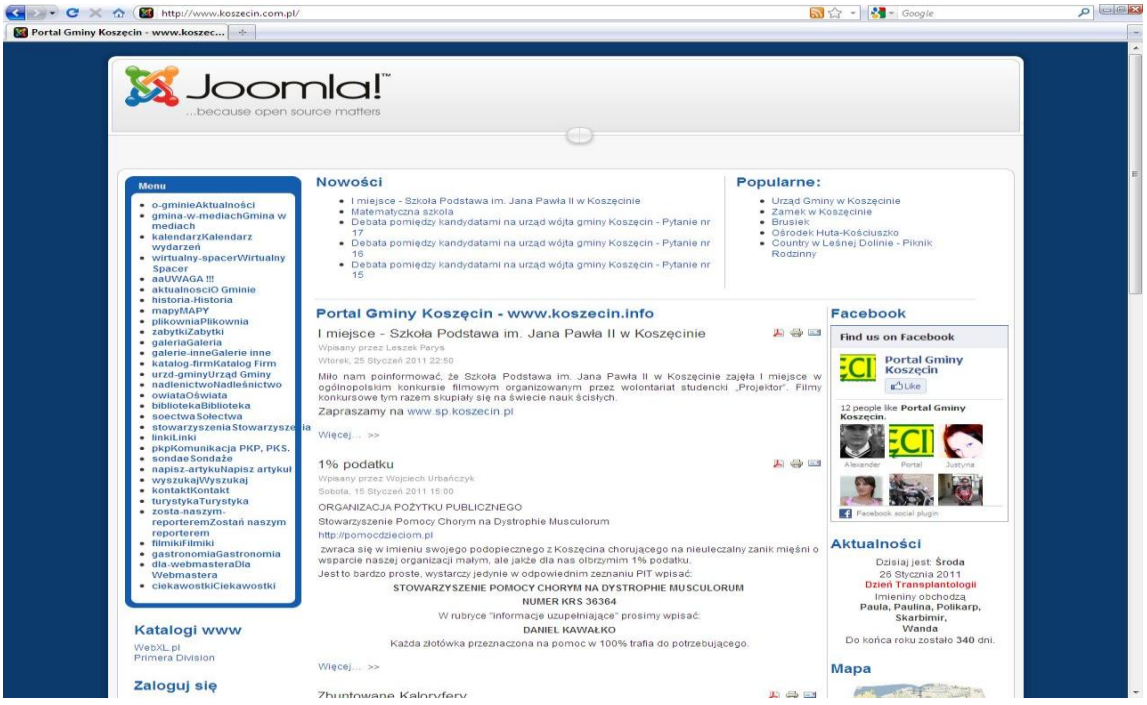
Rysunek 26: Witryna Urzędu Wojewódzkiego w Bydgoszczy.



Rysunek 27: Podmieniona witryna Urzędu Wojewódzkiego w Bydgoszczy.

4.4. Urząd Gminy Koszęcin

Urząd Gminy Koszęcin padł ofiarą ataku w maju 2010 r. – włamanie najprawdopodobniej nastąpiło wskutek wykradzionego hasła do konta FTP serwera. W wyniku tego działania podmieniono stronę główną. Sprawa prowadzona jest przez policję w Lublińcu.

