CERT.GOV.PL

Raport o stanie bezpieczeństwa cyberprzestrzeni RP w 2013 roku

CERT.GOV.PL / Warszawa 2014

CERT.GOV.PL

Rządowy Zespół Reagowania na Incydenty Komputerowe CERT.GOV.PL, pełni rolę głównego zespołu CERT odpowiadającego za koordynację procesu obsługi incydentów komputerowych w obszarze administracji rządowej Rzeczypospolitej Polskiej.

Zespół funkcjonuje od 1 lutego 2008 roku w Agencji Bezpieczeństwa Wewnętrznego. Zgodnie z *Polityką Ochrony Cyberprzestrzeni Rzeczypospolitej Polskiej*, podstawowym zadaniem Zespołu jest zapewnianie i rozwijanie zdolności jednostek organizacyjnych administracji publicznej RP 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 59 373

Fax.:
+48 22 58 58 833

Departament Bezpieczeństwa Teleinformatycznego
Agencji Bezpieczeństwa Wewnętrznego

ul. Rakowiecka 2A
00-993 Warszawa
Polska

Spis treści

1. Wstęp

Przyjęcie w 2013 roku *Polityki Ochrony Cyberprzestrzeni Rzeczypospolitej Polskiej* ustanowiło funkcjonowanie Rządowego Zespołu Reagowania na Incydenty Komputerowe CERT.GOV.PL (zwanego dalej Zespołem CERT.GOV.PL) w strukturze cyberbezpieczeństwa państwa jako część Krajowego Systemu Reagowania na Incydenty Komputerowe w Cyberprzestrzeni Rzeczypospolitej Polskiej. Celem Polityki jest podwyższenie poziomu bezpieczeństwa cyberprzestrzeni Polski oraz zwiększenie odporności państwa na ataki terrorystyczne prowadzone w cyberprzestrzeni.

Raport o stanie bezpieczeństwa cyberprzestrzeni RP w 2013 roku publikowany jest w celu podnoszenia poziomu świadomości użytkowników na temat zagrożeń ich skutków oraz informowaniu o istotnych zjawiskach w obszarze ochrony cyberprzestrzeni RP. Ponadto, cykliczne przedstawianie w raporcie danych statystycznych może pomóc zainteresowanym w śledzeniu trendów zagrożeń, co bywa użyteczne w przygotowaniach do przyszłych działań zabezpieczających.

Mając na uwadze uplasowanie Zespołu CERT.GOV.PL w strukturze Departamentu Bezpieczeństwa Teleinformatycznego Agencji Bezpieczeństwa Wewnętrznego, realizuje on zadania wynikające z *art. 5 ustawy z dnia 24 maja 2002 r. o Agencji Bezpieczeństwa Wewnętrznego oraz Agencji Wywiadu (Dz.U. 2010 nr 29 poz. 154),* tj. rozpoznawanie, zapobieganie oraz zwalczanie zagrożeń, które kierowane są przeciwko bezpieczeństwu wewnętrznemu państwa lub jego porządkowi konstytucyjnemu – a więc wartościami będącymi w istocie filarami bezpieczeństwa państwa polskiego, jako całości. Zadania te stanowią jednocześnie ramy prawne dla funkcjonowania Zespołu CERT.GOV.PL, jako komórki specjalistycznej do działania w obszarze cyberprzestrzeni RP.

2. Statystyki incydentów koordynowanych przez Zespół CERT.GOV.PL w 2013 roku

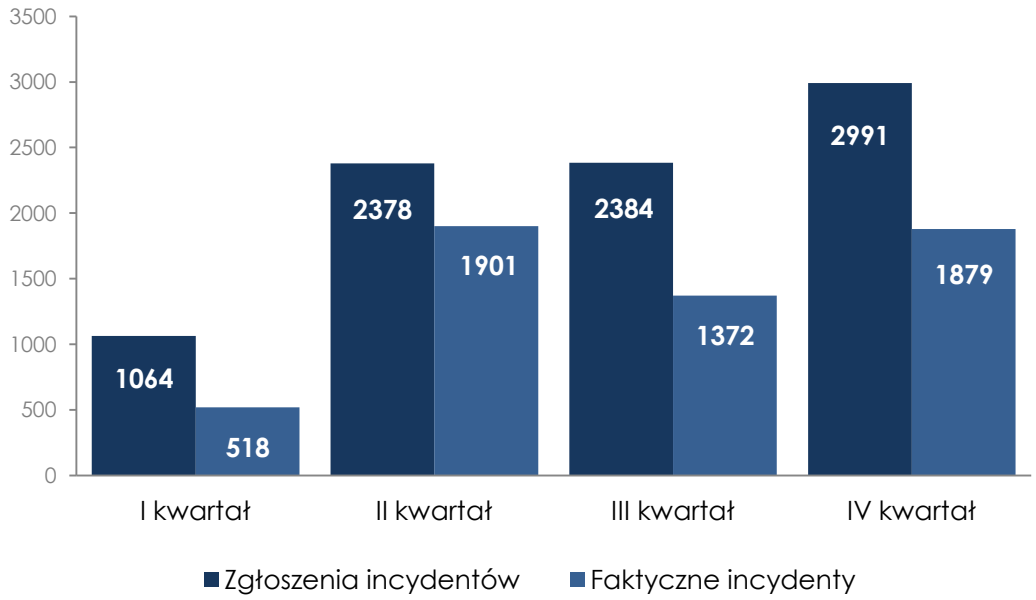
2.1.Zagrożenia

Rok 2013 pod względem liczby otrzymanych zgłoszeń oraz obsłużonych incydentów okazał się dla Zespołu CERT.GOV.PL rekordowy w stosunku do lat poprzednich. Zdecydowany wzrost liczby zgłoszeń nastąpił w drugim kwartale 2013 roku i spowodowany był przede wszystkim wykorzystaniem nowych źródeł danych dostarczających istotnych informacji o wykrytych zdarzeniach związanych z bezpieczeństwem teleinformatycznym w sektorze administracji rządowej. Nie oznacza to realnego wzrostu występujących zagrożeń, ale świadczy o istotnym postępie w procesie ich identyfikowania. Spowodowane to jest przede wszystkim obsługą dużej ilości zgłoszeń, przekazywanych za pośrednictwem platformy *N6*. Platforma *N6* została zbudowana przez Zespół CERT Polska[1] i służy gromadzeniu, przetwarzaniu oraz przekazywaniu informacji o zdarzeniach naruszających bezpieczeństwo teleinformatyczne. Informacje o incydentach, które wystąpią w sieciach bądź systemach teleinformatycznych administracji publicznej, są niezwłocznie przekazywane do Zespołu CERT.GOV.PL. Po przeprowadzeniu stosownej analizy, uzyskane wyniki przesyłane są do zagrożonej incydentem jednostki administracji publicznej, celem podjęcia koniecznych działań w ramach procesu reagowania na incydenty.

W sumie, w 2013 roku zarejestrowanych zostało aż 8817 zgłoszeń, z których 5670 zakwalifikowano, jako incydenty.

[1] Zespół CERT Polska działa w strukturach Naukowej i Akademickiej Sieci Komputerowej. Działalność zespołu finansowana jest przez NASK.

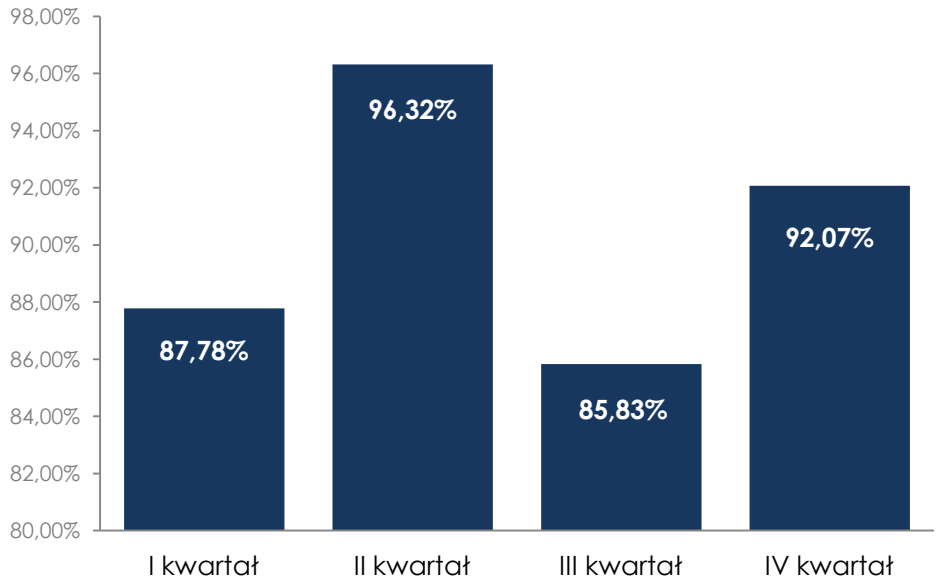
Poniższy rysunek obrazuje ilość zarejestrowanych zgłoszeń oraz obsłużonych przez Zespół CERT.GOV.PL incydentów teleinformatycznych w poszczególnych kwartałach 2013 roku.



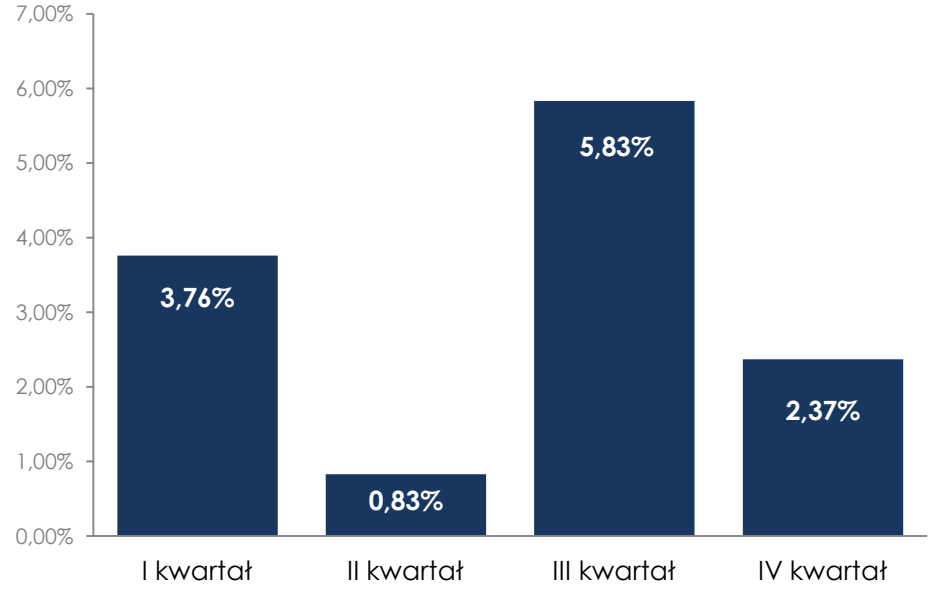
Rysunek 2-1: Liczba zarejestrowanych zgłoszeń oraz incydentów w poszczególnych kwartałach 2013 roku

Różnica w liczbie zarejestrowanych zgłoszeń oraz liczbie incydentów wynika z faktu, że część z nich stanowią tzw. „false-positives". Są to przypadki błędnej interpretacji przez zgłaszającego legalnego ruchu sieciowego. Drugą z przyczyn, szczególnie widoczną w przypadku zgłoszeń z systemów automatycznych, są wielokrotne zgłoszenia dotyczące tych samych incydentów. Ponadto, należy tu również zwrócić uwagę na fakt, iż zgłoszenia pochodzące z systemów autonomicznie raportujących zostają poddane późniejszej weryfikacji przez Zespół CERT.GOV.PL, który wskazuje, czy zgłoszeniom można nadać atrybut incydentu.

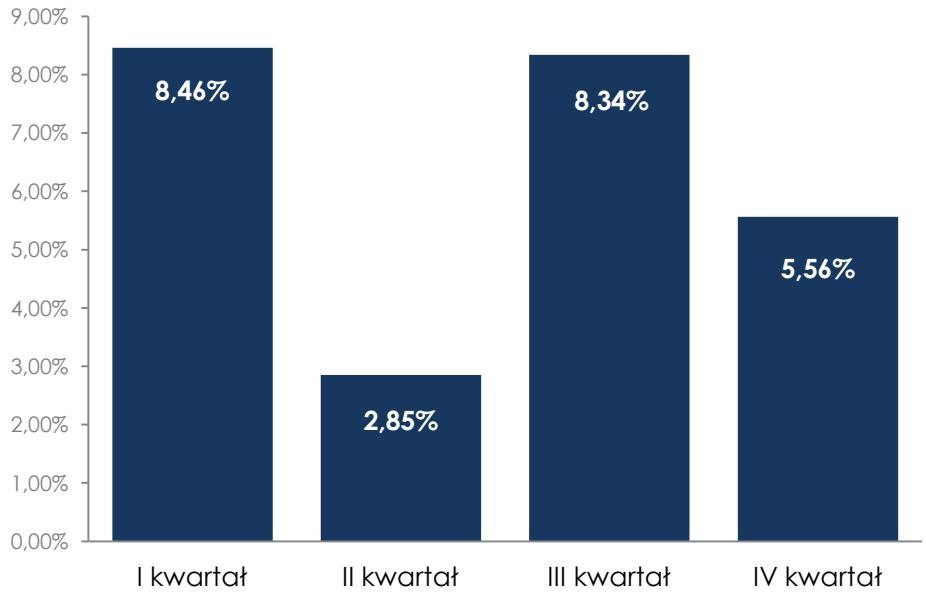
Poniższe wykresy przedstawiają szczegółowe statystyki źródeł zgłoszeń incydentów trafiających do Zespołu CERT.GOV.PL.



