CERT.GOV.PL

Raport o stanie bezpieczeństwa cyberprzestrzeni RP w 2016 roku

Warszawa, kwiecień 2017

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 występujące w obszarze administracji rządowej oraz infrastruktury krytycznej. Zespół CERT.GOV.PL funkcjonuje od 1 lutego 2008 roku w ramach Agencji Bezpieczeństwa Wewnętrznego. Jednym z jego podstawowych zadań jest rozpoznawanie, zapobieganie i wykrywanie zagrożeń godzących w bezpieczeństwo, istotnych z punktu widzenia ciągłości funkcjonowania państwa systemów teleinformatycznych organów administracji publicznej lub systemu sieci teleinformatycznych objętych jednolitym wykazem obiektów, instalacji, urządzeń i usług wchodzących w skład infrastruktury krytycznej, a także systemów teleinformatycznych właścicieli i posiadaczy obiektów, instalacji lub urządzeń infrastruktury krytycznej, o których mowa w art. 5b ust. 7 pkt 1 ustawy z dnia 26 kwietnia 2007 r. o zarządzaniu kryzysowym.

CERT.GOV.PL

dane kontaktowe

Agencja Bezpieczeństwa Wewnętrznego
ul. Rakowiecka 2a
00-993 Warszawa

www.cert.gov.pl
cert@cert.gov.pl
zgłaszanie incydentów: incydent@cert.gov.pl
tel: +48 22 58 59 373
faks: +48 22 58 58 833

Spis treści

Wstęp

Raport o stanie bezpieczeństwa cyberprzestrzeni RP publikowany przez Zespół CERT.GOV.PL zawiera informacje i dane statystyczne, które mają dostarczyć wiedzy niezbędnej dla procesów podnoszenia bezpieczeństwa systemów teleinformatycznych. Publikowany jest również w celu podnoszenia świadomości użytkowników o zagrożeniach i podatnościach. W 2016 roku Zespół CERT.GOV.PL łącznie zarejestrował 19 954 zgłoszenia, z których aż 9 288 zostało zakwalifikowanych jako faktyczne incydenty. Wzrost wyżej wymienionych statystyk jest odnotowywany corocznie: w 2015 roku zostały zarejestrowane 16 123 zgłoszenia, z czego 8 914 zostało zakwalifikowanych jako faktyczne incydenty.

W odniesieniu do kwestii źródeł zgłoszeń incydentów to podobnie jak w 2015 roku informacje o anomaliach występujących w systemach są w zdecydowanej większości dystrybuowane przez Zespół CERT.GOV.PL do instytucji. W tym kontekście ważnym wskaźnikiem jest również fakt, iż zgłoszenia ze strony instytucji do Zespołu CERT.GOV.PL w dalszym ciągu stanowią niewielki odsetek całości przedmiotowej komunikacji.

W 2016 roku wzrosła liczba incydentów w kategorii *Błędna Konfiguracja Urządzenia* (4 158 incydentów), co sprawiło, iż stanowi ona najliczniejszą kategorię w przedmiotowym okresie. Drugą najczęściej odnotowywaną kategorią incydentów w 2016 roku był *Klient Botnet* pomimo, iż w porównaniu z 2015 rokiem odnotowano znaczny spadek liczby (4 284 w 2015 roku, 2 836 w 2016 roku). Istotnym zauważalnym trendem jest rokroczny wzrost liczby incydentów w kategorii *Inżynieria Społeczna*. W 2015 roku odnotowano 257 incydentów tego typu, natomiast w 2016 roku liczba ta wzrosła do 382. Wskazana tendencja wzrostowa jest zauważalna na przestrzeni kilku ostatnich lat, co w sposób szczególny jest poddawane analizom w Zespole CERT.GOV.PL w związku z faktem, iż omawiana aktywność jest kierowana do instytucji administracji państwowej oraz operatorów infrastruktury krytycznej.

Również należy pochylić się nad liczbą wygenerowanych przez system ARAKIS 2.0 GOV alarmów, które są tworzone na podstawie danych z sieci teleinformatycznych podmiotów uczestniczących w projekcie. 2016 rok był pierwszym pełnym kalendarzowym rokiem, w którym w pełni funkcjonalności działał przedmiotowy system. Przełożyło się to na zanotowanych łącznie 338 430 181 przepływów, co wygenerowało 446 915 alarmów. Dla porównania należy wskazać, iż w 2015 roku system ARAKIS-GOV wygenerował 36 815 alarmów. Jak widać skala w obu przypadkach jest nieporównywalna.

Zespół CERT.GOV.PL obserwuje również od kilku lat wzrost liczby ataków ukierunkowanych, które bardzo często są atakami składającymi się z kilku różnych metod i technik mających na celu wieloetapową ingerencję w stacje robocze oraz