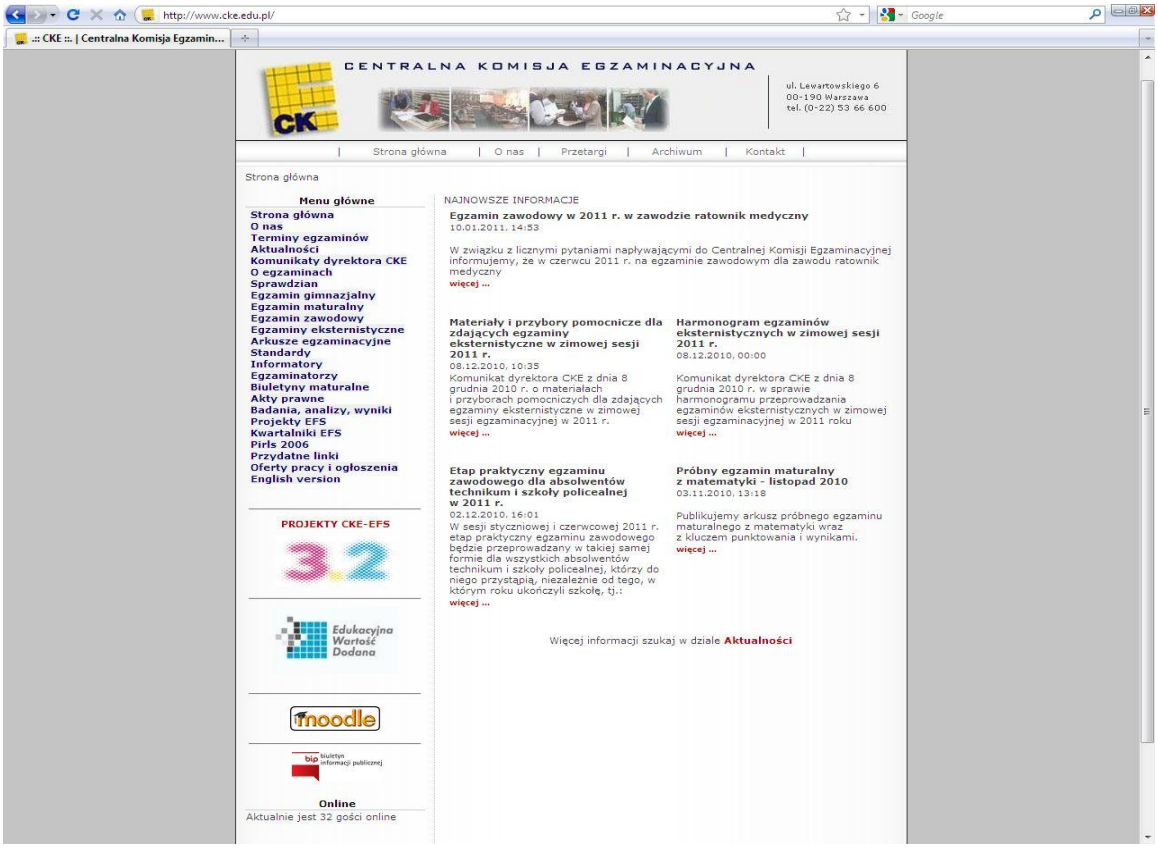


Rysunek 28: Witryna Urzędu Gminy Koszęcin

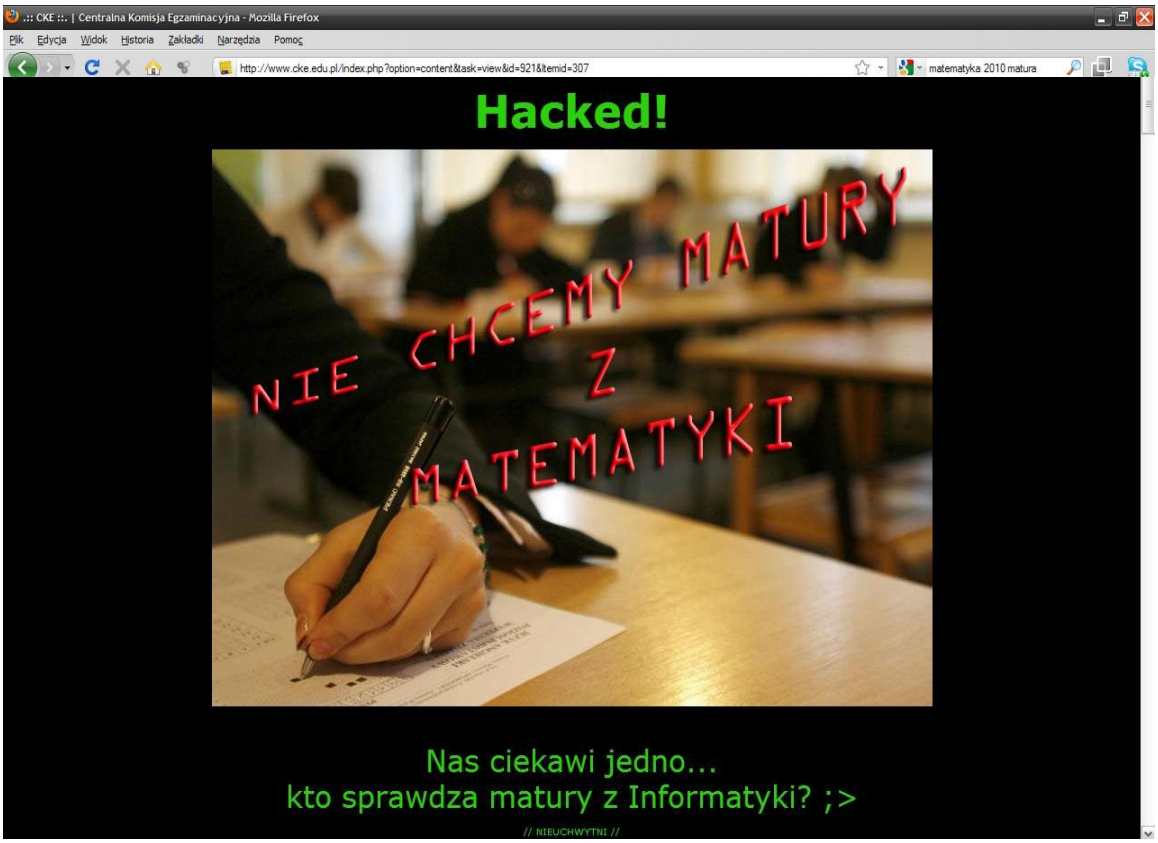
Rysunek 29: Podmieniona witryna Urzędu Gminy Koszęcin

4.5. Centralna Komisja Egzaminacyjna

W maju 2010 miało miejsce włamanie na stronę główną Centralnej Komisji Egzaminacyjnej cke.edu.pl wraz z podmianą zawartości. Podczas wykonywania czynności wyjaśniających stwierdzono obecność na serwerze kilku tzw. backdorów – aplikacji będących złośliwym oprogramowaniem dającym możliwość dostępu do serwera Centralnej Komisji Egzaminacyjne bez wiedzy administratorów. Analiza wykazała, że powyższe oprogramowanie zostało umieszczone na serwerze znacznie wcześniej niż sama podmiana zawartości strony głównej. Brak odpowiedniej współpracy oraz odmowa przez CKE zgłoszenia sprawy organom ścigania, uniemożliwiło ustalenie dokładnego czasu włamania i techniki użytej przez włamywaczy. Należy podkreślić, iż powyższy incydent jest kolejnym, udanym atakiem na w/w witrynę. Wcześniejszy miał miejsce w listopadzie 2009 roku (tuż po próbnych maturach z matematyki). Zgodnie z posiadaną wiedzą, ówczesny incydent również nie został zgłoszony do odpowiednich organów ścigania i w związku z tym uniemożliwił ściganie sprawców.