Rysunek 2-2: Źródła incydentów – zgłoszenia z wykorzystywanych przez CERT.GOV.PL systemów

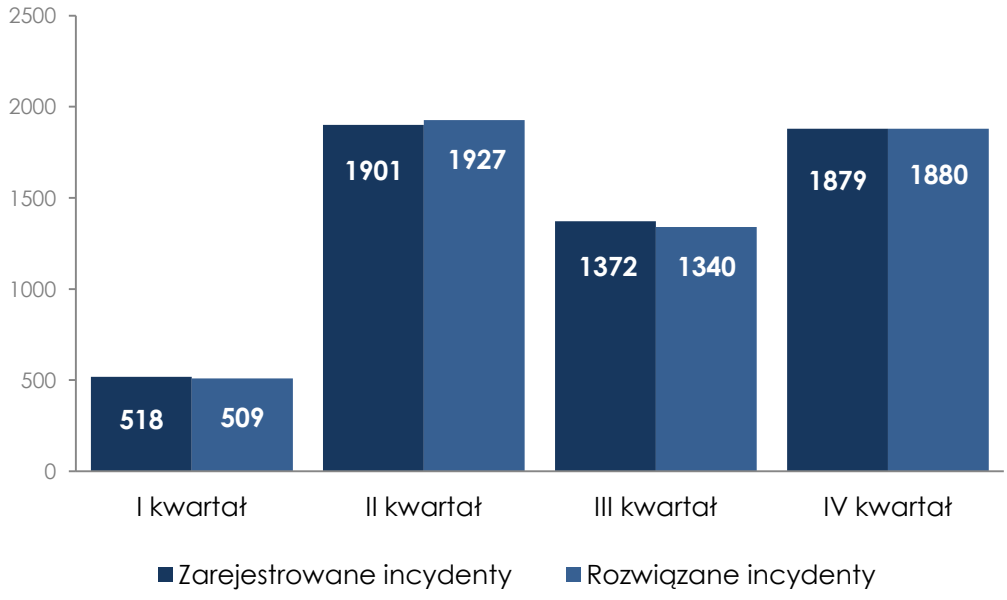


Rysunek 2-3: Źródła incydentów – ustalenia własne



Rysunek 2-4: Źródła incydentów – zgłoszenia podmiotów zewnętrznych

Porównanie liczby incydentów otwartych i zamkniętych przez Zespół CERT.GOV.PL w 2013 roku ilustruje poniższy rysunek.



Rysunek 2-5: Porównanie liczby incydentów otwartych i zamkniętych w poszczególnych kwartałach 2013 roku

Podział zarejestrowanych incydentów w 2013 roku na poszczególne kategorie przedstawia się następująco:

Rysunek 2-6: Statystyka incydentów w roku 2013 z podziałem na kategorie

W 2013 roku największą grupę, jak co roku, stanowiły incydenty w kategorii „botnety". Zespół CERT.GOV.PL zarejestrował aż 4270 incydentów dotyczących oprogramowania złośliwego działającego na stacjach roboczych, podłączonych do sieci teleinformatycznej jednostek administracji publicznej. Najczęściej występującymi typami botnetów w 2013 roku wykrytymi w infrastrukturze administracji państwowej, były botnety Citadel, Conficker oraz Downadup.

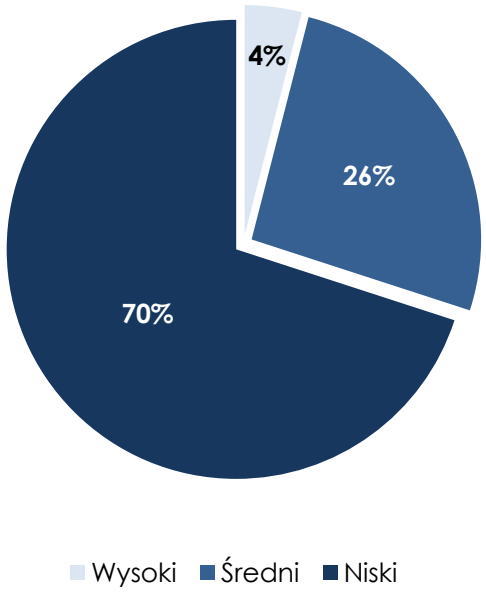
W kategorii „inne" uwzględniono informacje o podatnościach oraz błędach konfiguracji aplikacji, bądź urządzeń sieciowych. Znaczący wpływ na statystykę miały w tej kategorii pozyskane przez Zespół CERT.GOV.PL informacje o podatności serwerów DNS (DNSOpenResolver), dotyczące wielu podmiotów administracji publicznej oraz agend rządowych – w sumie 866 incydentów.

Ponadto, Zespół CERT.GOV.PL otrzymywał znaczną ilość zgłoszeń związanych ze skanowaniem sieci w poszukiwaniu błędów i podatności – 146 incydentów oraz dotyczących nieuprawnionej zmiany informacji, m.in. podmiany zawartości witryn internetowych tzw. *website defacement* – 124 incydenty. Warte odnotowania jest także występowanie innych kategorii incydentów, takich jak „spam", „błędy aplikacji web", „błędne konfiguracje urządzeń", „konie trojańskie" oraz pozostałe wymienione na *Rysunku 2-6*.

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

System ARAKIS-GOV[2] w 2013 roku zarejestrował 18317 alarmów, co stanowi nieznacznie mniejszą liczbę w stosunku do poprzedniego roku, gdzie odnotowano ich 20327. Mając na uwadze poziom istotności i zagrożenia, alarmy podzielono na trzy główne kategorie. Najmniej odnotowano alarmów najgroźniejszych o priorytecie „wysokim" - 644, co stanowiło 4% wszystkich zarejestrowanych. Najwięcej natomiast odnotowano alarmów o priorytecie „niskim" - 12900, które stanowiły 70% ogółu. Pozostałe alarmy to priorytet „średni", których odnotowano 4773.

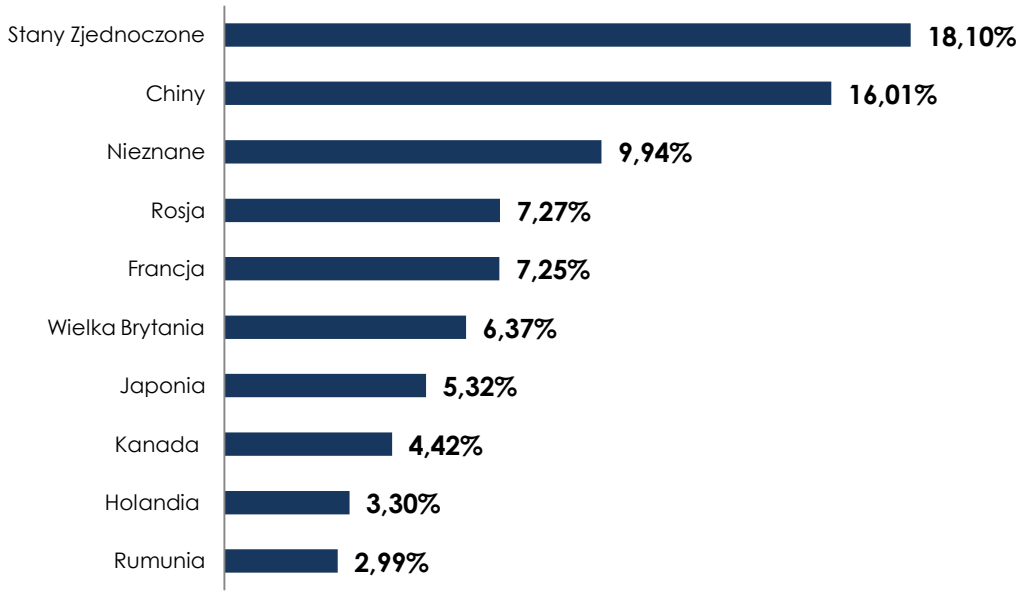
[2] System ARAKIS-GOV jest systemem wczesnego ostrzegania przed zagrożeniami w sieci Internet. Jego architektura oparta jest na rozproszonym zestawie sensorów instalowanych w chronionych instytucjach na styku sieci produkcyjnej z siecią Internet. Centralną część systemu stanowią serwery dokonujące m.in.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



Rysunek 2-7: Rozkład procentowy alarmów ze względu na priorytety

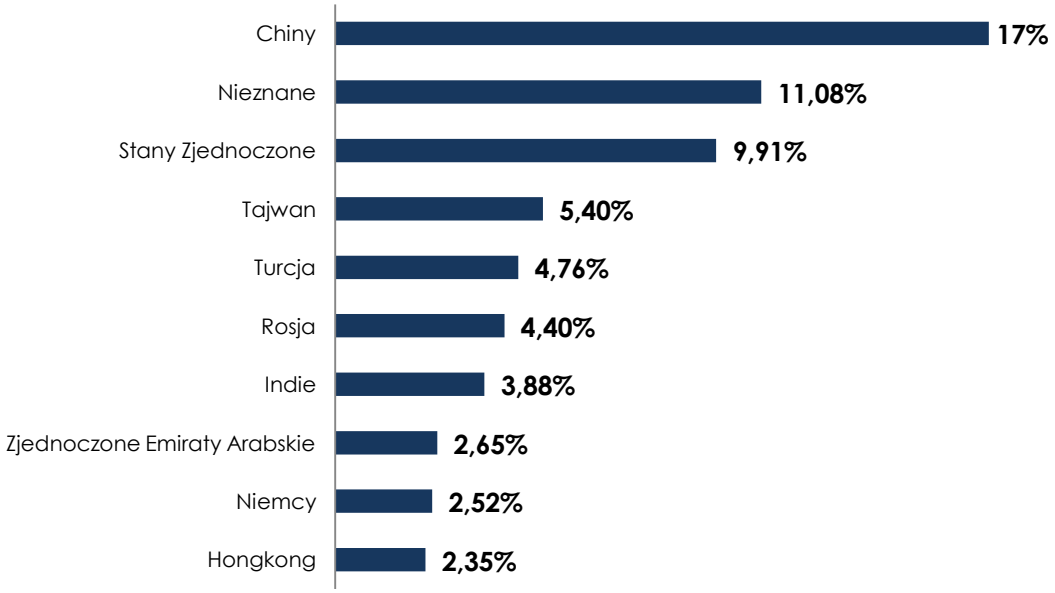
W odniesieniu do statystyk rozkładu procentowego alarmów pod kątem poziomu istotności za rok 2012, statystyki w roku 2013 przedstawiają bardzo podobną charakterystykę zidentyfikowanych zagrożeń.

Informacje gromadzone i analizowane przez system ARAKIS-GOV pozwalają na określenie lokalizacji geograficznej źródeł, z których wykonywano ataki na polskie sieci administracji publicznej. Do najbardziej aktywnych pod kątem ilości generowanych połączeń należą adresy IP przypisane do Stanów Zjednoczonych – około 18% i Chin – przeszło 16%.



Rysunek 2-8: Rozkład procentowy źródeł ataków na sieci monitorowane przez system ARAKIS-GOV pod kątem ilości generowanych połączeń

Nieznacznie różnią się statystki lokalizacji geograficznej źródłowych adresów IP pod kątem ich unikalnego występowania.



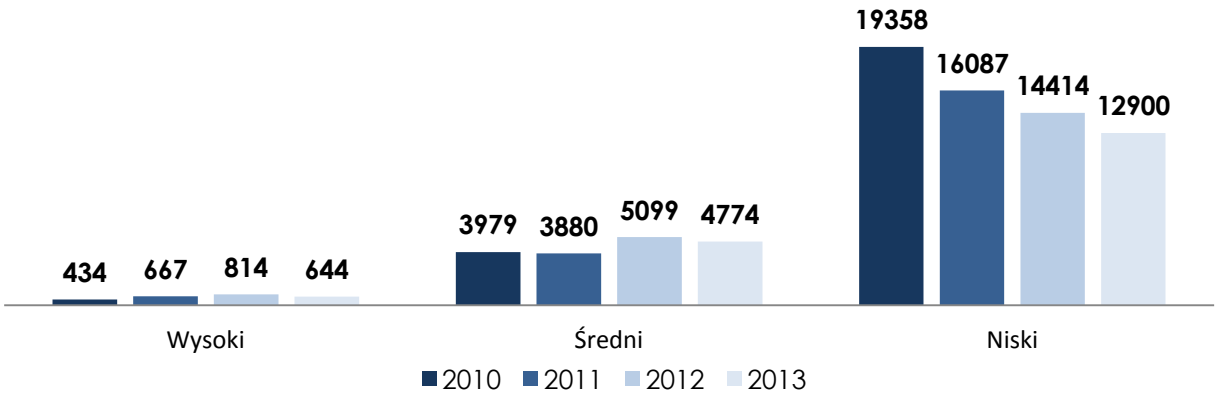
Rysunek 2-9: Rozkład procentowy źródeł ataków na sieci monitorowane przez system ARAKIS-GOV pod kątem unikalnych adresów IP

Jednakże patrząc ogólnie w stosunku do statystyk za rok 2012, statystyki źródeł ataków pod kątem pierwszych trzech pozycji w roku 2013 nie zmieniają się znacząco zarówno pod względem ilościowym, jak i samych źródeł ataków.

W powyższych wykresach dotyczących statystyk źródeł ataków, występuje element „nieznane", dotyczący adresów IP, które w chwili obecnej nie są przypisane do żadnego podmiotu – oznacza to, iż dokonano podszycia się (podmiany prawdziwego źródłowego adresu IP).

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

Poniżej, na *Rysunku 2-10* przedstawiono rozkład alarmów pod kątem poziomu istotności i zagrożeń, wygenerowanych przez system ARAKIS-GOV. Na podstawie przedmiotowego wykresu można zauważyć spadek ilości alarmów w każdym z poziomów zagrożenia. Różnica ilości alarmów w porównaniu z rokiem 2012 o poziomie istotności „wysoki" wyniosła 170, „średnim" 326 i „niskim" 1514.



Rysunek 2-10: Rozkład alarmów ze względu na priorytety w latach 2010-2013

Ze względu na fakt zastosowania w systemie ARAKIS-GOV systemów honeypot-owych do wykrywania ataków z sieci Internet, system dostarcza istotnych informacji na temat procesu rozpoznawania zasobów (skanowania). Na podstawie powyższych danych przedstawiono tabelę, zawierającą ranking skanowanych portów popularnych usług sieciowych pod względem liczby unikalnych adresów IP w skali całego roku.