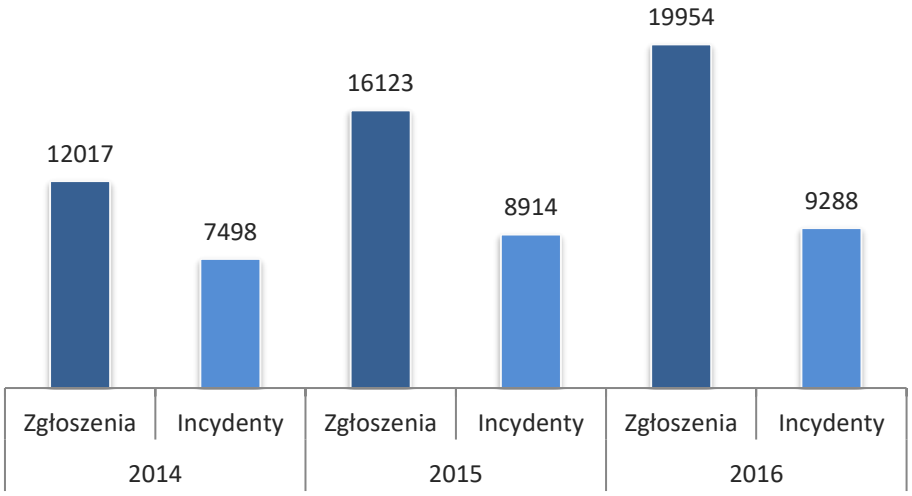
systemy teleinformatyczne. Bardzo często początkiem dla potencjalnego sukcesu omawianych kampanii stają się braki w podstawowych zasadach bezpieczeństwa jak np. brak cyklicznych aktualizacji systemów jak również często brak wiedzy lub podstawowej higieny użytkowania stacji roboczych i poruszania się po sieci Internet. W odniesieniu do tego problemu kluczowe nadal są takie kwestie jak prowadzenie przez instytucje szkoleń dla nowo przyjmowanych pracowników oraz szkoleń prowadzonych cyklicznie dla całej kadry jak również przeprowadzanie testów bezpieczeństwa nowych systemów. Mimo intensywnych działań podejmowanych przez Zespół CERT.GOV.PL mających na celu wyeliminowanie wyżej wskazanych braków m.in. prowadzenie dedykowanych szkoleń, wydawanie rekomendacji czy rozsyłanie do instytucji ostrzeżeń, należy zaznaczyć, iż najwięcej działań, które należy podjąć pozostaje po stronie samych zainteresowanych podmiotów.

1. STATYSTYKI INCYDENTÓW KOORDYNOWANYCH PRZEZ ZESPÓŁ CERT.GOV.PL

W 2016 roku Rządowy Zespół Reagowania na Incydenty Komputerowe CERT.GOV.PL w związku z realizacją nałożonych zadań odnotował aż 19 954 zgłoszenia o potencjalnym wystąpieniu incydentu komputerowego w sieciach znajdujących się w obszarze kompetencyjnym Zespołu. To stanowi znaczący wzrost względem 2015 roku, w którym takich zgłoszeń zarejestrowano 16 123. Przedmiotowe zgłoszenia poddawane są weryfikacji, w której określone zostaje czy uzyskana informacja nosi znamiona faktycznego incydentu komputerowego czy też jest tzw. *false positive*. Kolejną przyczyną powodującą różnice wartości przedmiotowych danych są wielokrotne zgłoszenia dotyczące tych samych incydentów. Są one szczególnie wyraźne w przypadku korzystania z systemów automatycznych. Zgłoszenia pochodzące z systemów automatycznych jak np. N6[1], zostają również poddawane weryfikacji przez Zespół CERT.GOV.PL.

W związku z tak prowadzonymi wstępnymi analizami w 2016 roku ustalono, iż ze zgłoszonych 19 954 incydentów faktyczne naruszenie bezpieczeństwa teleinformatycznego instytucji miało miejsce w 9 288 przypadkach, co również stanowi wzrost względem 2015 roku, w którym faktycznych incydentów odnotowano 8 914.

Poniższy wykres zestawia powyższe dane w ujęciu lat 2014, 2015 oraz 2016.

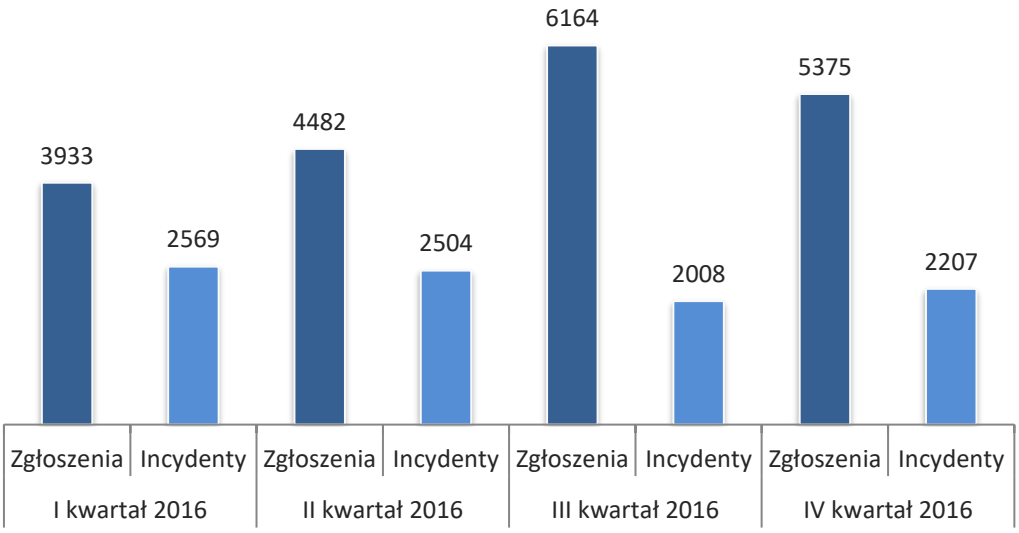


Wykres 1 Liczba zarejestrowanych zgłoszeń oraz incydentów w poszczególnych latach

Jak można odnotować na powyższym wykresie tendencja jest stale rosnąca. Na taki stan rzeczy wpływa wiele czynników. Należy wymienić m.in. fakt coraz szerszego zainteresowania potencjalnych atakujących m.in. sieciami rządowymi w Polsce. Inną istotną kwestią jest również ciągły rozwój wykorzystywanych przez Zespół CERT.GOV.PL systemów, które dzięki prowadzonym pracom stają się coraz

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

precyzyjniejsze w monitorowaniu sieci oraz w określaniu faktycznych zagrożeń dla systemów i sieci komputerowych.