Rysunek 30: Witryna CKE

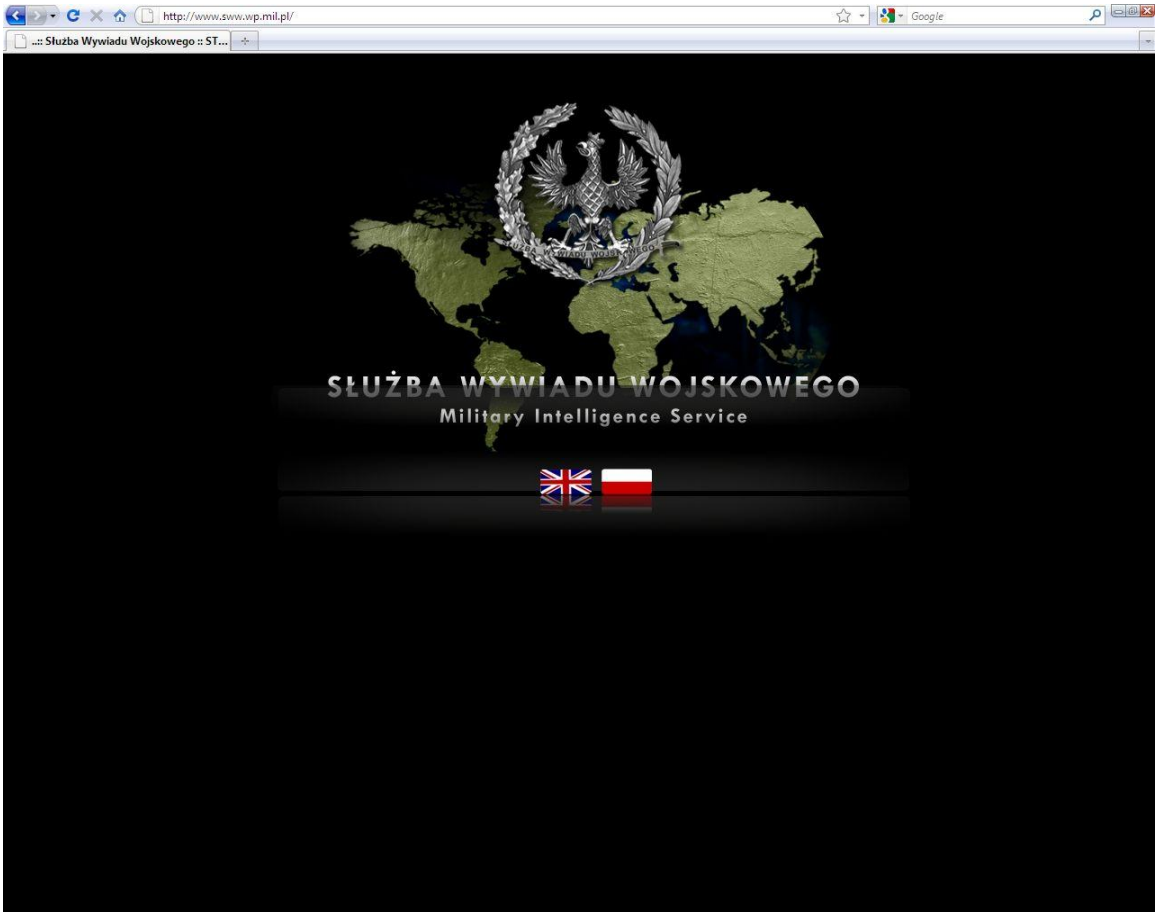


Rysunek 31: Włamanie na CKE z maja 2010 roku

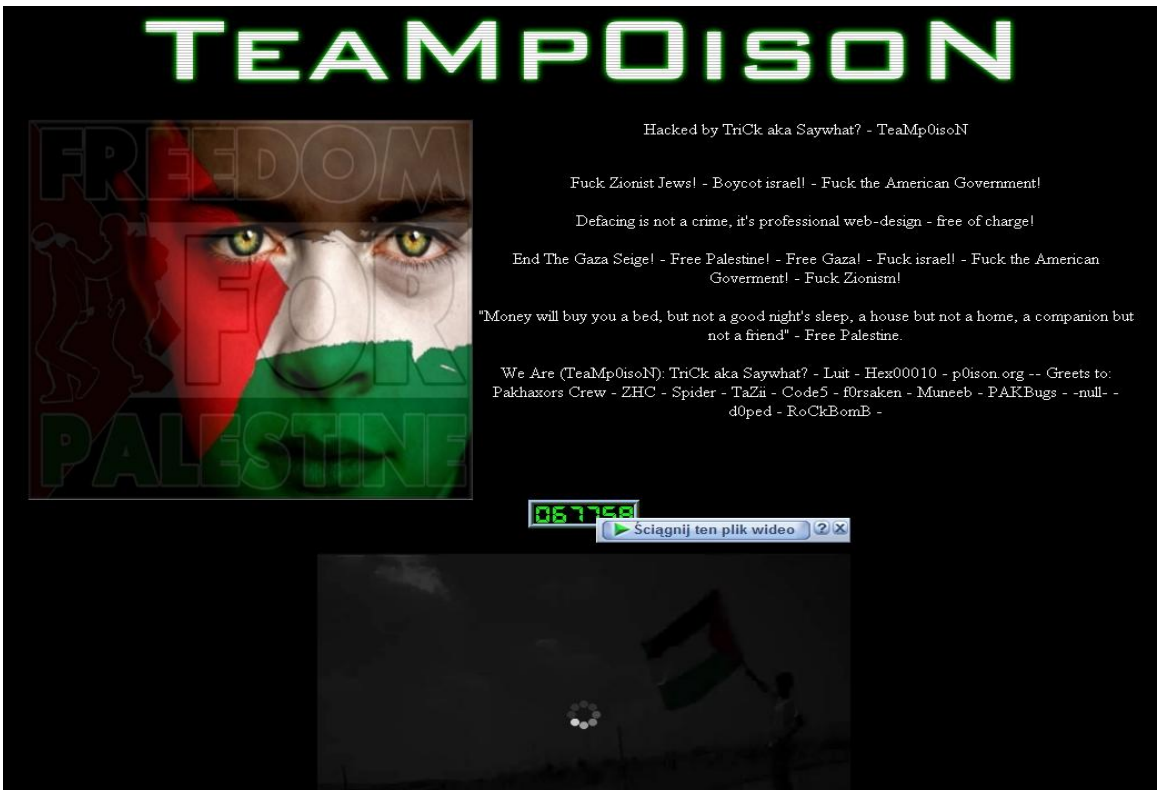
Rysunek 32: Włamanie na CKE z listopada 2009 roku

4.6. Służba Wywiadu Wojskowego

28 czerwca 2010 roku przeprowadzono udany atak na witryny znajdujące się w domenie *.mil.pl*. Atakiem padło sześć witryn (w tym witryna Służby Wywiadu Wojskowego) utrzymywanych na serwerze należącym do Ministerstwa Obrony Narodowej. Ataku dokonała grupa hakerska TeaMp0isoN. Informację o podmianie przekazano wojskowemu zespołowi reagowania na incydenty.



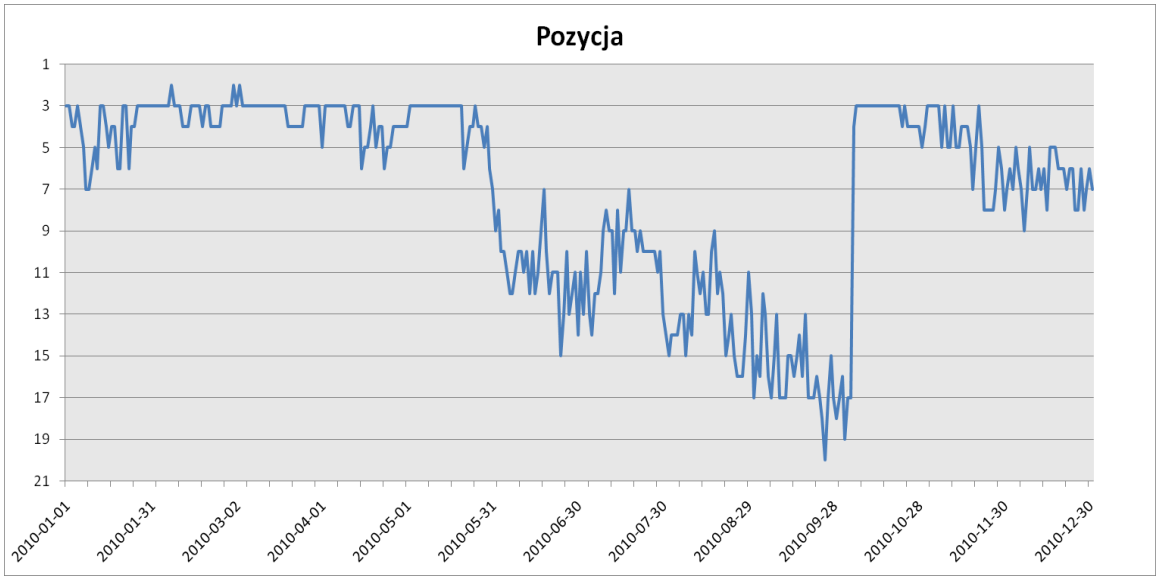
Rysunek 33: Witryna SWW



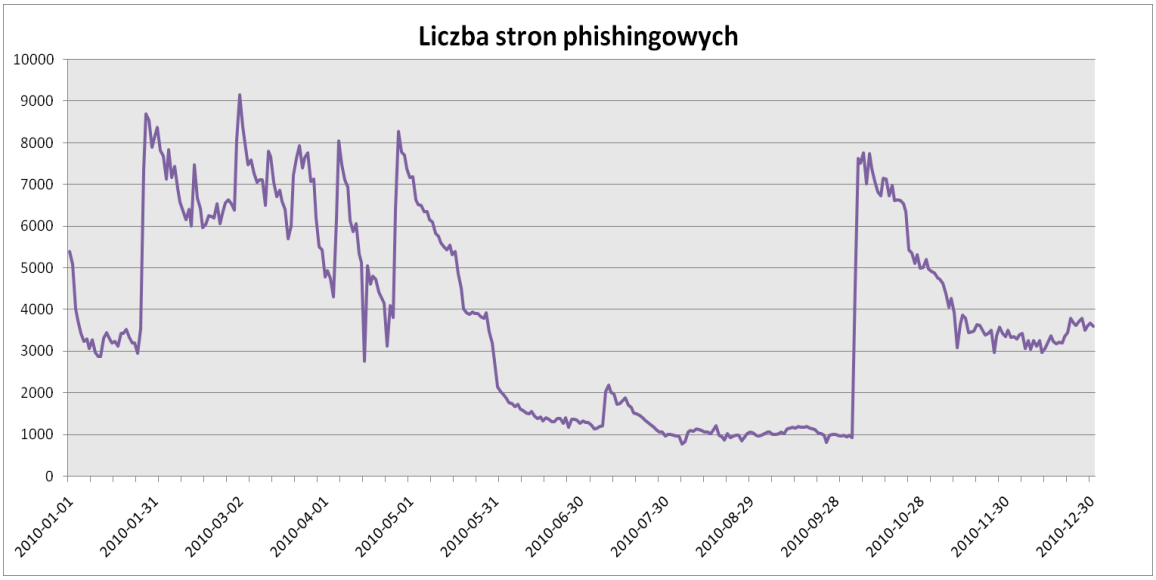
Rysunek 34: Przykładowy wygląd podmienionej witryny w domenie *.mon.pl*

4.7. Publikacja fałszywych stron

Drugim, bardzo popularnym obok *defacement*, celem ataków na witryny WWW jest atak wraz z umieszczeniem na serwerze fałszywej tzw. phishingowej witryny. Często wspomniane strony imitują witryny banków, instytucji finansowych, bądź portali społecznościowych, a ich głównym zadaniem jest wyłudzanie informacji wrażliwych m.in.: danych logowania, adresów email, kodów PIN itp. Z obserwacji prowadzonych przez zespół CERT.GOV.PL wynika, iż intensywność umieszczania witryn phishingowych na polskich serwerach wzrosła znacznie w październiku 2010 roku. Jest to zgodne z trendami ogólnoświatowymi (szacuje się, że na przełomie września i października liczba stron phishingowych wzrosła na świecie o blisko 40%). Jednakże według statystyk „ATLAS Arbor Net" liczba fałszywych stron w Polsce wzrosła aż siedmiokrotnie, co plasuje nas na trzeciej pozycji na świecie.