Pozycja	Docelowy port/protokół	Procent wszystkich unikalnych IP	Opis
1	23/TCP	18,85%	Ataki na usługę telnet
2	445/TCP	16,71%	Ataki typu bufferoverflow na usługi Windows RPC
3	1433/TCP	10,40%	Ataki na MSSQL
4	80/TCP	7,72%	Ataki na aplikacje webowe
5	22/TCP	7,15%	Ataki na usługę SSH
6	3389/TCP	6,48%	Ataki na usługę RDP (zdalny pulpit)
7	139/TCP	3,47%	Ataki na usługę NetBIOS
8	8080/TCP	2,76%	Skanowanie w poszukiwaniu serwerów open web proxy
9	25/TCP	2,43%	Skanowanie w poszukiwaniu serwerów pocztowych typu open relay
10	1234/TCP	2,03%	Ataki na usługę SSH

Tabela 2-1: Tabela atakowanych portów w roku 2013 na podstawie danych z systemu ARAKIS-GOV

Powyższa tabela obrazuje skalę zainteresowania konkretnymi usługami przez złośliwe oprogramowanie, bądź samych atakujących. Pierwsze miejsce zajmuje port 23/TCP (ataki na usługę telnet), na drugim miejscu znajduje się port 445/TCP, który związany jest z usługami działającymi na systemie operacyjnym z rodziny Windows. Powyższy port również wykorzystywany jest

przez wiele rodzajów oprogramowania złośliwego takiego jak Conficker. Trzecie miejsce w statystykach zajmuje port 1433/TCP, czyli wszelakiego rodzaju ataki na serwery baz danych firmy Microsoft.

System ARAKIS-GOV, na podstawie analizy zebranego ruchu, próbuje dokonać identyfikacji zagrożenia na podstawie bazy znanych zagrożeń w postaci reguł systemu Snort[3]. Na tej podstawie zidentyfikowano zestawienie najczęściej widocznych reguł systemu Snort w systemie ARAKIS-GOV.

Pozycja	Procent wszystkich unikalnych IP	Reguła SNORT
1	17,51%	ET POLICY RDP connection request
2	17,16%	MISC MS Terminal server request
3	14,33%	ET POLICY Radmin Remote Control Session Setup Initiate
4	9,23%	ET POLICY Suspicious inbound to MSSQL port 1433
5	6,72%	BLEEDING-EDGE RDP connection request
6	6,29%	WEB-IIS view source via translate header
7	3,38%	ET SCAN Potential SSH Scan
8	2,28%	ET SCAN DCERPC rpcmgmtifids Unauthenticated BIND
9	2,17%	BLEEDING-EDGE POLICY Reserved IP Space Traffic - Bogon Nets 2
10	2,10%	ET POLICY RDP disconnect request

Tabela 2-2: Najczęściej dopasowane reguły do ruchu sieciowego widzianego przez system ARAKIS-GOV

[3] Snort – sieciowy system wykrywania włamań, dostępny na wolnej licencji, posiadający szeroki zakres mechanizmów detekcji ataków oraz umożliwiający, w czasie rzeczywistym, dokonywanie analizy ruchu i rejestrowanie pakietów przechodzących przez sieci oparte na protokołach IP/TCP/UDP/ICMP

Pierwsze dwie pozycje w statystykach zajmują reguły dotyczące ataków na usługi pulpitu zdalnego RDP, w których częściowo połączenia mogą być związane z nadal widoczną aktywnością robaka Morto[4].

Wśród zestawienia najczęściej atakowanych usług/portów (nie jest widoczny w TOP10, jednak zajmuje dość wysokie miejsce 19 z około 1 % unikalnych adresów IP) pojawił się port UDP/53, czyli port, na którym domyślnie działa usługa DNS (Domain Name System). Ma to związek z obserwacją zjawiska polegającego na poszukiwaniu otwartych serwerów DNS, tzw. „OpenReslovers" w celu przeprowadzenia ataku typu DDoS (rozproszony atak odmowy usługi).

W ramach prowadzonego skanowania wykorzystywano dwie metody poszukiwania serwerów otwartych DNS. Pierwsza metoda to bezpośrednie odpytanie adresu docelowego o dowolną domenę i oczekiwanie na odpowiedź.

```
14:21:35.093928  IP  122.136.196.116.2717  >  148.81.194.52.53:    60907+  [1au]  A?
aa3247.com. (51)
        0x0000:  4500004f09bb00005a11c1607a88c474E..O....Z..`z..t
        0x0010:  9451c2340a9d0035003befeaedeb 0100  .Q.4...5.;.....
        0x0020:  0001 0000 0000 0001 0661 6133 3234 3703  .........aa3247.
        0x0030:  636f 6d00 0001 0001 0000 2910 0000 0000  com.......).....
        0x0040:  0000 0c50 fa00 0800 0120 007d db0d cb    ...P.......}...
```

Źródłowy adres IP w tym wypadku 122.136.196.116 (z powyższego adresu należącego do *China Unicom* odnotowano największą ilość zapytań

[4] Morto - robak sieciowy atakujący źle zabezpieczone systemy Microsoft Windows, wykorzystując do tego celu protokół RDP (Remote Desktop Protocol) wykorzystywany przez tzw. zdalny pulpit. Morto nie eksploituje żadnej luki w oprogramowaniu, a atak polega na próbie odgadnięcia nazwy użytkownika i hasła (brute-force).

74602) jest prawdopodobnie adresem zainfekowanej stacji roboczej wcześniej przejętej przez atakującego.

Druga metoda polegała na wykorzystaniu serwera DNS, jako licznika odpowiedzi i jednocześnie weryfikatora. Poprawnie skonfigurowany serwer DNS powinien odpowiadać na zapytania tylko z określonych adresów IP. Wykorzystując powyższy fakt, atakujący może ustawić (spoofing) jako adres źródłowy należący do podsieci, którą ma zamiar skanować. Ponadto, dokonuje on konstrukcji zapytania DNS o domenę, której serwer autorytatywny nadzoruje (administruje). W przypadku, gdy na docelowym adresie IP uruchomiona jest usługa serwera DNS, zostanie wysłane zapytanie do serwera autorytatywnego dla danej domeny, czyli serwera kontrolowanego przez atakującego, co w rezultacie dostarcza informacji atakującemu o działającym serwerze DNS.

Z atakiem tego typu Zespół CERT.GOV.PL miał do czynienia pod koniec marca 2013 roku, kiedy to przeprowadzono atak na organizację non-profit „Spamhause", ukierunkowaną na walkę z niechcianymi wiadomościami email typu SPAM. Atak prawdopodobnie był odwetem za zblokowanie serwerów dostawcy internetowego o nazwie „CyberBunker", znanego z faktu utrzymywania stron o tematyce pornograficznej, terrorystycznej i serwującej oprogramowanie złośliwe (ISP utrzymuje m.in. strony „The Pirate Bay" i „Wikileaks").

Z technicznego punktu widzenia przeprowadzony atak był atakiem typu „reflected-amplification". Ataki typu „reflected" polegają głównie na generowaniu ruchu z podmienionym źródłowym adresem IP. Sytuacja taka powoduje, iż odpowiedzi na wygenerowany ruch trafiają na adres IP, który został podmieniony. Należy jednak pamiętać, że ataki tego typu dotyczą tylko i wyłącznie protokołu UDP. Natomiast rodzaj ataku typu „amplification", charakteryzuje się tym, iż wysyłając zapytanie o małych rozmiarach, otrzymujemy odpowiedź o zdecydowanie większej zawartości danych.

Poniżej przedstawiono przykład zapytania do serwera DNS o domenę cert.gov.pl i jego odpowiedź.

```
IP (tos 0x0, ttl 64, id 0, offset 0, flags [DF], proto UDP (17), length 57)
    SPOOF_IP.34909 > OPEN-RESOVLER: cert.gov.pl. (29)
        0x0000:  4500 0039 0000 4000 4011 0ce8 c0a8 0b56  E..9..@.@......V
        0x0010:  c2cc 9f01 885d 0035 0025 2e03 ada9 0100  .....].5.%......
        0x0020:  0001 0000 0000 0000 0463 6572 7403 676f  .........cert.go
        0x0030:  7602 706c 0000 ff00 01                   v.pl.....
IP (tos 0x0, ttl 246, id 40754, offset 0, flags [DF], proto UDP (17), length 242)
    OPEN-RESOVLER > SPOOF_IP.34909
        0x0000:  4500 00f2 9f32 4000 f611 b6fb c2cc 9f01  E....2@.........
        0x0010:  c0a8 0b56 0035 885d 00de 3320 ada9 8180  ...V.5.]..3.....
        0x0020:  0001 0007 0000 0000 0463 6572 7403 676f  .........cert.go
        0x0030:  7602 706c 0000 ff00 01c0 0c00 0f00 0100  v.pl............
        0x0040:  00a8 c000 0900 0004 6d61 696c c00c c00c  ........mail....
        0x0050:  000f 0001 0000 a8c0 000c 0014 036d 7832  .............mx2
        0x0060:  0361 6277 c011 c00c 000f 0001 0000 a8c0  .abw............
        0x0070:  0008 000f 036d 7831 c044 c00c 0001 0001  .....mx1.D......
        0x0080:  0000 a8c0 0004 c2b5 0502 c00c 0006 0001  ................
        0x0090:  0000 a8c0 0030 0562 696c 626f 046e 6173  .....0.bilbo.nas
        0x00a0:  6b03 6f72 67c0 1503 646e 7304 6e61 736b  k.org...dns.nask
        0x00b0:  c015 77ee 8744 0000 7080 0000 0e10 0009  ..w..D..p.......
        0x00c0:  3a80 0000 5460 c00c 0002 0001 0000 a8c0  :...T`..........
        0x00d0:  0012 066b 6972 6461 6e04 6e61 736b 036e  ...kirdan.nask.n
        0x00e0:  6574 c015 c00c 0002 0001 0000 a8c0 0002  et..............
        0x00f0:  c07a                                     .z
```

Na podstawie powyższego widać, iż rozmiar zapytania wynosi 57 bajtów, a odpowiedź serwera zawiera już 242 bajtów. Wygenerowanie dużej ilości tego typu zapytań powoduje czterokrotnie większą ilość danych w odpowiedzi, które trafiają na adres IP ofiary, co powoduje stan wysycenia łącza i powodzenie ataku DoS.

2.3.Testy bezpieczeństwa witryn internetowych administracji publicznej

Od dnia 1 lipca 2008 roku Zespół 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

przebadano, zostały poinformowane o wynikach, wykrytych podatnościach istniejących w ich systemach i poinstruowane, jak podatności te usunąć.

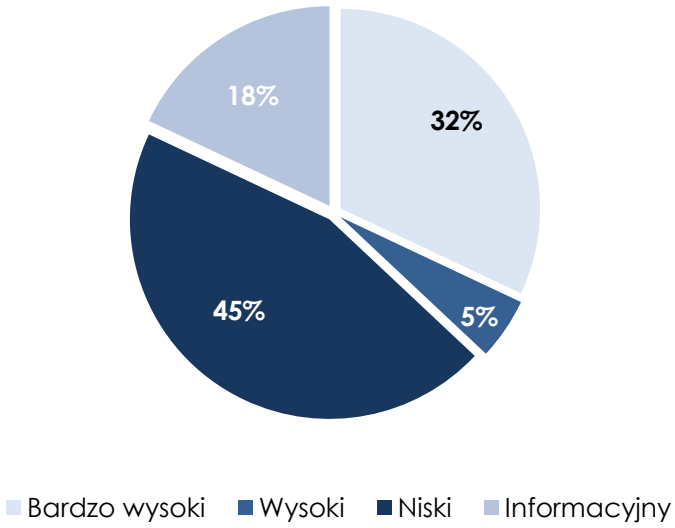
W 2013 roku przebadano 45 stron internetowych, należących do 15 instytucji państwowych. Stwierdzono ogółem 755 błędów w tym:

- 244 błędy o bardzo wysokim poziomie zagrożenia,
- 33 błędy o wysokim poziomie zagrożenia,
- 340 błędów o niskim poziomie zagrożenia,
- 138 błędów oznaczonych, jako informacyjne.

Wybrane podmioty, których strony WWW zostały przebadane przez Zespół CERT.GOV.PL pod kątem wykrycia ewentualnych podatności w 2013 roku:

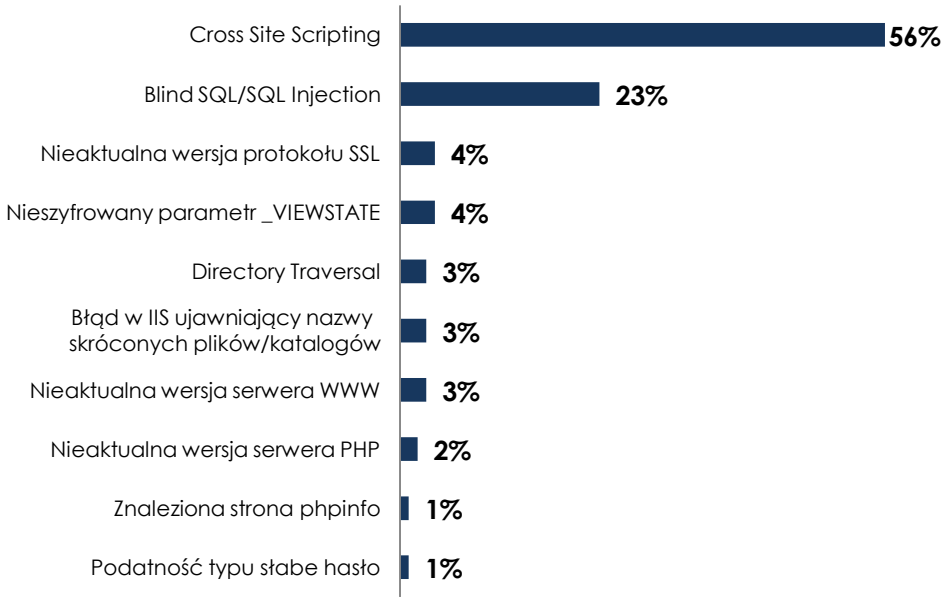
1. Ministerstwo Środowiska;
2. Ministerstwo Transportu, Budownictwa i Gospodarki Morskiej;
3. Narodowy Fundusz Zdrowia;
4. Urząd Komunikacji Elektronicznej;
5. Naczelny Sąd Administracyjny;
6. Mazowiecki Urząd Wojewódzki;
7. Zachodniopomorski Urząd Wojewódzki;
8. Urząd Miejski w Gdańsku;
9. Małopolski Urząd Wojewódzki;
10. Strony WWW należące do Ministerstwa Finansów (Izby Celne).