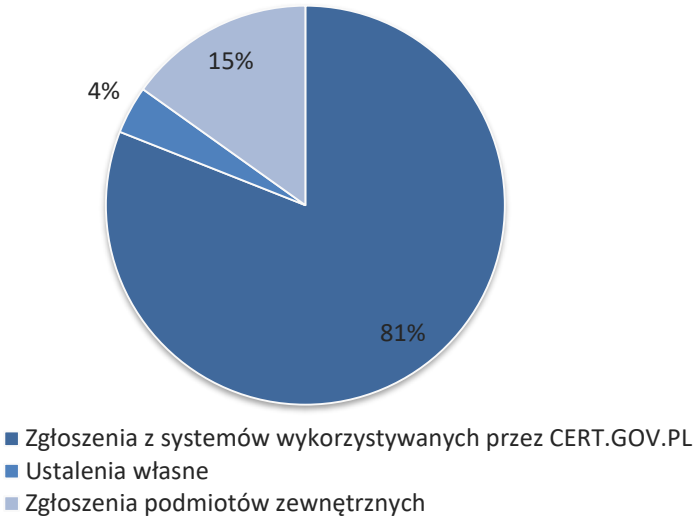
Wykres 2 Liczba zarejestrowanych zgłoszeń oraz incydentów w poszczególnych kwartałach 2016 roku

Powyższy wykres ukazuje rozkład kwartalny zarejestrowanych zgłoszeń oraz faktycznych incydentów bezpieczeństwa w 2016 roku. Warto zauważyć, iż III kwartał wyróżnia się znaczącą liczbą zgłoszeń zarejestrowanych przez Zespół CERT.GOV.PL. Jest to sytuacja o tyle ciekawa, iż w poprzednich latach zazwyczaj wskazany kwartał charakteryzował się stosunkowo niską liczbą zgłoszeń w porównaniu do pozostałych okresów w roku. Wynikało to głównie z faktu, iż w przedmiotowym kwartale znajdują się dwa miesiące wakacyjne powodowało zwykle mniejszą aktywność użytkowników sieci i systemów komputerowych.

Wydaje się, iż jednym z i jednocześnie najbardziej znaczącym powodem zaistniałej w 2016 roku sytuacji był fakt organizowania w Polsce dwóch wydarzeń o znaczeniu międzynarodowym, które jednocześnie potencjalnie mogły generować możliwość wystąpienia większej niż zazwyczaj aktywności cyberprzestępców w sieci. W lipcu 2016 roku w Warszawie odbywał się Szczyt Sojuszu Północnoatlantyckiego NATO natomiast zaraz po tym wydarzeniu miały miejsce Światowe Dni Młodzieży. Jednoczesne wzmożenie aktywności przestępców jak również zwiększona czujność użytkowników mogły w znaczący sposób wpłynąć na większą niż zwykle liczbę zarejestrowanych zgłoszeń o potencjalnych incydentach bezpieczeństwa. We wskazanym zestawieniu warto jednocześnie zauważyć, iż przy najwyższej liczbie zgłoszeń wystąpiła jednocześnie najniższa liczba faktycznych incydentów.

W odniesieniu do powyższych danych należy również zwrócić uwagę na źródła, z których Zespół CERT.GOV.PL czerpie informacje o zaistniałych bądź potencjalnych incydentach bezpieczeństwa teleinformatycznego. W tym kontekście należy zaznaczyć,

iż większość agregowanych informacji pozyskiwanych jest z wykorzystywanych przez Zespół CERT.GOV.PL systemów (aż 81% wszystkich). 4% to tzw. ustalenia własne wynikające z innych działań podejmowanych przez członków Zespołu, a 15% to zgłoszenia od podmiotów zewnętrznych. Obrazuje to poniższy wykres.

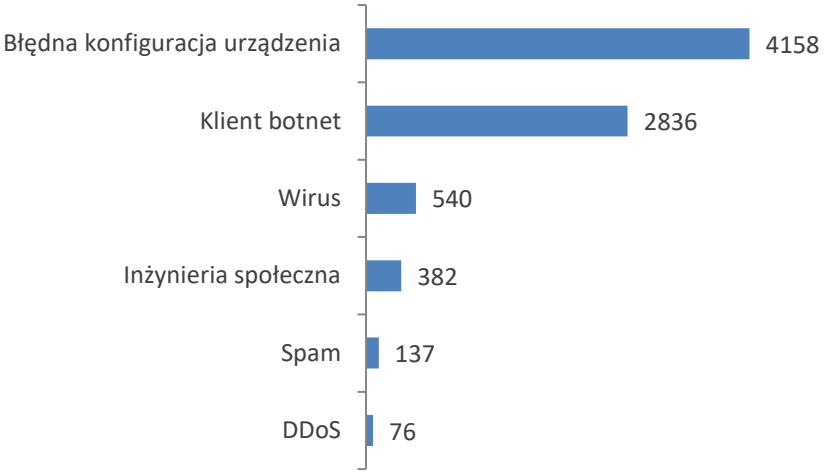


Wykres 3 Źródła zgłoszeń do Zespołu CERT.GOV.PL

Kolejnym istotnym zagadnieniem jest rodzaj odnotowywanych kategorii incydentów. Rokrocznie podobny typ incydentów odnotowywany jest najczęściej. W 2016 roku najczęściej występującą kategorią incydentów jest tzw. *Błędna Konfiguracja Urządzenia*. W tej kategorii odnotowano aż 4 158 incydentów (w latach 2014 oraz 2015 ta kategoria plasowała się na drugim miejscu pod względem liczby incydentów). Należy podkreślić, iż ten rodzaj zagrożenia bezpieczeństwa, choć nie wynika z ingerencji zewnętrznej w system, to w wielu przypadkach może stanowić furtkę do przeprowadzenia skutecznego ataku.