Rysunek 35: Zmiana pozycji Polski w przeciągu ciągu roku

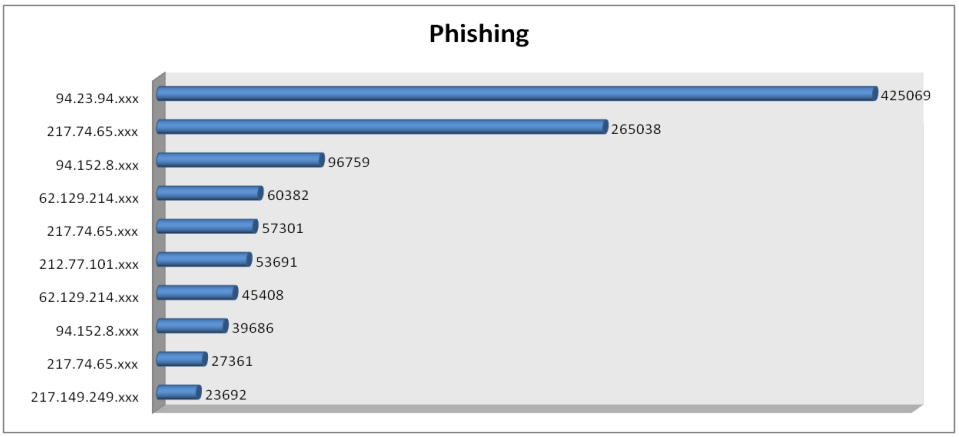


Rysunek 36: Zmiana liczby odnotowanych witryn phishingowych w przeciągu roku

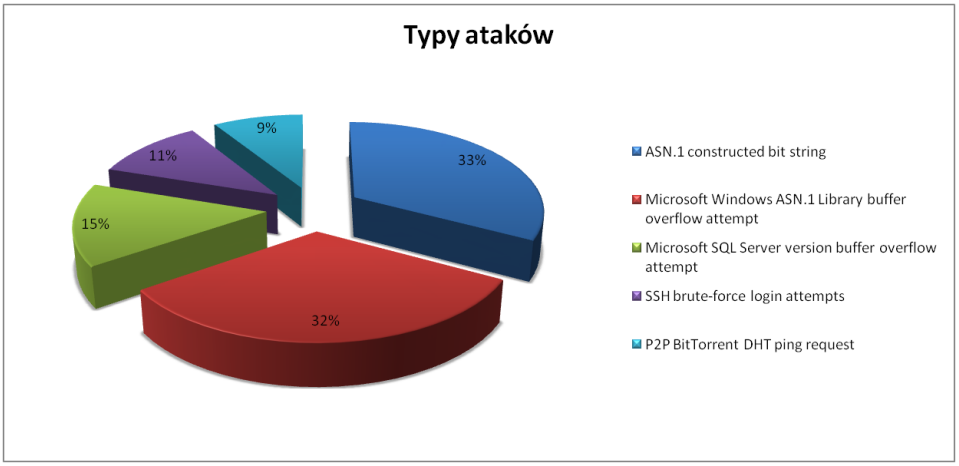
Sytuacja ta związana jest głównie ze stosowaniem najczęściej darmowych, ogólnodostępnych wersji CMS[8] (popularnych, przez co najczęściej atakowanych) oraz brakiem stosowania aktualizacji. Ważne jest tu także fakt wykorzystywania na jednym serwerze kilkudziesięciu czy nawet kilkuset virtualhostów. Przełamanie zabezpieczeń na jednym serwerze (wraz z odpowiednimi uprawnieniami do zapisu) może implikować możliwością zmiany zawartości na wszystkich, co w połączeniu z automatycznymi narzędziami eksploitującymi i generującymi nowe witryny, daje masową podmianę zawartości, bądź masową publikację phishingową.

Statystyki phishingu w 2010 roku przedstawiają się następująco:

[8] **CMS** - (ang. Content Management System, CMS) jest to aplikacja internetowa lub ich zestaw, pozwalająca na łatwe utworzenie serwisu WWW oraz jego późniejszą aktualizację i rozbudowę przez redakcyjny personel nietechniczny. Kształtowanie treści i sposobu ich prezentacji w serwisie zarządzanym przez CMS odbywa się za pomocą prostych w obsłudze interfejsów użytkownika, zazwyczaj w postaci stron WWW zawierających rozbudowane formularze i moduły.

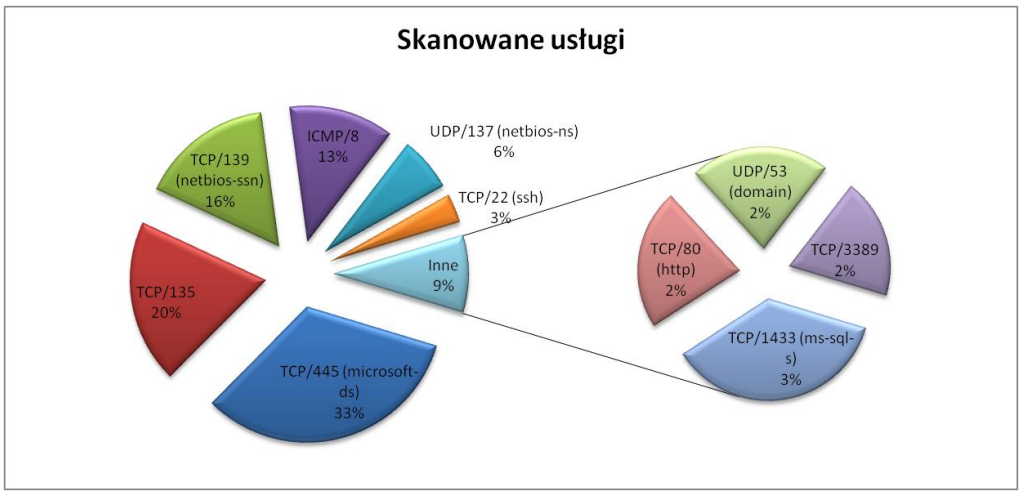


Rysunek 37: Statystyki phishingu wg systemu Atlas (udziały najbardziej aktywnych hostów w 2010 r.)
Trzy najbardziej aktywne hosty w statystykach phishingu znajdują się w adresacji przydzielonej dla firm: OVH Sp. z o.o. z siedzibą we Wrocławiu, INTERIA.PL S.A. z siedzibą w Krakowie, Krakowskie e-Centrum Informatyczne JUMP s.j.