W trakcie skanowania witryn stwierdzono, że około 26% przebadanych z nich zawierało przynajmniej jedną podatność, którą należało uznać za krytyczną dla bezpieczeństwa serwera i publikowanych na stronie treści. Na 18-tu z 45-iu przebadanych stronach, zabezpieczenia były skuteczne i nie stwierdzono w nich żadnych podatności.



Rysunek 2-11: Statystyka wykrytych podatności w witrynach WWW, należących do administracji publicznej, według poziomu zagrożenia

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



Rysunek 2-12: Procentowy rozkład najpoważniejszych błędów w witrynach WWW, należących do administracji publicznej

Stan bezpieczeństwa przebadanych witryn	Ilość stron
Bardzo dobry	18
Średni	15
Niski	12

Tabela 2-3: Stan bezpieczeństwa witryn WWW, należących do administracji publicznej

Niski poziom bezpieczeństwa w witrynach WWW, należących do administracji publicznej wynikał między innymi z wykrytych:

- **Podatności typu Blind SQL/SQLinjection**

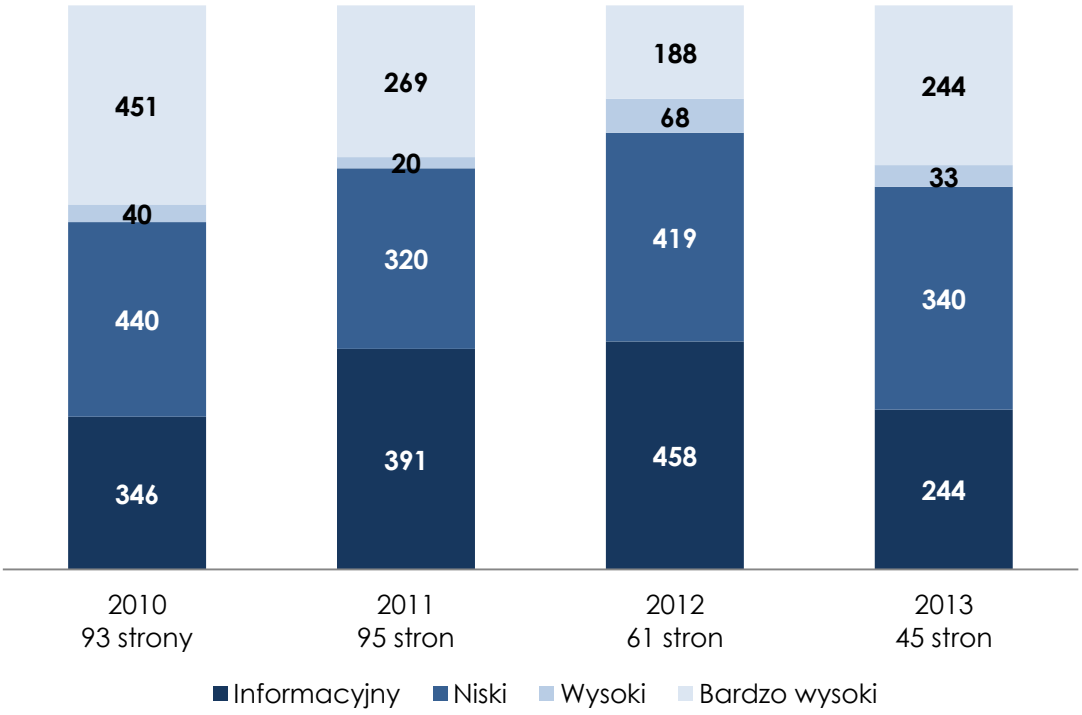
SQL injection / Blind SQL Injection jest podatnością pozwalającą atakującemu podmienić strukturę logiczną zapytania SQL kierowanego do produkcyjnej bazy danych, z której korzysta witryna WWW. Zagrożenie występuje, gdy aplikacja dołącza do zapytania SQL dane otrzymane od użytkownika strony bez filtrowania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

- **Podatności typu „słabe" hasło**

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

- **Podatności typu 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).



Rysunek 2-13: Liczbowy rozkład podatności przeskanowanych witryn z podziałem na istotność błędów w porównaniu z poprzednimi latami

3. Bezpieczeństwo internetowe administracji publicznej

Jak co roku, w 2013, odnotowano znaczną ilość ataków typu *website defacement*, których rezultatem była podmiana zawartości strony głównej portalu, umieszczenie na serwerze strony phishingowej lub dodanie pliku do witryny. Pomimo prowadzonych przez Zespół CERT.GOV.PL działań pro-aktywnych, takich jak testy bezpieczeństwa witryn oraz akcje uświadamiające, obszar cyberprzestrzeni polskiej administracji publicznej w dalszym ciągu jest podatny na tego typu ataki.

3.1. Incydenty obsługiwane przez Zespół CERT.GOV.PL

W zakresie podmian witryn administracji państwowej zaobserwowano głównie aktywność haktywistyczną, związaną z propagowaniem idei politycznych lub zwykłą dewastacją wizerunku strony. Rodzaj dokonywanych podmian wskazywał m.in. na sytuację w krajach Bliskiego Wschodu. Należy zauważyć, iż środowiska hakerskie włączają się w akcje polityczno-społeczne i dokonują ataków na strony internetowe w celu propagowania swoich poglądów, co w wypadku instytucji administracji publicznych, naraża je przede wszystkim na utratę wizerunku. Działania powyższe mogą również zachęcać do podejmowania tego typu zachowań przez kolejnych haktywistów. Aktywność haktywistyczna wykorzystuje przede wszystkim luki opublikowane w aplikacjach używanych do zarządzania witrynami internetowymi. Poniżej przedstawiony został przykład wykorzystania podatności występującej w systemie zarządzania treścią (CMS), pozwalającej na umieszczenie pliku na serwerze.

Rezultatem wykorzystania podatności był fakt dodania do systemu plików serwera skryptu, tzw. „shella", pozwalającego na zdalne zarządzanie witryną bez konieczności dokonania autoryzacji.

```
XXX.XXX.XXX.XXX - - [XX/ Aug /2013:16:56:30 +0200] "POST
/index.php?option=com_remository&Itemid=71&func=savefile HTTP/1.1" 200 2702
"https://XXX.gov.pl/index.php?option=com_remository&Itemid=71&func=addfile&id=
1" "Mozilla/5.0 (Windows NT 5.1; rv:2.0.1) Gecko/20100101 Firefox/4.0.1"
(…)
XXX.XXX.XXX.XXX - - [XX/ Aug /2013:16:56:34 +0200] "GET
/components/com_remository/images/search.gif HTTP/1.1" 200 1441
"https://XXX.gov.pl/index.php?option=com_remository&Itemid=71&func=savefile"
"Mozilla/5.0 (Windows NT 5.1; rv:2.0.1) Gecko/20100101 Firefox/4.0.1"
(…)
XXX.XXX.XXX.XXX - - [XX/Aug/2013:16:56:39 +0200] "GET
/components/com_remository_files/file_image_218/ HTTP/1.1" 200 373
"https://XXX.gov.pl/components/com_remository_files/" "Mozilla/5.0 (Windows NT 5.1;
rv:2.0.1) Gecko/20100101 Firefox/4.0.1"
```

Poniżej przedstawione zostały wybrane incydenty, związane z podmianą stron WWW, które obsługiwał Zespół CERT.GOV.PL w roku 2013:

- W dniu 9 stycznia 2013 roku miała miejsce podmiana witryny internetowej, należącej do Departamentu Analiz Ekonomicznych i Prognoz Ministerstwa Pracy i Polityki Społecznej;
- W dniu 14 stycznia 2013 roku miała miejsce podmiana witryny internetowej „otwarta szkoła", należącej do Ministerstwa Edukacji Narodowej;
- W dniu 28 marca 2013 roku podmieniono witrynę internetową, należącą do Powiatowego Inspektoratu Nadzoru Budowlanego Miasta Skierniewice;
- W dniu 17 czerwca 2013 roku miała miejsce podmiana witryny internetowej, należącej do Sądu Rejonowego w Wieluniu;
- W dniu 22 lipca 2013 roku miała miejsce podmiana witryny internetowej, należącej do Powiatowego Inspektoratu Weterynarii w Olecku;
- Dnia 29 lipca 2013 roku miały miejsce podmiana m. in. witryn internetowych, należących do Sądu Okręgowego we Wrocławiu;

- W dniu 13 sierpnia 2013 roku miała miejsce podmiana witryny internetowej, należącej do Kampinoskiego Parku Narodowego;
- W dniu 13 sierpnia 2013 roku miała miejsce podmiana witryn internetowych, należących do Sądów: Okręgowego i Rejonowego w Częstochowie;
- W dniu 16 sierpnia 2013 roku miała miejsce podmiana witryny internetowej, należącej do Powiatowego Inspektoratu Nadzoru Budowlanego w Inowrocławiu;
- W dniu 26 sierpnia 2013 roku miała miejsce podmiana witryny internetowej, należącej do Gminnego Zespołu Komunalnego Gminy Pawłowice;
- W dniu 30 sierpnia 2013 roku miała miejsce podmiana witryny internetowej, należącej do Miasta i Gminy Murowana Goślina;
- W dniu 1 września 2013 roku miała miejsce podmiana witryny internetowej, należącej do Polskiej Agencji Informacji i Inwestycji Zagranicznych;
- W dniu 18 września 2013 roku miała miejsce podmiana witryny internetowej, należącej do Powiatowego Urzędu Pracy w Kościanie;
- W dniu 18 września 2013 roku miała miejsce podmiana witryny internetowej, należącej do Centrum Geomatyki Stosowanej Wojskowej Akademii Technicznej;
- W dniu 28 października 2013 roku miała miejsce podmiana witryny internetowej, należącej do Krajowej Szkoły Administracji Publicznej oraz witryny internetowej należącej do Projektu Systemowego Ministerstwa Zdrowia;
- W dniu 6 listopada 2013 roku miała miejsce podmiana witryny internetowej, należącej do Polskiej Agencji Rozwoju Przedsiębiorczości;

- W dniu 15 listopada 2013 roku miała miejsce podmiana witryny internetowej, należącej do Wielkopolskiego Urzędu Wojewódzkiego w Poznaniu.

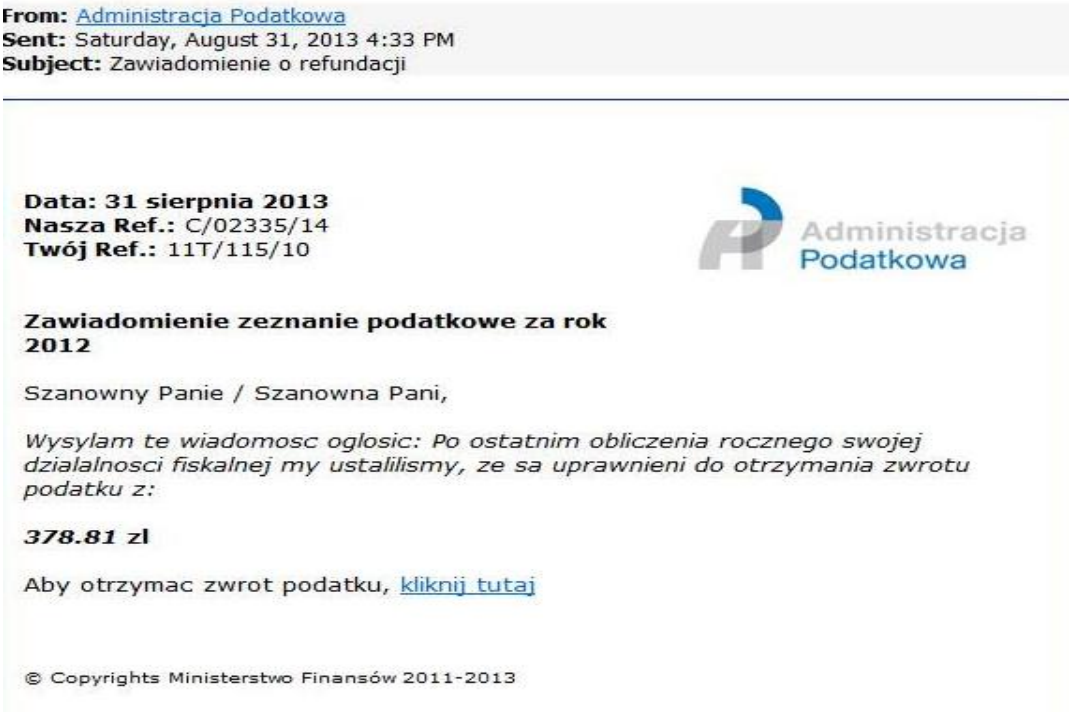
3.2. Przykłady analizy incydentów obsługiwanych przez Zespół CERT.GOV.PL

- W dniu 13 lutego 2013 roku Zespół CERT.GOV.PL uzyskał informację o skutecznej próbie uzyskania nieautoryzowanego dostępu do panelu administracyjnego portalu www.ewus.csioz.gov.pl, co skutkowało zmianą ustawień użytkowników portalu oraz edycją zawartości treści portalu informacyjnego. Zespół CERT.GOV.PL dokonał analizy powłamaniowej, jednocześnie wskazując błędy w zabezpieczeniu aplikacji, które to zostały usunięte przez administratorów serwisu.

```
1  GET /admin/users/ HTTP/1.1" 200
2  POST /admin/users/add HTTP/1.1" 302
3  GET /admin/users/edit/10
4  POST /admin/users/login HTTP/1.1" 302
5  GET /admin HTTP/1.1" 200
```

Rysunek 3-1: Mechanizm ataku na stronę http://www.ewus.csioz.gov.pl

- 2 września 2013 roku Zespół CERT.GOV.PL uzyskał informację o podszywaniu się pod instytucję administracji państwowej, celem wyłudzenia danych osobowych. Atakujący dokonał spreparowania wiadomości e-mail, zawierającej odnośnik do strony, na której umieszczono formularz do wypełnienia.