Drugą najczęściej występującą kategorią był tzw. *Klient Botnet*. Wskazana kategoria uzyskała wynik 2 836 incydentów (w latach 2014 oraz 2015 *Klient Botnet* osiągał pierwsze miejsce pod względem liczby zarejestrowanych incydentów). Ta kategoria oznacza w głównej mierze, iż urządzenia teleinformatyczne wykorzystywane w systemach zostały zainfekowane i prowadzą komunikację z tzw. serwerami *Command & Control.* Ta komunikacja może oznaczać, iż z poziomu wskazanych serwerów można zdalnie zarządzać niektórymi (wybranymi) funkcjonalnościami stacji zainfekowanej. To w dalszej kolejność oznacza, iż dane urządzenie należy do określonej sieci botnet.

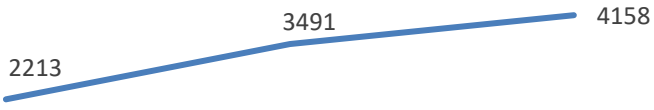
Poniższy wykres przedstawia rozkład liczbowy wybranych incydentów odnotowanych przez CERT.GOV.PL.



Wykres 4 Liczba wybranych incydentów w 2016 roku z podziałem na kategorie

Istotnym zauważalnym trendem jest coroczny wzrost liczby incydentów z kategorii *Inżynieria Społeczna*. W 2015 roku odnotowano 257 incydentów tego typu by w 2016 ta liczba wzrosła do 382. Zmiana ta jest o tyle istotna, iż kampanie phishingowe, które zawierają się w opisywanej kategorii mogą stanowić fazę inicjującą rozleglejszego ataku niekiedy dedykowanego jakiejś konkretnej instytucji lub grupie instytucji. Może być również fazą wstępną do ataku typu Advanced Persistent Threat (APT).

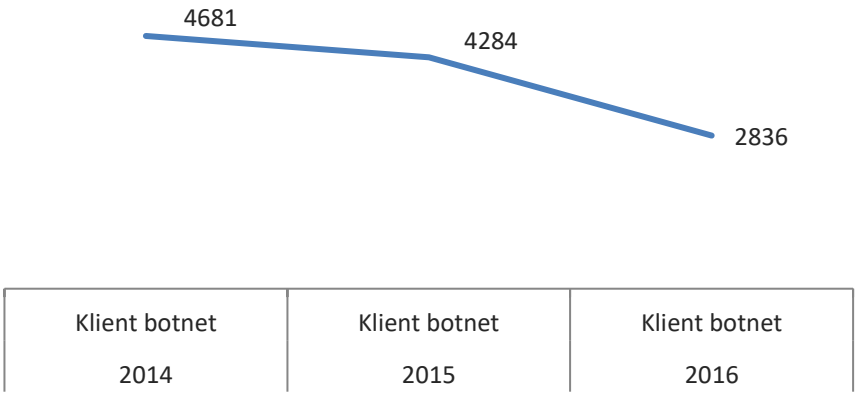
W kontekście powyższych informacji należy również zwrócić uwagę na przedmiotowe kategorie incydentów bezpieczeństwa w ujęciu trendów obserwowanych w ostatnich latach. Poniżej przedstawiono wykresy, które ukazują trendy w latach 2014, 2015 oraz 2016 w odniesieniu do kategorii: *Błędna Konfiguracja Urządzenia, Klient Botnet oraz Inżynieria Społeczna.*



Błędna konfiguracja urządzenia	Błędna konfiguracja urządzenia	Błędna konfiguracja urządzenia
2014	2015	2016

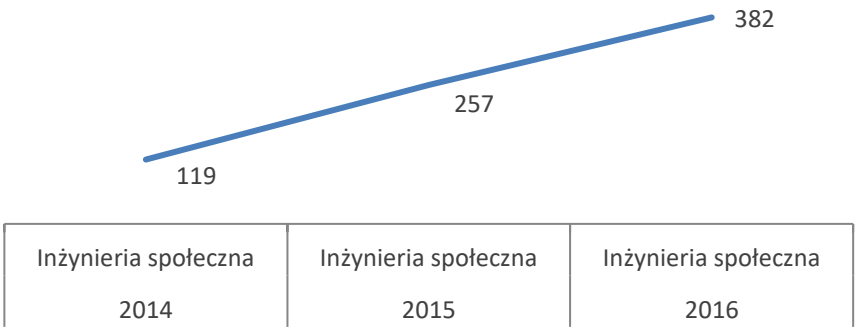
Wykres 5 Liczba zarejestrowanych incydentów w kategorii *Błędna Konfiguracja Urządzenia* w latach 2014 - 2016

Jak można zauważyć na powyższym wykresie, liczba wykrywanych błędów w konfiguracji urządzeń każdego roku rośnie. Może wynikać to z dwóch głównych powodów. Po pierwsze z coraz częściej wynajdowanych błędów na urządzeniach i wydawania coraz większej ilości zaleceń konfiguracyjnych, których administratorzy nie wprowadzają do administrowanych systemów. Tak znacząca liczba może również wynikać z braku aktualizacji w konfiguracji systemów w odniesieniu do informacji sygnalizowanych w poprzednich latach.