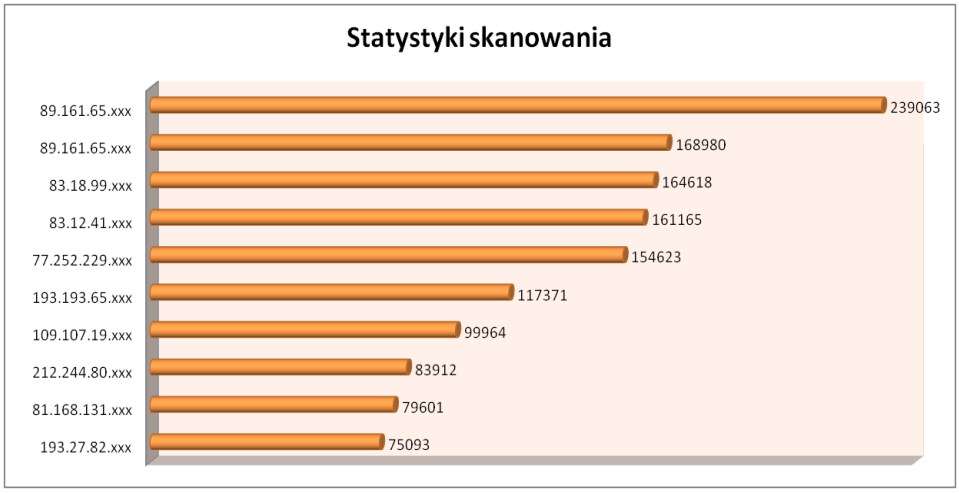


Rysunek 38: Statystyki ataków wg systemu Atlas w 2010 r. Pięć najczęściej występujących typów ataków wg systemu ATLAS – w 2010 r. (udział procentowy tylko dla tych usług)

Rysunek 39: Najbardziej aktywne hosty w Polsce wg systemu ATLAS – w 2010 r.
Trzy najbardziej aktywne hosty w statystykach ataków znajdują się w adresacji przydzielonej dla firm: TP S.A. rejon Zwierzyn, Telefonia Dialog S.A. z siedzibą we Wrocławiu, UPC Telewizja Kablowa Sp. z o.o. z siedzibą w Warszawie.



Rysunek 40: Statystyki skanowania wg systemu Atlas w 2010 r. Najczęściej skanowane porty/usługi wg systemu ATLAS – w 2010 r. (udział procentowy tylko dla tych usług)



Rysunek 41: Najbardziej aktywne hosty w Polsce wg systemu ATLAS – w 2010 r.

Trzy najbardziej aktywne hosty w statystykach skanowania znajdują się w adresacji przydzielonej dla firm: Telekomunikacja Podlasie Sp. z o.o. z siedzibą w Białymstoku (pierwsza oraz druga pozycja) oraz TP S.A. rejon Warszawa.

5. Edukacja i wsparcie

W ramach poprawy bezpieczeństwa cyberprzestrzeni prowadzona jest edukacja użytkowników w zakresie zagrożeń i sposobach ochrony. Obecnie prowadzi ją dla administracji publicznej CERT.GOV.PL.

5.1. Szkolenia z zakresu bezpieczeństwa teleinformatycznego

Funkcjonariusze z Rządowego Zespołu Reagowania na Incydenty Komputerowe CERT.GOV.PL w 2010 roku rozpoczęli 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 uczestnikom szkolenia przybliżony został cel oraz istota powołanego w dniu 1 lutego 2008 roku Rządowego Zespołu Reagowania na Incydenty Komputerowe, ze szczególnym uwzględnieniem problematyki dot. ataków ukierunkowanych na infrastrukturę krytyczną.

Jednocześnie w roku 2010 Rządowy Zespół Reagowania na Incydenty Komputerowe CERT.GOV.PL zorganizował cykl szkoleń dla przedstawicieli jednostek administracji samorządowej. Zakres szkoleń obejmował zarządzanie bezpieczeństwem w sieciach zarówno na poziomie projektowania sieci, systemów jak i samych aplikacji.

5.2. Koordynacja szkoleń dla administratorów sieci

Funkcjonariusze CERT.GOV.PL koordynują szkolenia dla administracji publicznej w ramach Programu Współpracy w Zakresie Bezpieczeństwa (SCP - *Security Cooperation Program).* Szkolenia te, przeprowadzane w autoryzowanych ośrodkach szkoleniowych, oferowane są bezpłatnie dla administratorów sieci oraz osób odpowiedzialnych za nadzór nad bezpieczeństwem systemów teleinformatycznych w instytucjach administracji publicznej. Dzięki tej inicjatywie, począwszy od 2007 roku, przeszkolono ponad 330 osób.

5.3. Publikacja istotnych informacji za pośrednictwem portalu www.cert.gov.pl

W 2008 roku uruchomiono witrynę internetową www.cert.gov.pl, na której publikowane są najważniejsze informacje dotyczące zagrożeń dla bezpieczeństwa teleinformatycznego. Na bieżąco umieszczane są informacje o nowych podatnościach w systemach i aplikacjach, najpopularniejszych formach ataków sieciowych oraz sposobach ochrony przed zagrożeniami. Na witrynie umieszczono również podstawowe informacje na temat zespołu CERT.GOV.PL, dane kontaktowe oraz formularz zgłoszenia incydentu, umożliwiający powiadomienie Zespołu o potencjalnym problemie. Witryna cały czas się rozwija i docelowo ma stać się podstawowym źródłem informacji na temat cyberbezpieczeństwa dla administratorów sieci administracji publicznej. Miesięcznie notowane jest od 3 do ponad 11 tysięcy unikalnych odsłon[9] witryny.

5.4. Ćwiczenia "Cyber Coalition 2010"

W dniach 16-18.11.2010 r. odbyły się ćwiczenia NATO pod nazwą "Cyber Coalition 2010". Po raz pierwszy aktywnie uczestniczył w nich Rządowy Zespół Reagowania na Incydenty Komputerowe CERT.GOV.PL.

Celem ćwiczeń było sprawdzenie zdolności reagowania na cyberincydenty, które uwzględniały podejmowanie strategicznych decyzji oraz efektywną współpracę pomiędzy poszczególnymi instytucjami państw członkowskich Sojuszu.

Scenariusz ćwiczeń opierał się na równoczesnym przeprowadzeniu wielu cyberataków skierowanych przeciwko systemom teleinformatycznym państw członkowskich Sojuszu NATO, biorących udział w ćwiczeniach.

Ćwiczenia "Cyber Coalition 2010" są standardowymi ćwiczeniami ochrony przed atakami sieciowymi i składają się z wielu technicznych etapów. W ćwiczeniach biorą udział instytucje państwowe właściwe w podejmowaniu decyzji w sprawach bezpieczeństwa sieci teleinformatycznych, NATO Cyber Defence Management Board, a także zespoły reagowania na incydenty komputerowe zarówno z NATO, jak i państw członkowskich.

[9] Unikalna odsłona strony to wejście z pojedynczego komputera. Oznacza to, że kolejne wejścia na daną stronę nie są zliczane do statystyki.

Ćwiczenia "Cyber Coalition 2010" odbyły się po raz trzeci. Pierwsza edycja miała miejsce w listopadzie 2008 roku i uczestniczył w niej wyłącznie Sojusz Północnoatlantycki. Począwszy od 2009 roku wszystkie kraje członkowskie są zapraszane do udziału w ćwiczeniach. W tegorocznej edycji Polskę reprezentował jedynie CERT.GOV.PL.
Ćwiczenia koordynowane były przez centralny zespół planujący w siedzibie Naczelnego Dowództwa Połączonych Sił Zbrojnych w Europie (SHAPE) pod Mons w Belgii. Pozostali uczestnicy wykonywali ćwiczenia bezpośrednio ze swoich krajów lub miejsc działania.