From: Administracja Podatkowa
Sent: Saturday, August 31, 2013 4:33 PM
Subject: Zawiadomienie o refundacji

Data: 31 sierpnia 2013
Nasza Ref.: C/02335/14
Twój Ref.: 11T/115/10

Administracja Podatkowa

Zawiadomienie zeznanie podatkowe za rok 2012

Szanowny Panie / Szanowna Pani,

Wysylam te wiadomosc oglosic: Po ostatnim obliczenia rocznego swojej dzialalnosci fiskalnej my ustalilismy, ze sa uprawnieni do otrzymania zwrotu podatku z:

378.81 zl

Aby otrzymac zwrot podatku, kliknij tutaj

© Copyrights Ministerstwo Finansów 2011-2013

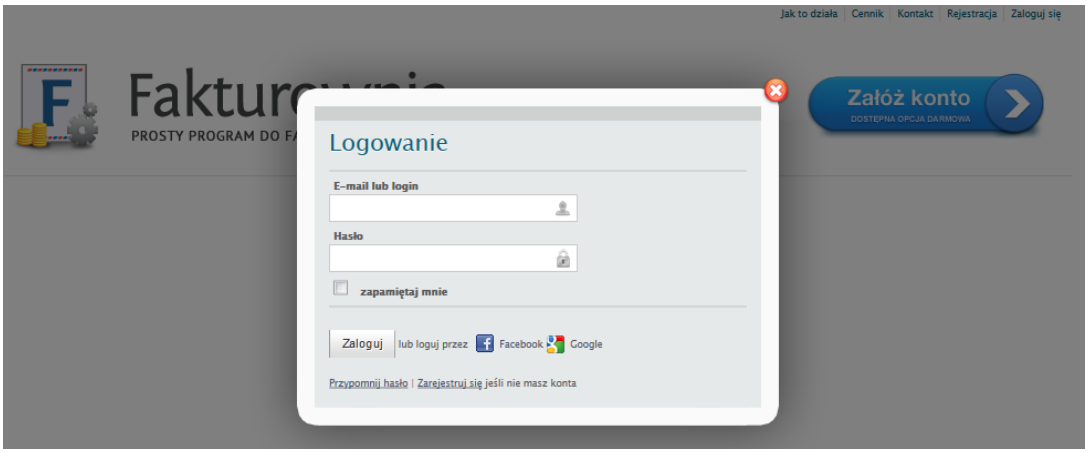
Rysunek 3-2: Wiadomość e-mail podszywająca się pod wiadomość przesłaną przez instytucję administracji państwowej.

- W dniu 30 września 2013 roku Zespół CERT.GOV.PL uzyskał informację, że w sieci lokalnej instytucji administracji państwowej znajdują się komputery zainfekowane złośliwym oprogramowaniem typu botnet "citadel". W wyniku kompromitacji stacji roboczych, atakujący uzyskał informacje na temat danych autoryzacyjnych do zasobów, stron oraz kont pocztowych pracowników instytucji administracji państwowej. Zespół CERT.GOV.PL poinformował administratorów instytucji, w których incydent miał miejsce i zalecił weryfikację wskazanych stacji roboczych pod kątem występowania oprogramowania złośliwego i zmianę wszelkich haseł dostępowych do skompromitowanych kont.

```
Serwer FTP: hot.sputniksoftware.com , Username: [redacted], Password: [redacted]
Poczta: [redacted]wp.pl, Username: [redacted], Password: bbxxxxxxxxxxxxx
Poczta: [redacted]gozdowo.eu, Username: [redacted], Password: Soxxxxxxxxxxxxx
Poczta: [redacted]wp.pl, Username: [redacted]wp.pl, Password: 98xxxxxxxxxxxxx
System Bankowości Elektronicznej: https://www.pekao24.pl/, Username: [redacted]
Poczta: poczta.o2.pl , Username: [redacted], Password: Tyxxxxxxxxxxxxx
Portal: http://www.ops.pl/forum.php, Username: [redacted], Password: oxxxxxxxxxxxxx
Poczta: https://poczta.interia.pl/, Username: [redacted]interia.pl, Password: maxxxxxxxxxxxxx
Poczta: [redacted]pup.sosnowiec.pl , Username: [redacted]pup.sosnowiec.pl, Password: sr4xxxxxxxxxxxxx
System bankowości elektronicznej: https://online.ingbank.pl, Username: [redacted]
System bankowości elektronicznej: https://login.ingbusinessonline.pl, Username: [redacted]
Poczta: http://wp.pl, Username: [redacted], Password: kakxxxxxxxxxxxx
```

Rysunek 3-3: Przykładowe skompromitowane dane autoryzacyjne

- W dniu 3 października 2013 roku Zespół CERT.GOV.PL uzyskał informację o upublicznieniu w sieci Internet danych dotyczących logowania do usług Adobe przez użytkowników instytucji administracji państwowej. W związku z powyższym, zwrócono się do administratorów zagrożonych instytucji o poinformowanie podległych jednostek o incydencie oraz zmianę haseł dostępowych do skrzynek pocztowych, w przypadkach gdy hasła były tożsame z hasłami do usług Adobe.
- Kolejnym incydentem obsługiwanym przez Zespół CERT.GOV.PL była próba pozyskania danych autoryzacyjnych użytkowników systemów teleinformatycznych instytucji administracji państwowej, polegająca na spreparowaniu stron o specjalnej zawartości, służących do przeprowadzenia ataków phishingowych. Dzięki działaniom podjętym przez Zespół CERT.GOV.PL ograniczono możliwość wyłudzeń danych.



Rysunek 3-4: Specjalnie spreparowana strona, służąca do wyłudzania danych

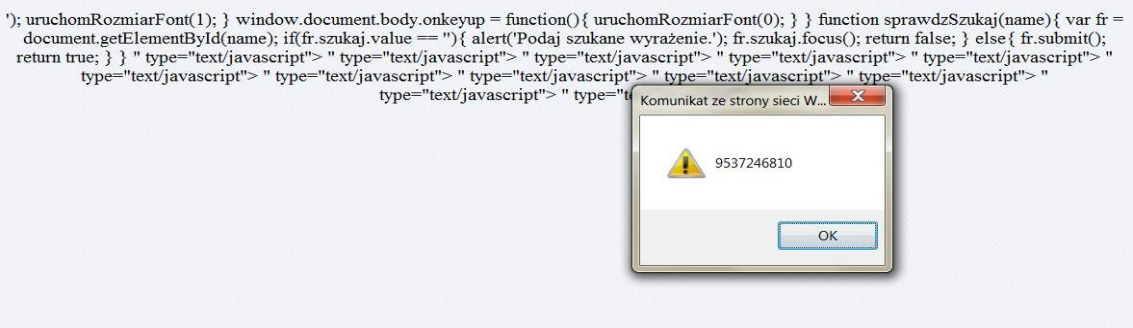
- Zespół CERT.GOV.PL obsługiwał również incydenty, dotyczące prób ataku typu SQL Injection i XSS (cross-sitescripting) na zasoby teleinformatyczne, znajdujące się w przestrzeni adresowej instytucji administracji państwowej. Ataki te mogły skutkować uzyskaniem informacji o strukturze bazy danych, wyciekiem, istotnych z punktu widzenia instytucji danych lub nieuprawnionym wykonywaniem dowolnego kodu. Zespół CERT.GOV.PL o próbach ataków poinformował odpowiednie zespoły Abuse, do których puli należały adresy IP, z których dokonano prób ataków.

```
---------------------- XSS ----------------------
2013-04-13
13:13:08
[redacted]
Mozilla/5.0 (Windows NT 6.1) AppleWebKit/537.31 (KHTML, like Gecko) Chrome/26.0.1410.64 Safari/537.3
przeszukiwanie (doc_odp)
ATAK! znak większości <script>/xss/</script> and <script>/xss/</script>


2013-04-13
13:13:04
[redacted]
Mozilla/5.0 (Windows NT 6.1) AppleWebKit/537.31 (KHTML, like Gecko) Chrome/26.0.1410.64 Safari/537.3
przeszukiwanie (doc_odp)
ATAK! znak większości <script>/xss/</script> and

---------------------- SQL Injection ----------------------
2013-04-11
19:06:43
[redacted]
Mozilla/5.0 (compatible; MSIE 9.0; Windows NT 6.1; WOW64; Trident/5.0)
chronologicznie (otk_odp)
ATAK! SELECT - : 1';SELECT PG_SLEEP(4); -- 01/01/1967 01/01/1967 data_desc ZU 1 1

2013-04-11
19:49:32
[redacted]
Mozilla/5.0 (compatible; MSIE 9.0; Windows NT 6.1; WOW64; Trident/5.0)
hasla2 (hjo2_odp)
ATAK! SELECT - : 1';SELECT PG_SLEEP(5.336); -- TAK
```

Rysunek 3-5: Zablokowane próby ataku typu XSS i SQL Injection

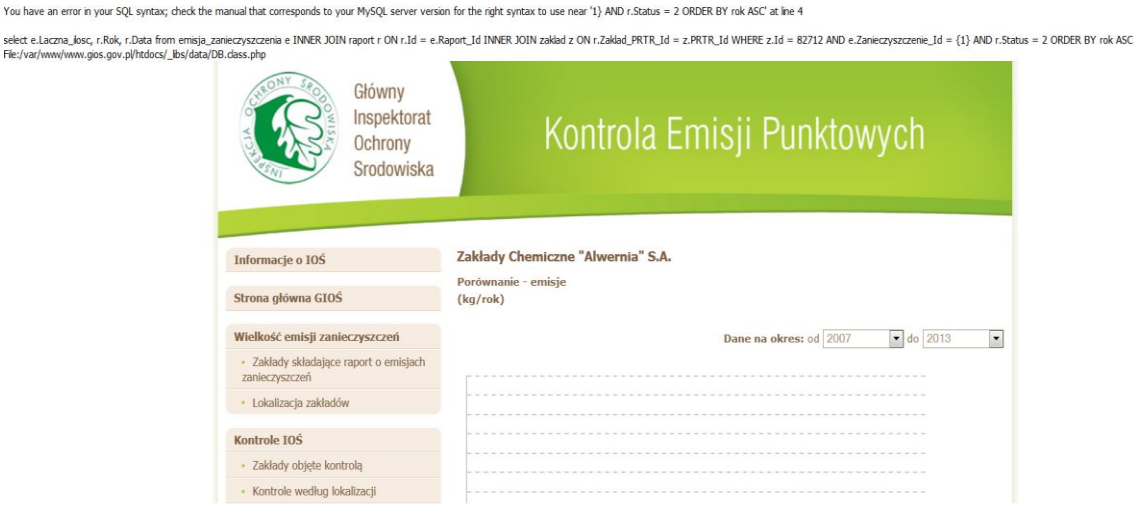
- Zespół CERT.GOV.PL obsługiwał również incydenty dotyczące podatności typu SQL Injection oraz XSS, występujące w witrynach instytucji administracji państwowej. Ataki te pozwalały na uzyskanie informacji o strukturze bazy danych oraz danych autoryzacyjnych (login i hasło) do strony lub też pozwalały na nieuprawnione wykonywanie

dowolnego kodu. Dzięki współpracy administratorów przedmiotowych serwisów z Zespołem CERT.GOV.PL większość błędów została zlokalizowana i usunięta.



Rysunek 3-6: Strony instytucji administracji państwowej podatne na ataki typu XSS

Rysunek 3-7: Strony instytucji administracji państwowej podatne na ataki typu XSS



Rysunek 3-8: Błąd typu SQL Injection

- Kolejnym przykładem incydentów, obsługiwanych przez Zespół CERT.GOV.PL, były zgłoszenia dotyczące publikacji na portalach internetowych baz danych użytkowników pochodzących z witryn należących do instytucji administracji państwowej. Poinformowano administratorów oraz osoby, których dane zostały udostępnione, a także zalecono im natychmiastową zmianę haseł do skompromitowanych kont, podjęcie działań mających na celu wykrycie oraz wyeliminowanie luk w systemach.

Rysunek 3-9: Przykładowe publikowane w sieci Internet dane użytkowników instytucji administracji państwowej

Rysunek 3-10: Przykładowe publikowane w sieci Internet dane użytkowników instytucji administracji państwowej

- W pierwszym kwartale 2013 roku Rządowy Zespół Reagowania na Incydenty Komputerowe CERT.GOV.PL uczestniczył w analizie incydentu dotyczącego ataku ukierunkowanego na zasoby teleinformatyczne Kancelarii Prezesa Rady Ministrów i Ministerstwa Spraw Zagranicznych. W wyniku przełamania zabezpieczeń nastąpił nieuprawniony dostęp do danych użytkowników systemu teleinformatycznego w tym m.in. loginów i kryptograficznych skrótów haseł. W przedmiotowych sprawach prowadzone jest aktualnie postępowanie przygotowawcze przez Prokuraturę Okręgową w Warszawie.
- W październiku 2013 roku Rządowy Zespół Reagowania na Incydenty Komputerowe CERT.GOV.PL brał udział w analizie incydentu związanego z uzyskaniem bez uprawnienia dostępu do informacji stanowiących dane informatyczne poczty elektronicznej w domenie trade.gov.pl należącej do Ministerstwa Gospodarki. W sprawie tej prowadzone jest postępowanie przygotowawcze przez Prokuraturę Rejonową w Warszawie.
- Zespół CERT.GOV.PL w listopadzie 2013 roku prowadził czynności zmierzające do ustalenia nadawcy wiadomości mailowych, zawierających groźby ataków bombowych. Groźby były wysyłane w nocy z 16 na 17 listopada 2013 roku do 87 instytucji na terenie całego kraju, w tym do ministerstw, prokuratur, komend policji oraz innych urzędów, co często powodowało ewakuację osób. Zespół CERT.GOV.PL brał czynny udział w ustaleniach nadawcy wysyłanych

wiadomości, współpracując z Policją. Rezultatem wspólnych działań było zatrzymanie przez funkcjonariuszy Policji osoby podejrzewanej o rozesłanie wiadomości mailowych, zawierających groźby związane z podłożeniem ładunków wybuchowych.