Wykres 6 Liczba zarejestrowanych incydentów w kategorii *Klient Botnet* w latach 2014 - 2016

Na powyższym wykresie widać utrzymującą się wyraźną tendencję spadkową w kategorii *Klient Botnet*. Taki stan rzeczy wynika m.in. z działań prowadzonych na całym świecie, które skierowane są przeciwko systemom kierującym grupami zarażonych komputerów, czyli tzw. serwerami C&C.



Wykres 7 Liczba zarejestrowanych incydentów w kategorii Inżynieria Społeczna w latach 2014 - 2016

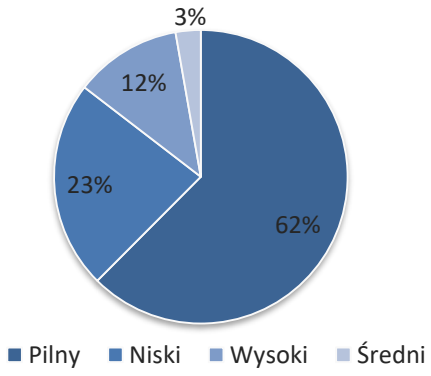
Jak wspomniano we wcześniejszej części raportu, tendencja wzrostowa jest zauważalna w przedmiotowej kategorii dosyć wyraźnie. Ten trend w sposób znaczący podlega analizie Zespołu CERT.GOV.PL. Wynika to m.in. z faktu, iż jak podają niektóre źródła aż 90% wszystkich skutecznych ataków teleinformatycznych inicjowanych jest poprzez atak typu phishing wykorzystujący inżynierię społeczną jako podstawę swojej skuteczności.

2. ANALIZA ALARMÓW NA PODSTAWIE SYSTEMU ARAKIS 2.0 GOV

System ARAKIS 2.0 GOV to dedykowany, rozproszony system wczesnego ostrzegania o zagrożeniach teleinformatycznych występujących na styku sieci wewnętrznej z siecią Internet. Głównym zadaniem systemu jest wykrywanie i zautomatyzowane opisywanie zagrożeń występujących w sieciach teleinformatycznych na podstawie agregacji, analizy i korelacji danych z różnych źródeł.

W 2016 roku w sieciach teleinformatycznych podmiotów uczestniczących w projekcie ARAKIS 2.0 GOV zanotowano łącznie 338 430 181 przepływów, co przełożyło się na 446 915 wygenerowanych przez system alarmów[2]. Wśród zanotowanych alarmów:

- 279 181 alarmów miało priorytet pilny tzn. wymagało natychmiastowej reakcji na zagrożenie ze strony administratorów, niosło duże ryzyko przełamania zabezpieczeń;
- 52 766 alarmów miało priorytet wysoki tzn. wymagało wzmożonej uwagi w kontekście zagrożenia wskazanego w alarmie, niosło średnie ryzyko przełamania zabezpieczeń;
- 12 365 alarmów miało priorytet średni tzn. były to alarmy informujące o dobrze znanym zagrożeniu, które niosły małe ryzyko przełamania zabezpieczeń;
- 102 603 alarmów miało priorytet niski tzn. były to alarmy czysto informacyjne dot. aktualnej sytuacji na styku sieci wewnętrznej z siecią Internet.

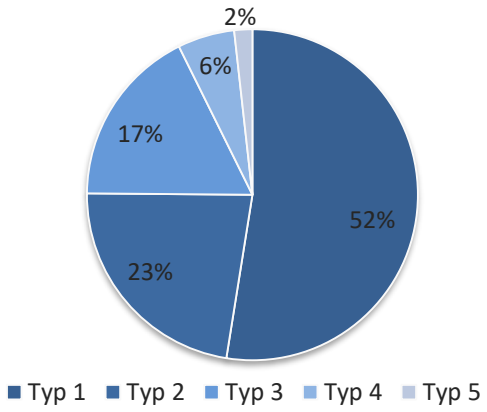


Wykres 8 Procentowy rozkład alarmów

[2] Pojedynczy alarm może składać się z wielu przepływów.

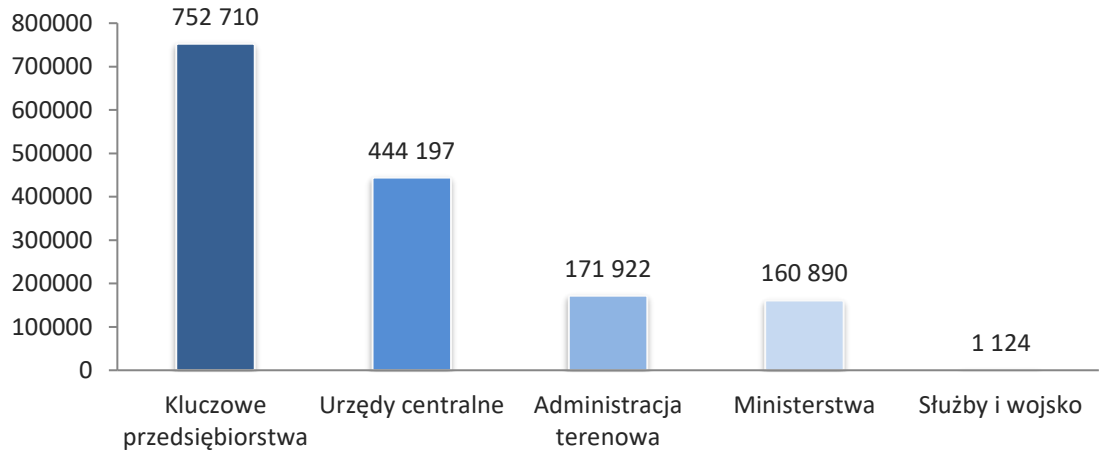
Każdy z zanotowanych alarmów posiada dokładne dane techniczne, pozwalające na jego weryfikację oraz jest szczegółowo klasyfikowany przez system. W ramach klasyfikacji każdy alarm może zostać przypisany do jednego z pięciu podstawowych typów:

- Typ 1 – komunikacja do złośliwych adresów;
- Typ 2 – skanowania;
- Typ 3 – wykryte znane ataki;
- Typ 4 – wykryte nieopisane ataki;
- Typ 5 – infekcje wewnętrzne.