Za każdorazowe przygotowanie i przeprowadzenie ćwiczeń odpowiedzialne są wspólnie NATO Headquarters International Military Staff w Brukseli; NATO Computer Incident Response Capability Technical Centre (NCSA NCIRC TC) w Mons (Belgia); NATO Consultations, Command and Control Agency (NC3A) w Brukseli oraz Cooperative Cyber Defence Centre of Excellence (CCD COE) w Tallinie.

Udział w ćwiczeniach pozwolił na identyfikację słabych i mocnych stron zespołu, co w rezultacie zaowocowało podwyższeniem stanu gotowości i wiedzy.

6. Wnioski i rekomendacje dotyczące bezpieczeństwa teleinformatycznego jednostek administracji państwowej

W roku 2010 zanotowano niewielki spadek (z 177 do 155) liczby incydentów zgłoszonych do Rządowego Zespołu Reagowania na Incydenty Komputerowe CERT.GOV.PL w porównaniu z rokiem 2009. Oprócz spadku ilości przedmiotowych incydentów zaobserwowano również znaczne przesunięcie obszaru działań nielegalnych w cyberprzestrzeni (z aktów czysto kryminalnych, na ataki o charakterze szpiegowskim, lub noszące znamiona cyber – wojny). Oznacza to przesunięcie problematyki bezpieczeństwa teleinformatycznego z obszaru ochrony bezpieczeństwa i porządku publicznego (za którego ochronę, zgodnie z art. 29 ust. 1 pkt 1 ustawy z dnia 4 września 1997 r. o działach administracji rządowej (Dz.U. Nr 65, poz. 427, z późn. zm.), odpowiada MSWiA oraz podległe mu służby), do obszaru ochrony bezpieczeństwa państwa.

Stan bezpieczeństwa cyberprzestrzeni Rzeczpospolitej Polskiej należy ocenić jako niewystarczający, głównie z powodu braku rozwiązań systemowych w zakresie przeciwdziałania cyberzagrożeniom oraz niskiej świadomości użytkowników, administratorów i kadry zarządzającej. Główne typy zagrożeń w roku 2010 dla sieci instytucji państwowych obejmowały:

- ataki ukierunkowane na użytkowników sieci administracji publicznej, mające charakter szpiegostwa komputerowego – wykonywane za pomocą niebezpiecznych załączników poczty elektronicznej i nacechowane elementami inżynierii społecznej.
- błędy w aplikacjach WWW, które prowadziły do podmian treści na witrynach instytucji administracji publicznej. W opinii CERT.GOV.PL podmiany treści tych witryn stanowią atak na Państwo, z uwagi na fakt, iż podważają zaufanie obywateli do instytucji państwowych.
- skanowanie przestrzeni adresowej, w celu rozpoznania topologii sieci przed wykonaniem faktycznego ataku.

Rządowy Zespół Reagowania na Incydenty Komputerowe CERT.GOV.PL prognozuje, iż rok 2011 przyniesie wzrost zagrożeń ukierunkowanych na eksfiltrację dokumentów z systemów teleinformatycznych urzędów administracji publicznej. Ataki te będą przybierać formę coraz lepiej przygotowanych działań socjotechnicznych, mających

nakłonić użytkownika do otwarcia załącznika poczty elektronicznej, bądź skorzystania z nośnika wymienialnego USB / CD / DVD. Należy również założyć, iż pod względem technicznym do przeprowadzania ataków używane będą nieznane podatności „*0-day*", dla których nie istnieje stosowna poprawka oprogramowania, a możliwość wykrycia ataku przez systemy antywirusowe jest niewielka.

Dodatkowo, w ramach działań proaktywnych, niezbędne jest przeprowadzenie akcji uświadamiającej, której celem będzie wzrost poziomu świadomości użytkowników na zagrożenia w sieciach oraz systemach teleinformatycznych, wpłynięcie na zmianę ich zachowań oraz zwiększenie percepcji w postrzeganiu tego rodzaju niebezpieczeństw. Ponieważ czynnik ludzki bardzo często jest najsłabszym ogniwem w całej strukturze bezpieczeństwa, tylko stanowcza zmiana ludzkich zachowań oraz przyzwyczajeń może zdecydowanie zredukować występowanie incydentów komputerowych. Wysoki poziom świadomości użytkowników oraz poznanie podstawowych zasad bezpieczeństwa, stanowią pierwszą linię obrony przed nimi.

Powyższa inicjatywa uświadamiająca winna być skierowana do możliwie jak największej grupy odbiorców, począwszy od zwykłych, domowych użytkowników komputerów, a skończywszy na pracownikach dużych organizacji wykorzystujących systemy informatyczne. Należy wykorzystać takie metody uświadamiania jak: szkolenia, plakaty oraz gadżety reklamowe, różnego rodzaju broszury, czy foldery, a nawet proste dodatki do systemów operacyjnych np. tapety, tematy pulpitu, wygaszacze ekranu itp. Ich celem jest dotarcie, w możliwie jak najprostszy sposób, do jak największej grupy odbiorców, co powinno skłonić użytkowników do podjęcia konkretnych działań i nabycia odpowiednich „nawyków" poruszania się w cyberprzestrzeni.

Zgodnie z dokumentem „Rządowy Program Ochrony Cyberprzestrzeni na lata 2009-2011 – założenia" przyjętym przez Komitet Stały Rady Ministrów w dniu 9 marca 2009 roku, odpowiedzialnymi za opracowanie i wdrożenie są: Ministrowie Edukacji Narodowej (w zakresie dostosowania programów nauczania dla szkół) oraz Nauki i Szkolnictwa Wyższego (zalecenia dla uczelni wyższych w sferze cyberbezpieczeństwa).

W celu poprawy bezpieczeństwa teleinformatycznego sieci administracji publicznej oraz implementacji systemowego rozwiązania procesu zarządzania bezpieczeństwem,

stworzono zalecenia i rekomendacje kierowane do kierowników i administratorów sieci jednostek administracji. Zastosowanie się do poniższych wytycznych pozwoli zminimalizować zagrożenia dla cyberprzestrzeni administracji publicznej w Polsce.

6.1. Zalecenia organizacyjne dla kierowników jednostek administracji państwowej

W celu usprawnienia procesu zarządzania bezpieczeństwem cyberprzestrzeni w obszarze administracji państwowej rekomenduje się zastosowanie do następujących wytycznych.

I. Wyznaczenie w każdej samodzielnej jednostce organizacyjnej organów władzy publicznej, przez kierownika danej jednostki, spośród pracowników odpowiedzialnych za utrzymanie systemów teleinformatycznych osoby, której zakres obowiązków uzupełniany jest o następujące punkty:
   - odpowiedzialność za wdrażanie wytycznych dotyczących bezpieczeństwa teleinformatycznego;
   - pełnienie roli punktu kontaktowego w obszarze bezpieczeństwa teleinformatycznego;
   - współpraca z osobami odpowiedzialnymi w danej jednostce w obszarze ochrony systemów niejawnych oraz systemów przetwarzających dane osobowe;
   - analiza incydentów w zarządzanych sieciach i systemach teleinformatycznych;
   - bezzwłoczne informowanie CERT.GOV.PL o incydentach, które mogły stanowić zagrożenie dla innych systemów teleinformatycznych lub obywateli;
   - stworzenie i aktualizacja planów ciągłości działania systemów;
   - przeprowadzenie analizy ryzyka dla podległych systemów;
   - tworzenie kwartalnych raportów o stanie bezpieczeństwa teleinformatycznego w danej jednostce.

II. Na poziomie naczelnego, centralnego lub terenowego organu administracji rządowej, organu wykonawczego na poziomie województwa lub administracji państwowej (jednostki nie należące do administracji rządowej i samorządowej) w/w osoba dodatkowo odpowiedzialna jest za agregację raportów z jednostek

podległych i przesyłanie tak stworzonych raportów obszarowych do CERT.GOV.PL.