4. Współpraca krajowa i międzynarodowa

W ramach prowadzonej współpracy krajowej Zespół CERT.GOV.PL brał aktywny udział w opracowywaniu dokumentu pt. *Polityka Ochrony Cyberprzestrzeni Rzeczypospolitej Polskiej*, przyjętego uchwałą Nr 101 Rady Ministrów w dniu 25 czerwca 2013 roku.

Ponadto, w roku 2013 odbyły się kolejne edycje ćwiczeń w obszarze reagowania na incydenty bezpieczeństwa w cyberprzestrzeni, w tym m.in. międzynarodowe ćwiczenia NATO Cyber Coalition 2013 (zwanych dalej NATO CC 2013).

4.1. Polityka Ochrony Cyberprzestrzeni Rzeczypospolitej Polskiej

Zespół CERT.GOV.PL współpracował z Ministerstwem Administracji i Cyfryzacji w opracowaniu dokumentu pt. *Polityka Ochrony Cyberprzestrzeni Rzeczypospolitej Polskiej* (zwany dalej *Polityką*). Przedmiotowy dokument wyznacza kierunki działania państwa w obszarze cyberprzestrzeni RP (zwanej dalej CRP). Celem strategicznym wszystkich działań jest osiągnięcie akceptowalnego poziomu cyberbezpieczeństwa państwa. Do stosowania zapisów *Polityki* zobligowane są wszystkie podmioty administracji rządowej, natomiast pozostałe jednostki i urzędy państwowe mogą stosować się do jej treści na zasadzie rekomendacji. Adresatami *Polityki*, poza wymienionymi podmiotami, są także wszyscy użytkownicy cyberprzestrzeni, zarówno osoby fizyczne, jak i przedsiębiorcy korzystający z sieci Internet.

Polityka stanowi podstawę do wypracowania koncepcji zarządzania bezpieczeństwem infrastruktury, funkcjonującej w ramach CRP oraz wytycznych do opracowania podstaw wykonywania zadań w tym zakresie przez administrację rządową. Jednym z elementów służącym podniesieniu bezpieczeństwa ma być wdrożenie w jednostkach administracji publicznej, a także rekomendowanie wdrożenia w podmiotach niepublicznych,

mechanizmów służących zapobieganiu i wczesnemu wykrywaniu zagrożeń oraz właściwemu postępowaniu w przypadku stwierdzonych incydentów. Kluczowym elementem zapewnienia bezpieczeństwa w cyberprzestrzeni ma być szacowanie ryzyka, które zgodnie z zapisami dokumentu, mają dokonywać jednostki administracji rządowej. Biorąc pod uwagę powyższe, Zespół CERT.GOV.PL przedstawił ministrowi właściwemu ds. informatyzacji katalog zawierający specyfikację zagrożeń oraz możliwych podatności godzących w bezpieczeństwo cyberprzestrzeni RP. Przygotowano też rekomendacje dotyczące metodologii szacowania ryzyka w instytucjach państwowych. W celu realizacji zapisu *Polityki,* związanego z kształceniem kadry urzędniczej w dziedzinie bezpieczeństwa systemów eleinformatycznych, Zespół CERT.GOV.PL w 2013 roku przeprowadził kolejną serię bezpłatnych szkoleń dla administratorów systemów teleinformatycznych administracji publicznej. Szkolenia oferowane były w ramach współpracy Agencji Bezpieczeństwa Wewnętrznego z firmą Microsoft w zakresie bezpieczeństwa teleinformatycznego SCP (Security Cooperation Program). Szkolenia, w których uczestniczyło 120 osób, kierowane były do administratorów administracji rządowej i samorządowej w zakresie:

- podstaw bezpieczeństwa, administracji i zarządzania systemami Microsoft Windows 7 oraz omówienie nowości dotyczących bezpieczeństwa w Microsoft Windows 8;
- bezpieczeństwa, administracji i zarządzania systemami Microsoft Windows Server 2008 oraz nowości dotyczących bezpieczeństwa w Microsoft Windows Server 2012.

Ponadto, Zespół CERT.GOV.PL zorganizował szkolenia dla użytkowników systemu ARAKIS-GOV, w których udział wzięło 40 osób.

Rezultatem prowadzonych działań w ramach realizacji zapisów *Polityki* miało być wdrożenie skutecznego systemu koordynacji i wymiany informacji pomiędzy publicznymi i prywatnymi podmiotami, odpowiedzialnymi za

bezpieczeństwo cyberprzestrzeni. W związku z powyższym, ustanowiony został Krajowy System Reagowania na Incydenty Komputerowe w CRP, w ramach którego Zespół CERT.GOV.PL realizuje zdania reagowania na incydenty we współpracy z Resortowym Centrum Zarządzania Bezpieczeństwem Sieci i Usług Teleinformatycznych, właściwym dla sfery militarnej.

Efektem realizacji *Polityki* ma być wyższy poziom bezpieczeństwa cyberprzestrzeni Polski oraz zwiększenie odporności państwa na ataki terrorystyczne prowadzone w cyberprzestrzeni. Wzrosnąć ma także efektywność wprowadzanych zabezpieczeń, wynikająca z zaangażowania w proces podniesienia bezpieczeństwa w cyberprzestrzeni wszystkich użytkowników.

4.2. Ćwiczenia NATO Cyber Coalition 2013

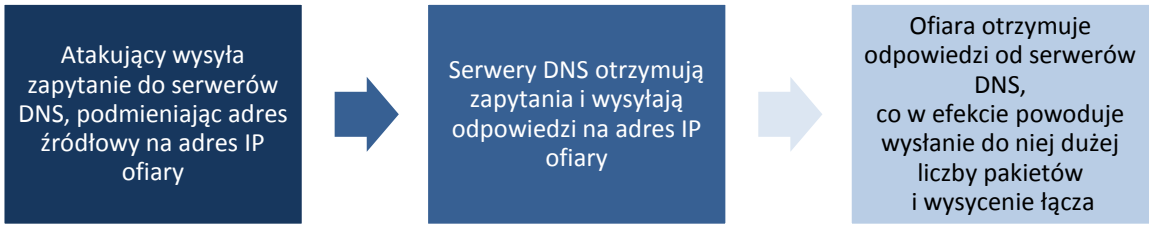
Kolejna edycja ćwiczeń dotyczyła wymiany informacji o incydentach i przeprowadzania wspólnej analizy zagrożeń cyberprzestrzeni państw NATO. Podjęte działania pozwoliły na testowanie (w obszarze technicznym) możliwości działania Zespołu CERT.GOV.PL w zakresie wykrywania ataków i reagowania, we współpracy z innymi zespołami bezpieczeństwa państw NATO. Działania Zespołu CERT.GOV.PL polegały głównie na analizie i przekazywaniu informacji o wykrytych zagrożeniach, dotyczących sieci teleinformatycznych, do innych zespołów reagowania państw NATO. Główna rola koordynatora w zakresie reagowania państw NATO należała do zespołu NATO Computer Incident Response Capability.

W ćwiczeniach wzięło udział ponad 30 krajów. Główną siedzibą ćwiczeń był ośrodek szkoleniowy w Estonii. Poza krajami członkowskimi NATO, w ćwiczeniach NATO CC 2013, brały udział także Austria, Finlandia, Irlandia, Szwecja i Szwajcaria. Status obserwatora miały Nowa Zelandia i Unia Europejska.

5. Podsumowanie roku

5.1. Open DNS Resolver

W 2013 roku Zespół CERT.GOV.PL zaobserwował podatności serwerów DNS znajdujących się w przestrzeni adresowej instytucji administracji państwowej, pozwalających na wykonanie zapytania DNS o dowolną domenę, z dowolnego adresu IP z sieci Internet. Usługa DNS, która standardowo działa na porcie 53, pozwala na translację ciągu znaków tworzących adresy witryn internetowych, które są zrozumiałe dla człowieka, na adresy IP zrozumiałe dla urządzeń sieciowych.



Rysunek 5-1: Schemat wykorzystania podatności DNS

Podatność ta może być wykorzystana do przeprowadzenia ataku ze zwielokrotnieniem (ang. amplification attack), który jest jedną z odmian ataku Distributed Denial of Service. Jednym ze sposobów na przeprowadzenie ataku jest wysyłanie, do powszechnie dostępnego serwera DNS zapytań DNS lookup ze zmodyfikowanym (podmienionym) adresem źródłowym, ustawionym na adres IP ofiary. W wyniku powyższego, wszystkie odpowiedzi kierowane do serwera DNS, są przesyłane na adres IP ofiary, co w rezultacie powoduje wysłanie do niego ogromnej liczby pakietów. Na *Rysunkach: 5-2 i 5-3* przedstawiono kolejno: odpowiedź od serwera DNS wykazującego podatność i odpowiedź od poprawnie skonfigurowanego serwera DNS.

```
bash-4.2$ dig google.pl @IP serwera DNS

; <<>> DiG 9.9.1-P3 <<>> google.pl @IP serwera DNS
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 45204
;; flags: qr rd ra; QUERY: 1, ANSWER: 3, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 4000
;; QUESTION SECTION:
;google.pl.                     IN      A

;; ANSWER SECTION:
google.pl.              103     IN      A       173.194.116.151
google.pl.              103     IN      A       173.194.116.152
google.pl.              103     IN      A       173.194.116.159

;; Query time: 12 msec
;; SERVER: IP serwera DNS  #53( IP serwera DNS )
;; WHEN: Mon Jan 20 16:25:07 2014
;; MSG SIZE  rcvd: 86

bash-4.2$
```

Rysunek 5-2: Odpowiedź otrzymana od niepoprawnie skonfigurowanego serwera DNS

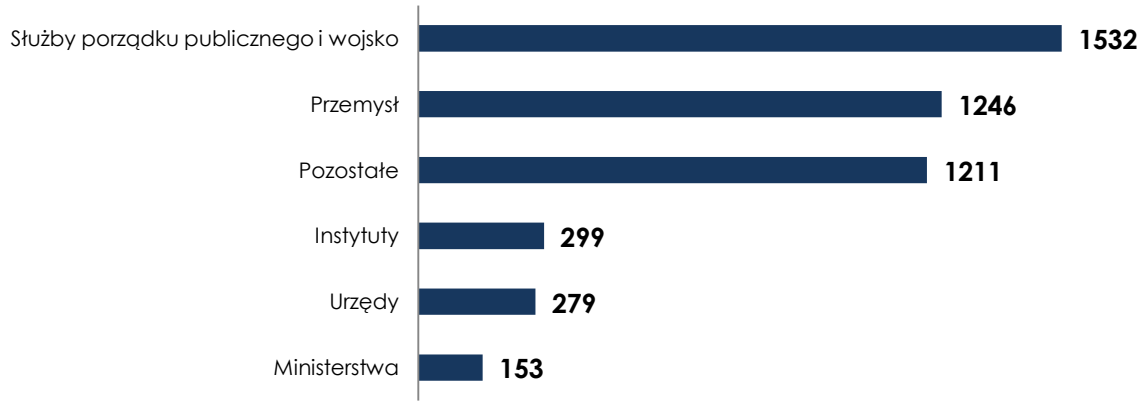
```
bash-4.2$ dig google.pl @IP serwera DNS

; <<>> DiG 9.9.1-P3 <<>> google.pl @IP serwera DNS
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: SERVFAIL, id: 28425
;; flags: qr rd; QUERY: 1, ANSWER: 0, AUTHORITY: 0, ADDITIONAL: 1
;; WARNING: recursion requested but not available

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 1280
;; QUESTION SECTION:
;google.pl.                     IN      A

;; Query time: 23 msec
;; SERVER: IP serwera DNS  #53( IP serwera DNS  )
;; WHEN: Mon Jan 20 16:20:31 2014
;; MSG SIZE  rcvd: 38

bash-4.2$
```

Rysunek 5-3: Odpowiedź otrzymana od poprawnie skonfigurowanego serwera DNS

Poniżej zaprezentowany został przykład zmian konfiguracyjnych, jakie należy wprowadzić do serwera DNS Bind 9.x Authoritative[5], aby wyeliminować opisywaną powyżej podatność (zmiany spowodują wyłączenie rekursji).