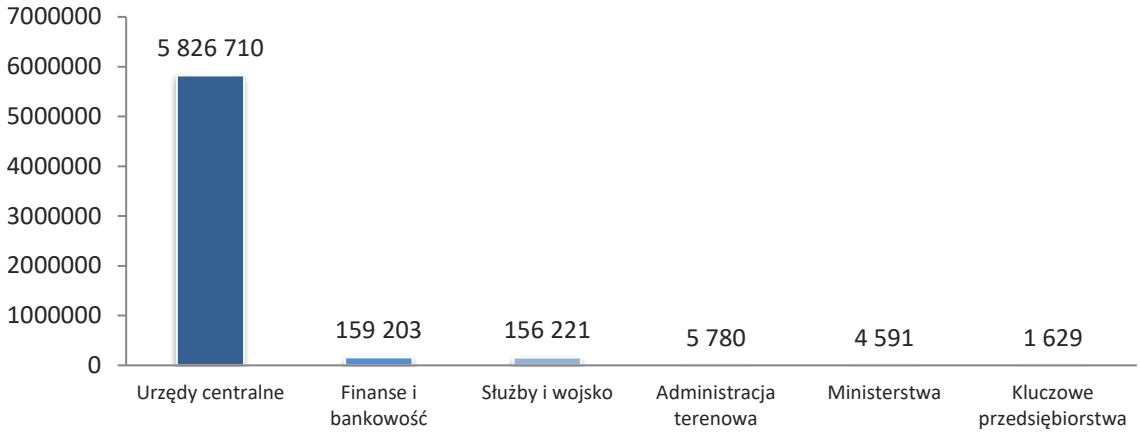
Wykres 9 Procentowy podział alarmów ze względu na typ

Wśród alarmów typu 1 najwięcej przepływów zostało zanotowanych w instytucjach skategoryzowanych jako „Kluczowe przedsiębiorstwa” (49%) oraz „Urzędy centralne” (29%), co może wynikać bezpośrednio z ilości generowanego przez podmioty ruchu sieciowego.



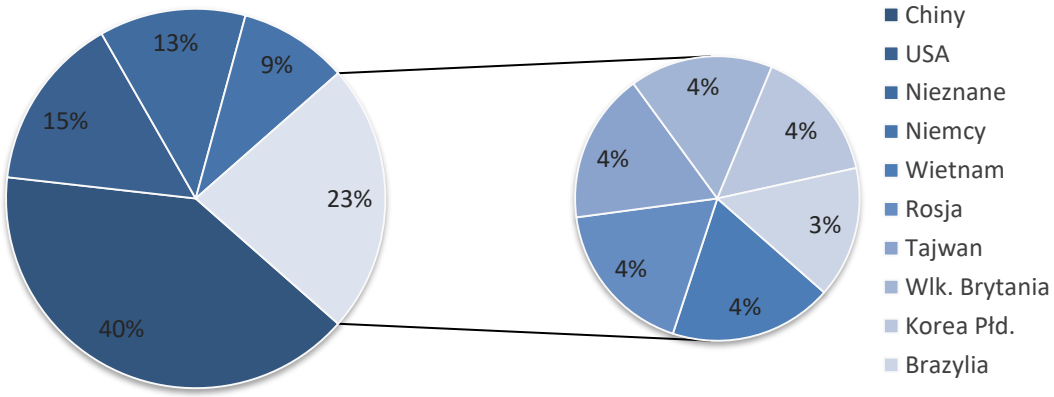
Wykres 10 Liczba przepływów alarmów Typu 1 w instytucjach

Wśród alarmów typu 5 najwięcej przepływów zostało zanotowanych w instytucjach skategoryzowanych jako „Urzędy centralne” (95%), co wprost wynika z ilości posiadanych urządzeń końcowych.



Wykres 11 Liczba przepływów alarmów Typu 5 w instytucjach

Do najbardziej aktywnych krajów pod kątem liczby generowanych przepływów należą Chiny (40% przepływów) oraz Stany Zjednoczone (15% przepływów). Należy zwrócić uwagę na duży stosunek przepływów pochodzących z adresów aktualnie nieprzypisanych do żadnego z krajów bądź podmiotów (nieznane – 13%).



Wykres 12 Procentowy rozkład źródeł ataków na sieci monitorowane przez system ARAKIS 2.0 GOV pod kątem liczby generowanych przepływów

Biorąc pod uwagę specyfikę sieci Internet (tzw. „brak granic”), infrastruktura teleinformatyczna podmiotów generujących przepływy w stronę systemu ARAKIS 2.0 GOV może być rozproszona oraz zlokalizowana na terytorium dowolnych państw na całym świecie. W związku z powyższym zaprezentowaną powyżej statystykę należy traktować jedynie w kategoriach podglądowych.

W tabeli poniżej zaprezentowano informację o portach docelowych, na które wygenerowano największą ilość przepływów celem identyfikacji istniejących zasobów teleinformatycznych bądź próby ich eksploitacji.