W celu zapewnienia minimalnego poziomu bezpieczeństwa CERT.GOV.PL, na podstawie zaobserwowanych incydentów w 2010 roku, proponuje dla kierowników jednostek administracji państwowej wdrożenie poniższych zaleceń:

I. ochrona przetwarzanych informacji w ramach instytucji zgodnie z obowiązującymi przepisami

II. przeprowadzenie inwentaryzacji wszystkich posiadanych systemów teleinformatycznych wraz z ich ogólną charakterystyką zawierająca przede wszystkim rolę systemu, ew. klauzulę niejawności, powiązanie z innymi systemami, określenie, czy system jest izolowany, czy podłączony do sieci rozległych oraz określenie poziomu kontroli nad nim (samodzielna administracja na własnym sprzęcie, outsourcing usług, kolokacja, system jako usługa firmy zewnętrznej itp.)

III. stosowanie systemowego podejścia do zarządzania bezpieczeństwem informacji w kontekście ryzyka stwarzanego dla działalności instytucji wzorując się na wytycznych Polskich Norm z zakresu bezpieczeństwa informacji, a w szczególności grupy norm serii PN/ISO ICE 27000 i norm związanych

IV. przeprowadzenie dla wszystkich systemów procesu analizy ryzyka, zgodnie z wytycznymi Polskich Norm z zakresu bezpieczeństwa informacji, a w szczególności grupy norm serii PN/ISO ICE 27000 i norm związanych

V. stworzenie pełnej dokumentacji bezpieczeństwa systemów, zgodnie z wytycznymi Polskich Norm z zakresu bezpieczeństwa informacji, a w szczególności grupy norm serii PN/ISO ICE 27000 i norm związanych

VI. przeprowadzanie okresowych audytów bezpieczeństwa systemów teleinformatycznych (w pierwszej kolejności tych, które posiadają punkt styku z siecią Internet)

VII. niezwłoczne wdrożenie zaleceń wynikających z analizy ryzyka oraz audytów

VIII. zapewnienie bieżących aktualizacji dokumentacji związanej z bezpieczeństwem teleinformatycznym jednostki

IX. zwracanie uwagi na mechanizmy socjotechniczne („social engineering") w kontekście wykradania poufnych informacji i przeciwdziałanie ich propagowaniu w instytucji (np. poprzez email, strony WWW lub inne sposoby w zależności od usług dostępnych w sieci instytucji)

X. organizowanie szkoleń w zakresie bezpieczeństwa teleinformatycznego dla administratorów systemów

XI. organizowanie szkoleń w zakresie bezpieczeństwa korzystania z systemów i infrastruktury teleinformatycznej jednostki dla użytkowników końcowych

XII. tworzenie kultury pracy przy stanowiskach dla użytkowników końcowych poprzez wprowadzanie dobrych praktyk pracy w oparciu o stosowana politykę bezpieczeństwa teleinformatycznego instytucji

XIII. wyznaczenie osób merytorycznych w jednostce odpowiedzialnych za nadzór i realizację zadań zawartych w powyższych punktach

Stosowanie powyższych zaleceń w instytucji umożliwi minimalizację wystąpienia ataków cybernetycznych na systemy i infrastrukturę teleinformatyczną jednostki, jak również szybkie podejmowanie decyzji w przypadku zaistnienia incydentów.

6.2. Minimalne zalecenia dla administratorów systemów jednostek administracji państwowej

W celu ograniczenia możliwości dokonania kompromitacji systemów teleinformatycznych instytucji zaleca się administratorom jednostek administracji państwowej przestrzeganie następujących zaleceń:

I. Powinno się zakładać oddzielne konta użytkowników dla poszczególnych osób oraz dla różnych rodzajowo zadań realizowanych w systemie, np. konta użytkowników z ograniczeniami dostępu do konfiguracji stanowiska komputerowego oraz braku możliwości instalacji oprogramowania. W celu zapewnienia bezpieczeństwa należy odebrać użytkownikowi możliwość ingerencji w system operacyjny stanowiska komputerowego.

II. W systemach przetwarzania danych, dostęp do informacji winien być zorganizowany na zasadach dostępu minimalnego, tj. domyślnie użytkownik nie

ma żadnych praw dostępu, które otrzymuje jedynie do potrzebnych mu zasobów, a nie odwrotnie.

III. Należy zablokować nieużywane konta użytkowników w systemie, np. konto „gość" w systemie Windows.

IV. Podczas opuszczenia stanowiska należy zabezpieczyć je przed nieautoryzowanym dostępem np. poprzez wylogowanie się lub zastosowanie wygaszacza ekranu z hasłem dostępu. Blokada powinna następować automatycznie.

V. Na stanowisku komputerowym należy pracować z uprawnieniami właściwymi dla rodzaju wykonywanych czynności, np. nie pracować z uprawnieniami administratora w przypadku typowej pracy biurowej.

VI. Instalacja oprogramowania może być przeprowadzana tylko przez administratora systemu.

VII. Na każdym stanowisku należy zainstalować oprogramowanie typu "antywirus" oraz "antyspam" a także stale przeprowadzać jego aktualizację.

VIII. Należy zachować ostrożność podczas instalacji oprogramowania pobranego ze stron internetowych. W szczególności należy sprawdzać wiarygodność źródła oraz skanować pobrane aplikacje programem antywirusowym.

IX. Powinno się zwracać szczególną uwagę na wydawane przez producentów aktualizacje oprogramowania dotyczące bezpieczeństwa aplikacji i pobierać je bezpośrednio ze strony producenta.

X. Wskazany jest stały przegląd zamieszczanych w sieci informacji na temat podatności wykrytych w użytkowanym oprogramowaniu. Należy zapoznawać się z wiadomościami umieszczanymi na stronach poświęconych przedmiotowej tematyce np. **www.cert.gov.pl**.

XI. Trzeba szczególnie ostrożnie obchodzić się z danymi identyfikującymi użytkownika w systemie, tzn. hasłami i nazwami kont użytkowników. Hasła oraz nazwy kont powinny być chronione w sposób gwarantujący brak dostępu do nich nieuprawnionych osób.

XII. Należy zaimplementować politykę bezpieczeństwa poczty internetowej urzędu, a w szczególności sposób postępowania z załącznikami poczty elektronicznej. W razie wątpliwości należy skontaktować się z nadawcą w celu potwierdzenia źródła

pochodzenia, dokonać skanowania załącznika oprogramowaniem antywirusowym, lub skontaktować się z Rządowym Zespołem Reagowania na Incydenty Komputerowe CERT.GOV.PL

XIII. Powinno się uniemożliwić użytkownikom korzystanie z nośników w sposób umożliwiający pozyskanie i wyniesienie danych przetwarzanych na danym stanowisku.

XIV. Wskazane jest regularne wykonywanie kopii danych na zewnętrze, autoryzowane nośniki na wypadek konieczności odtworzenia informacji w związku z możliwością ich utraty w przypadku zaistnienia nieprzewidzianych czynników.

XV. Należy wyłączyć wszystkie usługi w systemie, które nie są wykorzystywane do pracy w sieci czy na stanowisku, np. udostępnianie drukarki.

XVI. Przy wykorzystywaniu dostępu typu WiFi należy korzystać z punktów dostępu oferujących wysoki poziom zabezpieczeń (zalecane WPA2). Korzystać w miarę możliwości z dostępu przewodowego do sieci.

XVII. Przeprowadzać regularnie audyt informatyczny w celu identyfikowania najsłabszych elementów systemu teleinformatycznego.