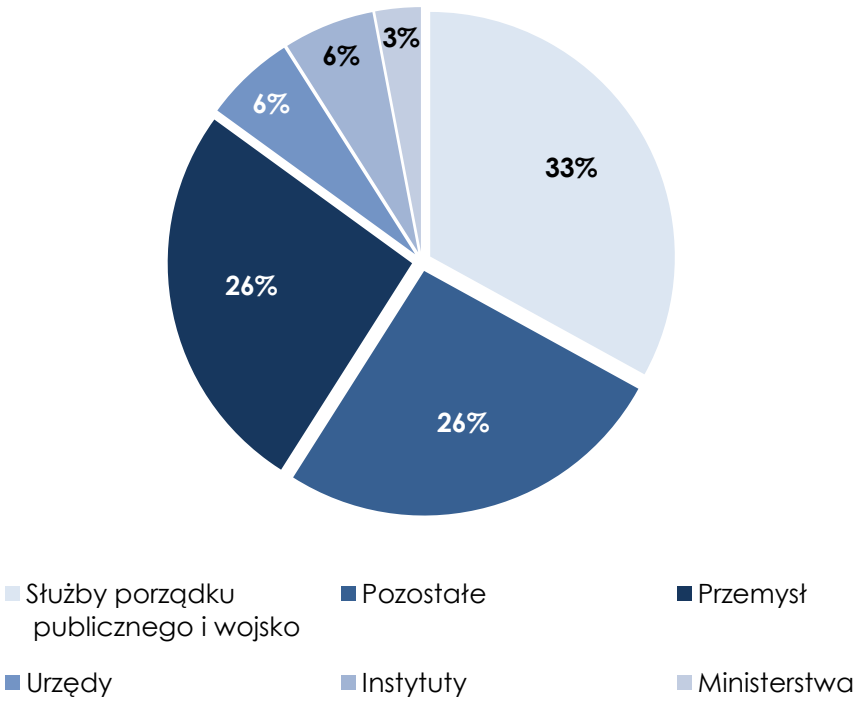
```
options {
    recursion no;
    additional-from-cache no;
        };
```

W 2013 roku Zespół CERT.GOV.PL wysłał do instytucji administracji państwowej 4 716 informacji o podatności serwerów DNS. Najwięcej powiadomień zostało wysłanych do instytucji skategoryzowanych jako „służby porządku publicznego i wojsko" (33% wszystkich wysłanych powiadomień) oraz „przemysł" (26%). Czołowe miejsce w statystykach instytucji z przedmiotowych sektorów spowodowane jest m.in. dużą liczbą ich struktur organizacyjnych na terytorium Rzeczypospolitej Polskiej.



Rysunek 5-4: Ilość wysłanych informacji o podatności DNS do instytucji administracji państwowej

[5] Serwer udzielając odpowiedzi odwołuje się wyłącznie do posiadanych przez siebie danych (brak rekursji).



Rysunek 5-5: Udział procentowy typów instytucji do ilości wysłanych zgłoszeń w roku 2013

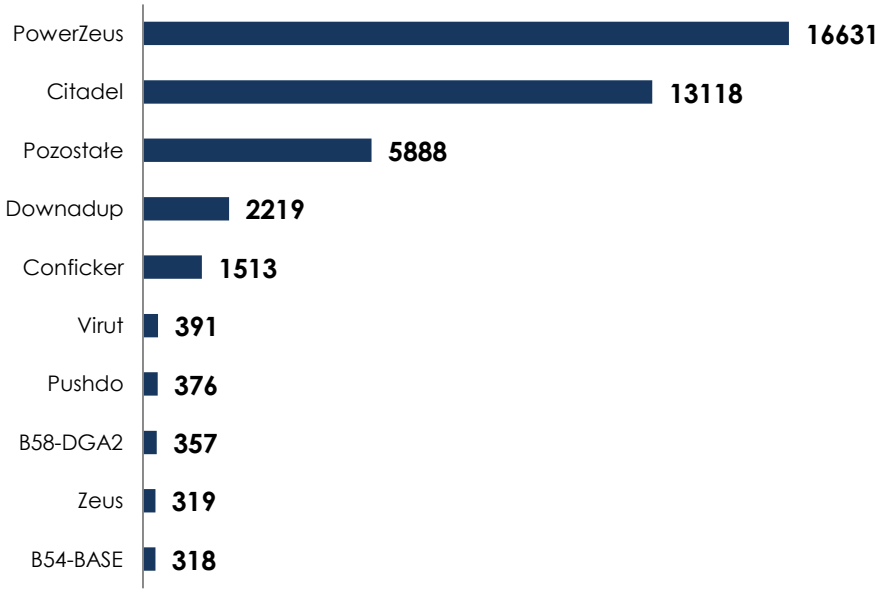
5.2. Botnety

W wyniku prowadzonych działań w roku 2013 Zespół CERT.GOV.PL zarejestrował 39 369 przepływów, polegających na połączeniach z infrastruktury teleinformatycznej instytucji administracji państwowej do sieci botnet.

Sieci botnet klasyfikowane są jako typ oprogramowania złośliwego, wytworzonego w celu przejęcia kontroli nad hostem komputerowym do wykonywania założonych przez twórców celów, np. kradzieży poufnych informacji, przeprowadzania ataków na inne systemy, propagacji infekcji na inne komputery, rozsyłania niechcianej korespondencji (spam), itp. Skala infekcji oprogramowaniem typu botnet jest zróżnicowana, jednak przytaczane przez głównych producentów oprogramowania

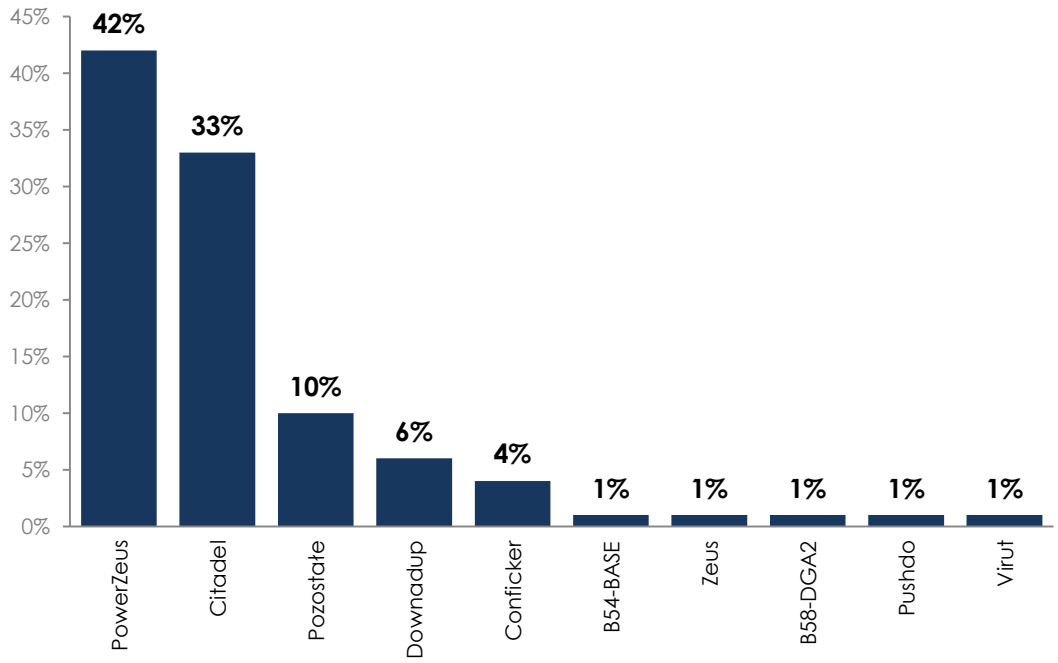
antywirusowego statystyki, pozwalają stwierdzić, że aktywność sieci botnet jest proporcjonalna do skali penetracji sieci Internet w danym kraju.

Tego typu incydenty obsługiwane są przez Zespół CERT.GOV.PL, dzięki dostępowi do systemu detekcji sieci botnet, pozwalającego na informowanie o zainfekowanych hostach z klasy adresów, należących do instytucji państwowych. W ramach obsługi incydentów, stosowne informacje przekazywane są do administratorów sieci instytucji, celem wykrycia źródła infekcji. Z uwagi na stosowane zasady i mechanizmy bezpieczeństwa w systemach administracji państwowej, zagrożenia tego typu są zwykle szybko neutralizowane.



Rysunek 5-6: Top 10 ilości przepływów z instytucji administracji państwowej do sieci botnet

W 2013 roku, wśród najczęściej wykrywanych typów sieci botnet w instytucjach administracji państwowej, wymienić należy: PowerZeus (42%), Citadel (33%), Downadup (6%) i Conficker (4%).



Rysunek 5-7: Udział procentowy ilości przepływów do sieci botnet w roku 2013

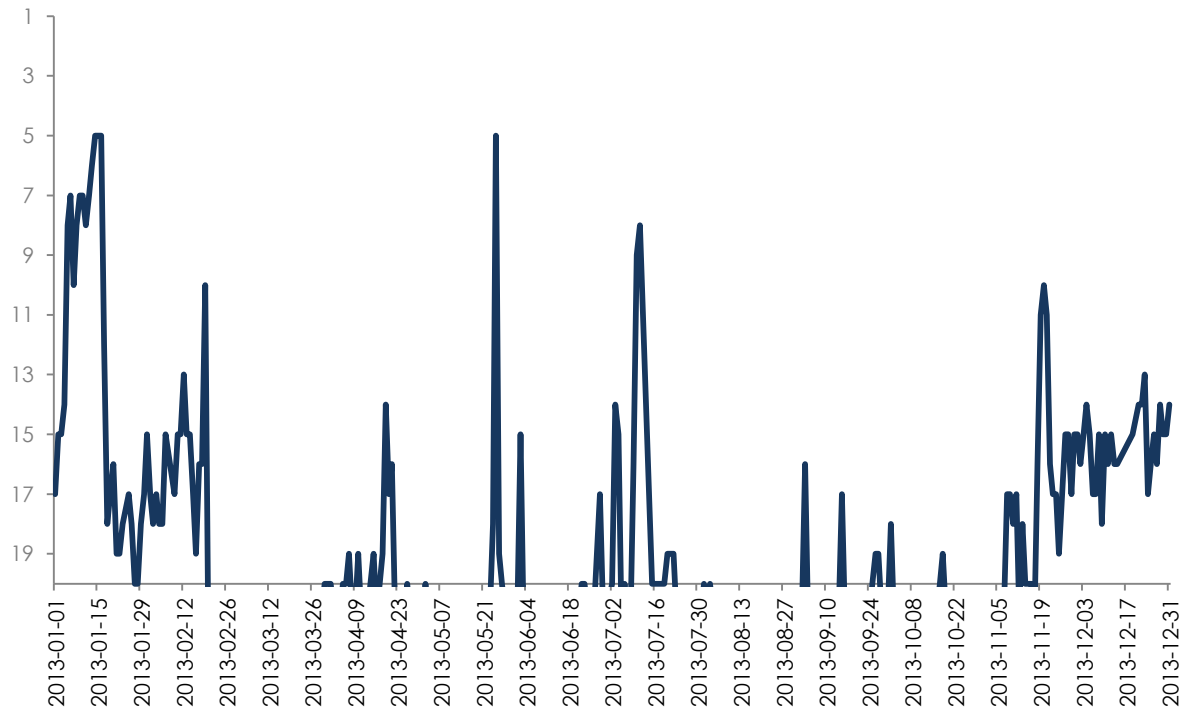
W celu minimalizacji zagrożeń typu botnet Zespół CERT.GOV.PL zalecał stosowanie tradycyjnych metod ochrony dla stacji klienckich, tzn. bieżącą aktualizację systemów operacyjnych, silników i definicji antywirusowych, zachowanie rozwagi przy otwieraniu niechcianej i podejrzanej poczty elektronicznej oraz stosowanie dodatkowych narzędzi wykorzystujących analizę behawioralną. Jednocześnie, zalecane było stosowanie w sieciach urządzeń typu firewall, IDS/IPS oraz mechanizmów typu blacklisting lub SRP[6]. Wskazane było również logowanie zdarzeń oraz odrzuconych pakietów z zapór sieciowych, co w znaczny sposób ułatwiało i przyśpieszało późniejszą analizę, mającą na celu identyfikację zainfekowanych hostów.

[6] SRP – Software Restriction Policies – mechanizm pozwalający na kontrolę nad aplikacjami uruchamianymi na systemach operacyjnych WindowsXP lub nowszych.

5.3. Informacje z systemu zewnętrznego Atlas

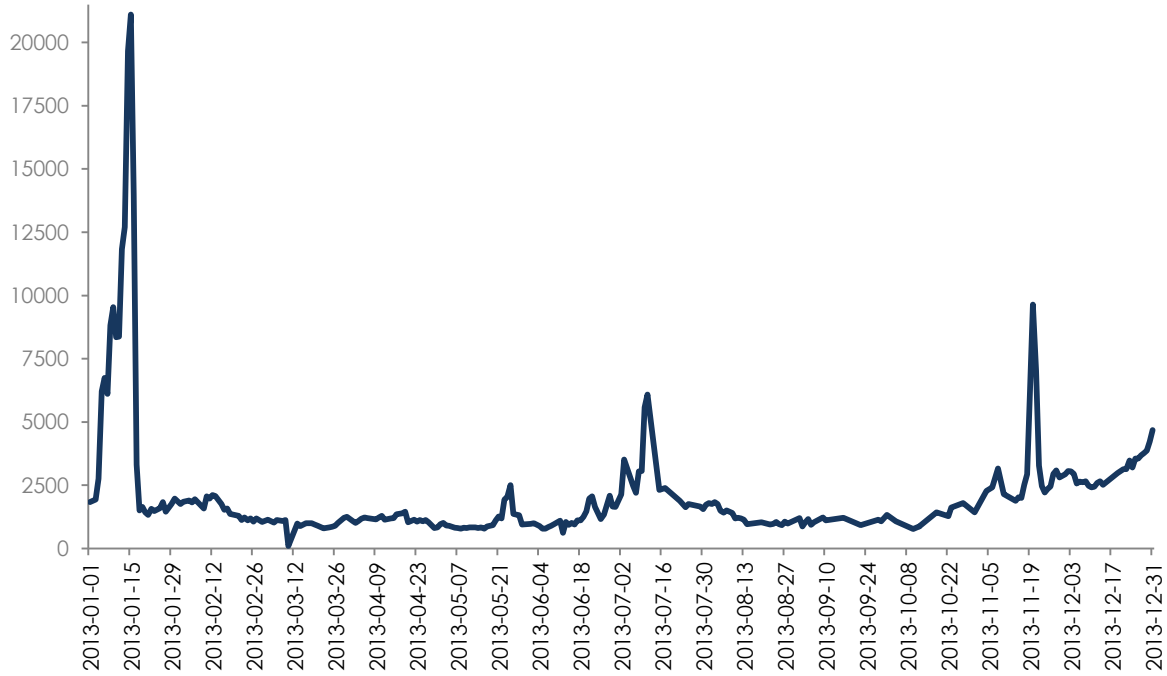
System ATLAS[7], prowadzony przez firmę ARBOR, gromadzi informacje na temat zagrożeń teleinformatycznych w sieci Internet i agreguje je pod względem m.in. klas adresowych poszczególnych państw oraz poszczególnych typów zagrożeń. Na podstawie powyższych danych tworzona jest klasyfikacja krajów pod względem ilości zagrożeń. Statystyka aktualizowana jest w cyklu dobowym na podstawie danych z ponad 270 sond rozmieszczonych u operatorów sieci Internet na świecie i przedstawia 20 krajów o największej liczbie zagrożeń.