L.p.	Docelowy port/protokół	Ilość przepływów	Opis
1	23/TCP	55 253 404	Ataki na usługę telnet
2	22/TCP	46 361 141	Ataki na usługę SSH
3	8080/TCP	32 150 584	Skanowania w poszukiwaniu serwerów open web proxy
4	80/TCP	22 828 571	Ataki na aplikacje webowe
5	5060/UDP	11 822 266	Ataki na usługę SIP VoIP
6	1433/TCP	8 819 387	Ataki na bazę danych MSSQL
7	445/TCP	6 940 390	Ataki na usługę Windows SMB
8	53413/UDP	6 641 750	Próby wykorzystania backdoora w routerach Netis
9	3306/TCP	5 735 154	Ataki na bazę danych MySQL
10	2323/TCP	4 553 231	Ataki na usługę telnet

Tabela 1 Zidentyfikowane w 2016 roku skanowania i próby eksploitacji usług na podstawie danych z systemu ARAKIS 2.0 GOV

Od kilku lat niezmiennie najczęściej atakowanymi usługami są usługi zapewniające zdalny dostęp do danego zasobu teleinformatycznego (SSH, telnet). Najczęstszym scenariuszem próby przełamania zabezpieczeń w tym przypadku są ataki słownikowe (brute-force). Duża ilość przepływów w roku 2016 odnotowana na portach 23/TCP i 2323/TCP jest częściowo powiązana z aktywnością botnetu Mirai (skanowanie w poszukiwaniu urządzeń IoT).

W roku 2016 zidentyfikowano 17 411 979 dopasowań reguł SNORT do obserwowanego ruchu sieciowego. Przedmiotowe dopasowania mają odzwierciedlenie m.in. w ruchu zaprezentowanym w poprzedniej tabeli na poszczególne porty docelowe– najczęściej wykrywane są reguły dotyczące prób nieuprawnionego wykorzystania usług SSH, SIP VoIP oraz ataków na usługi webowe.

L.p.	Ilość przepływów	Reguła SNORT
1	5 772 866	ET SCAN Potential SSH Scan OUTBOUND
2	3 216 099	ET SCAN SSH BruteForce Tool with fake PUTTY version
3	2 194 889	ET SCAN Sipvicious User-Agent Detected (friendly-scanner)
4	1 841 602	ET SCAN Potential SSH Scan
5	1 031 067	ET SCAN Sipvicious Scan
6	569 010	GPL NETBIOS SMB-DS IPC$ unicode share access
7	315 675	ET WEB_SERVER WGET Command Specifying Output in HTTP Headers
8	281 776	ET SCAN SipCLI VOIP Scan
9	263 811	ET SCAN LibSSH Based Frequent SSH Connections Likely BruteForce Attack
10	214 820	ET WEB_SERVER CURL Command Specifying Output in HTTP Headers

Tabela 2 Najczęściej dopasowane reguły do ruchu sieciowego widzianego przez system ARAKIS 2.0 GOV

3. REGULACJE PRAWNE DOT. ZADAŃ ZESPOŁU CERT.GOV.PL

3.1. Rejestr zdarzeń naruszających bezpieczeństwo systemów teleinformatycznych

Wprowadzenie w życie przepisów Ustawy z dnia 10 czerwca 2016 r. *o działaniach antyterrorystycznych* oraz art. 32d. *ustawy o Agencji Bezpieczeństwa Wewnętrznego oraz Agencji Wywiadu*, nałożyło na Szefa ABW obowiązek prowadzenia rejestru zdarzeń naruszających bezpieczeństwo systemów teleinformatycznych, o których mowa w art. 5 ust. 1 pkt 2a *ustawy o ABW oraz AW*.
Zgodnie z powyższym, w przypadku odnotowania zdarzenia naruszającego bezpieczeństwo wskazanych systemów, ich administratorzy zobligowani są do niezwłocznego zgłaszania przypadków infekcji do Rządowego Zespołu Reagowania na Incydenty Komputerowe, który jest właściwy ze strony Agencji Bezpieczeństwa Wewnętrznego w obszarze obsługi przedmiotowych zdarzeń. Można to zrobić wysyłając zgłoszenie bezpośrednio na adres mailowy incydent@cert.gov.pl lub zgłaszając telefonicznie pod nr tel. 22 58 59 373. W celu uproszczenia zgłaszania zdarzeń, na witrynie internetowej Rządowego Zespołu Reagowania na Incydenty Komputerowe CERT.GOV.PL w zakładce "zgłaszanie incydentu" opublikowany jest aktualnie obowiązujący formularz, który po wypełnieniu należy przesłać na adres e-mail: incydent@cert.gov.pl.

3.2. Stopnie alarmowe

Ustawa z dnia 10 czerwca 2016 r. *o działaniach antyterrorystycznych*[3] wraz z Rozporządzeniem Prezesa Rady Ministrów z dnia 25 lipca 2016 *r. w sprawie zakresu przedsięwzięć wykonywanych w poszczególnych stopniach alarmowych i stopniach alarmowych CRP* wprowadziły nowe zadania do realizacji przez jednostki związanie z wprowadzeniem stopni alarmowych CRP. Obecnie, w przypadku zagrożenia wystąpienia zdarzenia o charakterze terrorystycznym dotyczącego systemów teleinformatycznych organów administracji publicznej lub systemów teleinformatycznych wchodzących w skład infrastruktury krytycznej albo w przypadku wystąpienia takiego zdarzenia można wprowadzić jeden z czterech stopni alarmowych CRP:

1) pierwszy stopień alarmowy CRP (stopień ALFA-CRP);
2) drugi stopień alarmowy CRP (stopień BRAVO-CRP);
3) trzeci stopień alarmowy CRP (stopień CHARLIE-CRP);
4) czwarty stopień alarmowy CRP (stopień DELTA-CRP).