XVIII. Wszystkie systemy teleinformatyczne muszą posiadać aktualną dokumentację techniczną oraz procedury eksploatacji napisane w sposób zrozumiały i umożliwiający ich wdrożenie i stosowanie.

XIX. Wszyscy użytkownicy powinni być przeszkoleni oraz muszą posiadać wiedzę na temat zagrożeń i metod przeciwdziałania.

6.3. Rekomendacje w celu ograniczenia zjawiska propagowania phishingu

Występowanie wielu incydentów związanych z podmianą stron internetowych, a także wykradanie za ich pomocą wrażliwych informacji, stanowi stale dominujący trend w zakresie cyberprzestępczości. W celu ograniczenia tego typu zjawiska CERT.GOV.PL rekomenduje przestrzeganie następujących zasad:

I. Zabezpieczenia serwera, na którym dostępne są usługi WWW poprzez:

- określenie niezbędnych usług sieciowych uruchomionych na serwerze;

- aktualizacje systemu operacyjnego serwera;
- w miarę potrzeby instalacje i konfiguracje dodatkowych narzędzi zwiększających bezpieczeństwo;
- dokonywanie regularnych backup-ów systemu zgodnie z planem archiwizacji systemu.

II. Zwracanie uwagi na używane wersje oprogramowania typu „system zarządzania treścią" („content management system") i dokonywanie jego stałej aktualizacji, szczególnie pod kątem wykrytych podatności.

III. Stosowanie różnych reguł ograniczania dostępu do treści stron serwera np. poprzez kontrolę dostępu z określonych klas adresowych lub umieszczanie określonych adresów na tzw. „blackliście".

IV. Wykorzystywanie z ograniczonym zaufaniem, a w miarę możliwości niestosowanie gotowych skryptów dostępnych w sieci Internet do generowania zawartości aktywnej strony

V. Separowanie w oddzielnych katalogach plików konfiguracyjnych serwera www, a także pilików skryptowych i wykonywalnych serwera od pozostałych plików z prawami do zapisu w katalogu

VI. Stałe dokonywanie audytu serwera www w zakresie podatności prezentowanych stron internetowych.

VII. Zwracanie uwagi na zapisywanie logów połączeń z serwerem www i ich archiwizację .

6.4 Zalecenia dla implementacji telefonii internetowej VOIP

Ataki na systemy VoIP są w ostatnim czasie rosnącym trendem w grupie zagrożeń pochodzących z Internetu. Jest to spowodowane faktem, iż w stosunkowo łatwy sposób włamanie do takiego systemu można przełożyć na zysk finansowy dla atakującego.

- Podobnie jak przy innych systemach muszą zostać zachowane podstawowe zasady bezpieczeństwa – oprogramowanie (zarówno system operacyjny, jak i serwer

VoIP) musi być na bieżąco aktualizowane i działać pod nadzorem systemu antywirusowego.

- Bezwzględnie konieczne jest odpowiednie skonfigurowanie aplikacji, tj. zmiana domyślnych haseł, wyłączenie niepotrzebnych opcji, pozostawienie tylko upoważnionych kont użytkowników.
- Należy stosować systemy IPS/IDS posiadające możliwość aktywnego nadzoru ruchu. W przypadku VoIP właśnie wykrycie anomalii w transferze danych może pozwolić na wczesne wykrycie włamania i zapobieżenie dalszym stratom.
- Wprowadzając rozwiązania bramek międzywarstwowych (application-level gateways) można przenieść serwer VoIP w głąb warstw zabezpieczeń. Użycie tych specjalizowanych komponentów, poza inspekcją pakietów na poziomie warstwy aplikacji, po połączeniu z systemami firewall, pozwala m.in. na otwieranie połączeń jedynie dla potrzeb chwilowych aplikacji, ustanowienie jej w podsieci używającej NAT, a nawet na aktywne skanowanie treści pakietów, pod względem potencjalnych złośliwych danych mogących doprowadzić do incydentu bezpieczeństwa.
- Konieczne jest również zastosowanie działań na poziomie aplikacyjnym. Niezbędnym jest wprowadzenie silnej identyfikacji i autoryzacji na poziomie SIP. Dodatkowo, należy rozpatrzyć użycie IPSec w celu uzyskania dodatkowej warstwy bezpieczeństwa na poziomie sieciowym, poprzez szyfrowanie i podpisywanie wszystkich pakietów SIP.
- Dobrym zwyczajem, w przypadku większej ilości systemów VoIP, jest ich podział na grupy i zezwolenie na ruch pomiędzy strefami regulowany za pomocą z góry ustalonych, restrykcyjnych polityk.
- W przypadku ruchu VoIP pomiędzy lokalizacjami, w przypadku gdy ruch ten przebiega po sieciach otwartych, bezwzględnie należy zabezpieczyć się przed podsłuchem. Sugerowanym rozwiązaniem jest zestawienie tuneli VPN do tego celu.
- W sieciach lokalnych można rozpatrzyć odpowiednią konfigurację VLAN. Zabezpieczy to przez nieuprawnionym dostępem do danych przez użytkowników wewnętrznych i może ułatwić priorytetyzację ruchu VoIP.

Przy projektowaniu i wdrażaniu systemu VoIP na własny użytek należy odpowiednio zdefiniować odbiorców usług i w oparciu o to przeprowadzić analizę ryzyka. Odpowiednie zaprojektowanie warstwy bezpieczeństwa pozwala optymalnie określić koszty wdrożenia. Dokładanie zabezpieczeń do istniejącego systemu jest zazwyczaj o wiele droższe.

6.5. Rekomendacje prawno-organizacyjne

Należy dążyć do zdefiniowania jednolitego znaczeniowo słownika w zakresie systemów teleinformatycznych, który jest nieustalony dotychczasowym prawodawstwem. W opinii CERT.GOV.PL należy przyjąć:

- cyberprzestrzeń jako cyfrową przestrzeń przetwarzania i wymiany informacji tworzoną przez systemy i sieci teleinformatyczne wraz z powiązaniami pomiędzy nimi oraz relacjami z użytkownikami;
- cyberprzestrzeń RP jako cyberprzestrzeń w obrębie terytorium państwa Polskiego i w lokalizacjach poza terytorium, gdzie funkcjonują przedstawiciele RP (placówki dyplomatyczne, kontyngenty wojskowe);
- cyberprzestępstwo jako czyn zabroniony, popełniony w obszarze cyberprzestrzeni;
- cyberterroryzm jako cyberprzestępstwo o charakterze terrorystycznym;
- cyberatak jako celowe zakłócenie prawidłowego funkcjonowania cyberprzestrzeni;
- incydent związany z bezpieczeństwem informacji (incydent teleinformatyczny) jako pojedyncze zdarzenie lub seria niepożądanych zdarzeń związanych z bezpieczeństwem, które stwarzają znaczne prawdopodobieństwo zakłócenia działań biznesowych i zagrażają bezpieczeństwu informacji (wg normy PN-ISO/IEC 27001);
- ochronę cyberprzestrzeni jako zespół przedsięwzięć organizacyjno-prawnych, technicznych, fizycznych i edukacyjnych mający na celu niezakłócone funkcjonowanie i bezpieczeństwo cyberprzestrzeni.

Powyższe rekomendacje wynikają z zapisów przyjętego przez Komitet Stały Rady Ministrów dokumentu „Rządowy Program Ochrony Cyberprzestrzeni RP na lata 2009-2011 – założenia". W świetle obowiązującego prawa rekomendacje zawarte w rozdziale 6 nie stanowią norm, lecz są zbiorem dobrych praktyk. Ich wdrożenie stanowi jedynie podstawę do budowy całego systemu bezpieczeństwa.