Poniższe wykresy przedstawiają pozycję Polski w rankingach ATLAS w roku 2013.

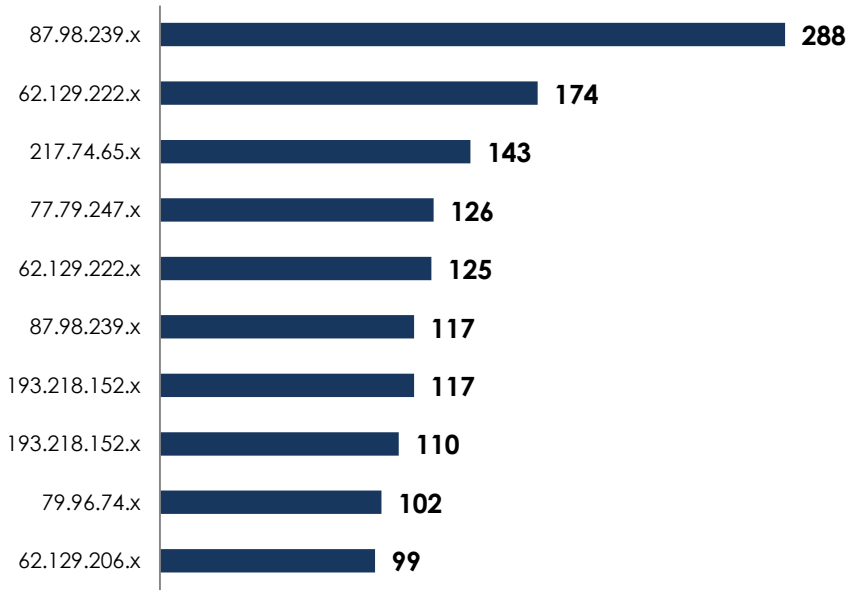


Rysunek 5-8: Pozycja Polski w rankingu Atlas

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

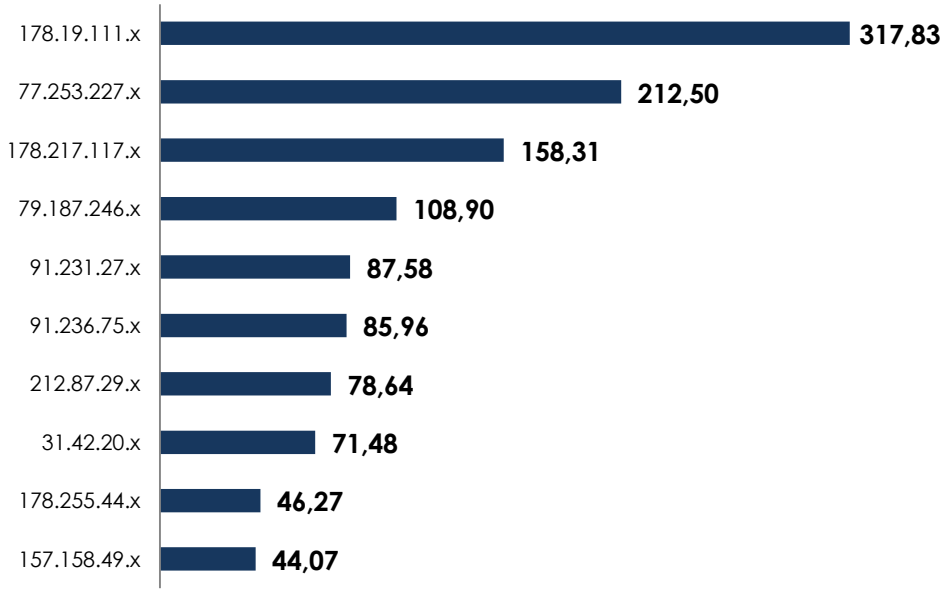


Rysunek 5-9: Liczba phishingowych adresów URL w Polsce wg systemu Atlas

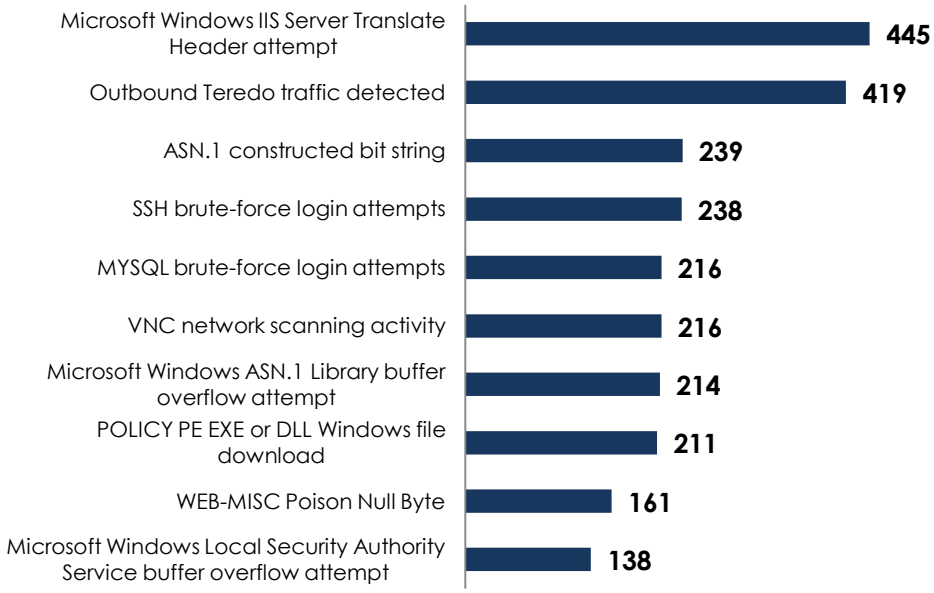


Rysunek 5-10: Statystyki phishingu w Polsce wg systemu Atlas (ilość wystąpień najbardziej aktywnych hostów lub ich sumy dla wystąpień w ramach jednej podsieci)

5.3.1. Statystyki ataków wg systemu Atlas

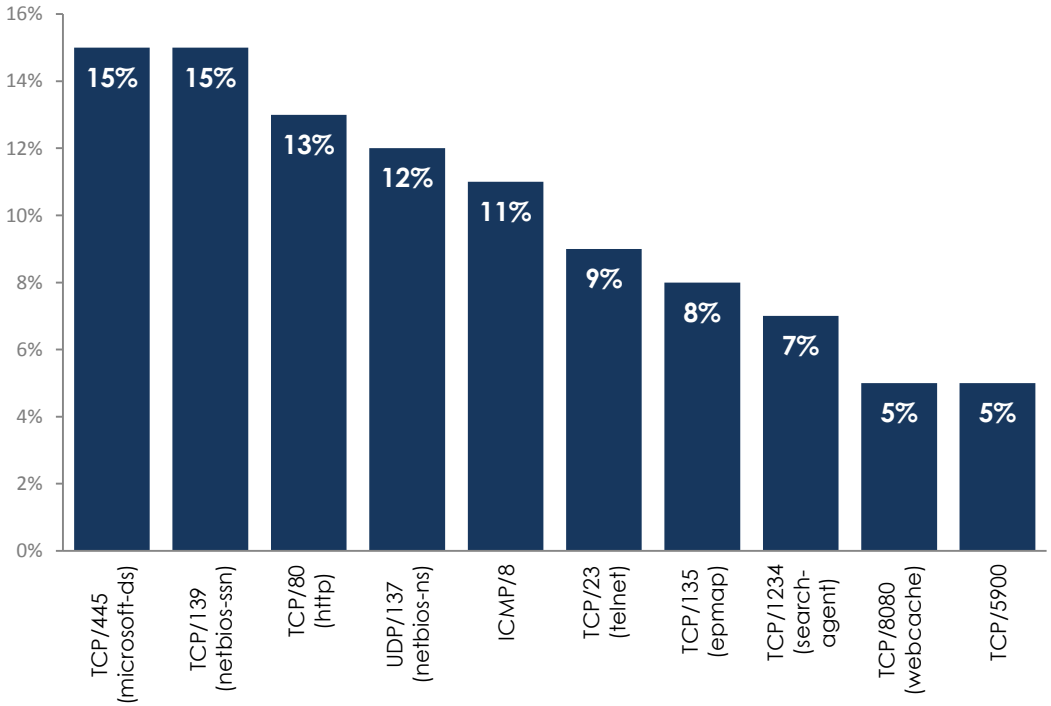


Rysunek 5-11: Najbardziej aktywne hosty w Polsce wg systemu Atlas (ilość wystąpień lub sumy dla hostów w jednej podsieci)

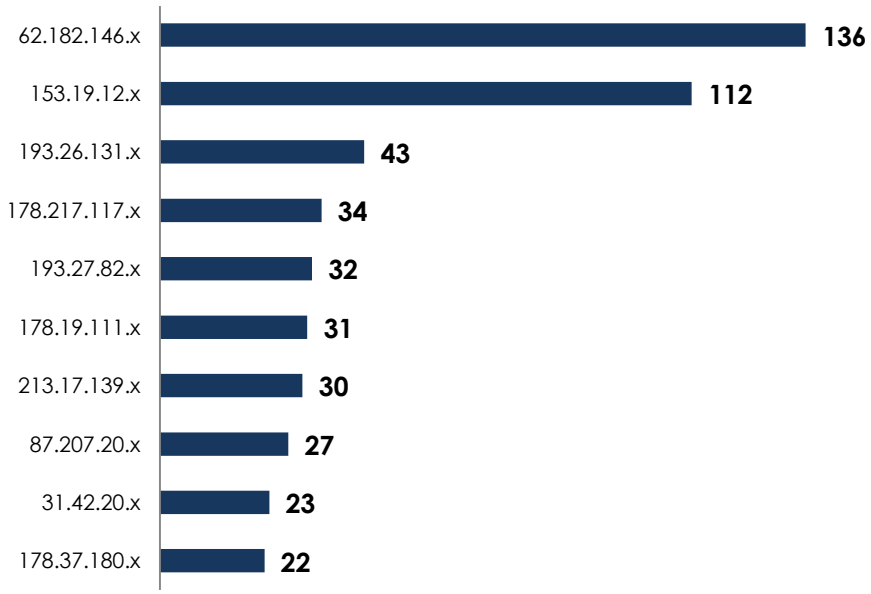


Rysunek 5-12: Dziesięć najczęściej występujących typów ataków w Polsce wg systemu Atlas (ilości wystąpień)

5.3.2. Statystyki skanowania wg systemu Atlas



Rysunek 5-13: Najczęściej skanowane porty/usługi w Polsce wg systemu Atlas (odnotowane ilości wystąpień)



Rysunek 5-14: Najbardziej aktywne hosty w Polsce wg systemu Atlas (ilość wystąpień lub ich sumy dla hostów w jednej podsieci)

Analizując powyższe wykresy można stwierdzić, iż pozycja Polski pod względem ilości zagrożeń dla bezpieczeństwa teleinformatycznego w całym 2013 roku, utrzymywała się na stosunkowo wysokim poziomie.

Statystyki systemu Atlas pokazują, że pozycja Polski pod względem głównych źródeł zagrożeń oscyluje zwykle w granicach 15 miejsca (na podstawie danych z ponad 270 sond rozmieszczonych u ISP na świecie). Spowodowane jest to m.in. dużą ilością phishingowych adresów URL oraz wysokim współczynnikiem ataków pochodzących z adresów IP, należących do polskiej przestrzeni adresowej.

Na uwagę zasługuje również fakt, że najczęściej występujące typy ataków w 2013 roku, to przede wszystkim ataki dotyczące usług Microsoft Windows Internet Information Services (IIS) Server Translate Header attempt oraz Outbound Teredo traffic.

W przypadku Microsoft Windows IIS Server Translate Header attempt, który w roku 2013 miał aż 18 procentowy udział w statystykach, atak polegał na wykorzystaniu żądania http zawierającego specjalnie spreparowane nagłówki, które mogły spowodować odmowę usługi dla niektórych serwerów IIS.

Atak Outbound Teredo traffic umożliwia natomiast ominięcie reguł zapory blokującej i w rezultacie uzyskanie informacji za pośrednictwem spreparowanego ruchu IPv6. W roku 2013 tego typu atak stanowił 17 procent całości sklasyfikowanych ataków.

6. Podsumowanie

Zwiększająca się liczba użytkowników sieci Internet, korzystająca z zaawansowanych technologii determinuje opracowywanie oraz wdrażanie nowych rozwiązań technicznych służących ochronie cyberprzestrzeni RP.

Atakujący stale zmieniają profil prowadzonych działań oraz wykorzystują nowe metody służące do przeprowadzania ataków, co implikuje konieczność zintensyfikowania prowadzonych działań w sferze organizacyjnej oraz technicznej.

W 2013 roku Zespół CERT.GOV.PL zarejestrował 5670 incydentów teleinformatycznych. Stosunkowo duża liczba incydentów obrazuje wysoki poziom zagrożenia dla bezpieczeństwa teleinformatycznego Polski, a jednocześnie wskazuje na zwiększającą się wykrywalność szkodliwych działań, ukierunkowanych na systemy teleinformatyczne w sektorze GOV.PL.

Wzrastająca liczba ataków na zasoby teleinformatyczne administracji publicznej dowodzi, iż konieczne jest kontynuowanie realizowanej przez Zespół CERT.GOV.PL działalności informacyjnej i szkoleniowej na rzecz administratorów i użytkowników istotnych systemów komputerowych.