Przedsięwzięcia wykonywane w ramach kompetencji ustawowych przez organy administracji publicznej oraz kierowników służb i instytucji właściwych w sprawach bezpieczeństwa i zarządzania kryzysowego w stopniach alarmowych CRP:

[3] Dz. U. 2016 poz. 904

1. Po wprowadzeniu **pierwszego stopnia alarmowego CRP (stopień ALFA-CRP)** należy wykonać w szczególności następujące zadania:

1) wprowadzić wzmożone monitorowanie stanu bezpieczeństwa systemów teleinformatycznych organów administracji publicznej lub systemów teleinformatycznych wchodzących w skład infrastruktury krytycznej, zwanych dalej "systemami", w szczególności wykorzystując zalecenia Szefa Agencji Bezpieczeństwa Wewnętrznego lub komórek odpowiedzialnych za system reagowania zgodnie z właściwością, oraz:
   a) monitorować i weryfikować, czy nie doszło do naruszenia bezpieczeństwa komunikacji elektronicznej,
   b) sprawdzać dostępność usług elektronicznych,
   c) dokonywać, w razie potrzeby, zmian w dostępie do systemów;
2) poinformować personel instytucji o konieczności zachowania zwiększonej czujności w stosunku do stanów odbiegających od normy, w szczególności personel odpowiedzialny za bezpieczeństwo systemów;
3) sprawdzić kanały łączności z innymi, właściwymi dla rodzaju stopnia alarmowego CRP, podmiotami biorącymi udział w reagowaniu kryzysowym, dokonać weryfikacji ustanowionych punktów kontaktowych z zespołami reagowania na incydenty bezpieczeństwa teleinformatycznego właściwymi dla rodzaju działania organizacji oraz ministrem właściwym do spraw informatyzacji;
4) dokonać przeglądu stosownych procedur oraz zadań związanych z wprowadzeniem stopni alarmowych CRP, w szczególności dokonać weryfikacji posiadanej kopii zapasowej systemów w stosunku do systemów teleinformatycznych wchodzących w skład infrastruktury krytycznej oraz systemów kluczowych dla funkcjonowania organizacji, oraz weryfikacji czasu wymaganego na przywrócenie poprawności funkcjonowania systemu;
5) sprawdzić aktualny stan bezpieczeństwa systemów i ocenić wpływ zagrożenia na bezpieczeństwo teleinformatyczne na podstawie bieżących informacji i prognoz wydarzeń;
6) informować na bieżąco o efektach przeprowadzanych działań zespoły reagowania na incydenty bezpieczeństwa teleinformatycznego właściwe dla rodzaju działania organizacji oraz współdziałające centra zarządzania kryzysowego, a także ministra właściwego do spraw informatyzacji.

2. Po wprowadzeniu **drugiego stopnia alarmowego CRP (stopień BRAVO-CRP)** należy wykonać zadania wymienione dla pierwszego stopnia alarmowego CRP oraz kontynuować lub sprawdzić wykonanie tych zadań, jeżeli wcześniej był wprowadzony stopień ALFA-CRP. Ponadto należy:

1) zapewnić dostępność w trybie alarmowym personelu odpowiedzialnego za bezpieczeństwo systemów;

2) wprowadzić całodobowe dyżury administratorów systemów kluczowych dla funkcjonowania organizacji oraz personelu uprawnionego do podejmowania decyzji w sprawach bezpieczeństwa systemów teleinformatycznych.

3. Po wprowadzeniu **trzeciego stopnia alarmowego CRP (stopień CHARLIE-CRP)** należy wykonać zadania wymienione dla pierwszego i drugiego stopnia alarmowego CRP oraz kontynuować lub sprawdzić wykonanie tych zadań, jeżeli wcześniej był wprowadzony stopień ALFA-CRP lub BRAVO-CRP. Ponadto należy wykonać w szczególności następujące zadania:

1) wprowadzić całodobowe dyżury administratorów systemów kluczowych dla funkcjonowania organizacji oraz personelu uprawnionego do podejmowania decyzji w sprawach bezpieczeństwa systemów;
2) dokonać przeglądu dostępnych zasobów zapasowych pod względem możliwości ich wykorzystania w przypadku zaistnienia ataku;
3) przygotować się do uruchomienia planów umożliwiających zachowanie ciągłości działania po wystąpieniu potencjalnego ataku, w tym:
   a) dokonać przeglądu i ewentualnego audytu planów awaryjnych oraz systemów,
   b) przygotować się do ograniczenia operacji na serwerach, w celu możliwości ich szybkiego i bezawaryjnego zamknięcia.

4. Po wprowadzeniu **czwartego stopnia alarmowego CRP (stopień DELTA-CRP)** należy wykonać zadania wymienione dla pierwszego, drugiego i trzeciego stopnia alarmowego CRP oraz kontynuować lub sprawdzić wykonanie tych zadań, jeżeli wcześniej był wprowadzony stopień ALFA-CRP, BRAVO-CRP lub CHARLIE-CRP. Ponadto należy wykonać w szczególności następujące zadania:
1) uruchomić plany awaryjne lub plany ciągłości działania organizacji w sytuacjach awarii lub utraty ciągłości działania;
2) stosownie do sytuacji przystąpić do realizacji procedur przywracania ciągłości działania.

Zaznaczyć również należy, iż organy administracji publicznej oraz kierownicy służb i instytucji właściwych w sprawach bezpieczeństwa i zarządzania kryzysowego w terminie 6 miesięcy od dnia wejścia w życie właściwego rozporządzenia zobowiązani zostali do określenia procedur realizacji przedsięwzięć w ramach poszczególnych stopni alarmowych i stopni alarmowych CRP, w tym moduły zadaniowe dla każdego stopnia.

Spis Tabel

Spis Wykresów