CSIRT GOV

Raport o stanie bezpieczeństwa cyberprzestrzeni RP w 2018 roku

Warszawa, kwiecień 2019 r.

ZESPÓŁ CSIRT GOV

Zespół Reagowania na Incydenty Bezpieczeństwa Komputerowego CSIRT GOV, prowadzony przez Szefa Agencji Bezpieczeństwa Wewnętrznego, pełni rolę Zespołu CSIRT poziomu krajowego. Odpowiada on za koordynację procesu reagowania na incydenty komputerowe występujące w obszarze wskazanym w art. 26 ust 7 *ustawy z dnia 5 lipca 2018 roku o krajowym systemie cyberbezpieczeństwa* (Dz.U.2018 poz.1560, dalej: *ustawa o ksc*). 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 (Dz.U.2018.1401)*.

CSIRT GOV

dane kontaktowe

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

www.csirt.gov.pl
csirt@csirt.gov.pl
tel.: +48 22 58 59 373
faks: +48 22 58 58 833

Spis treści

Wstęp

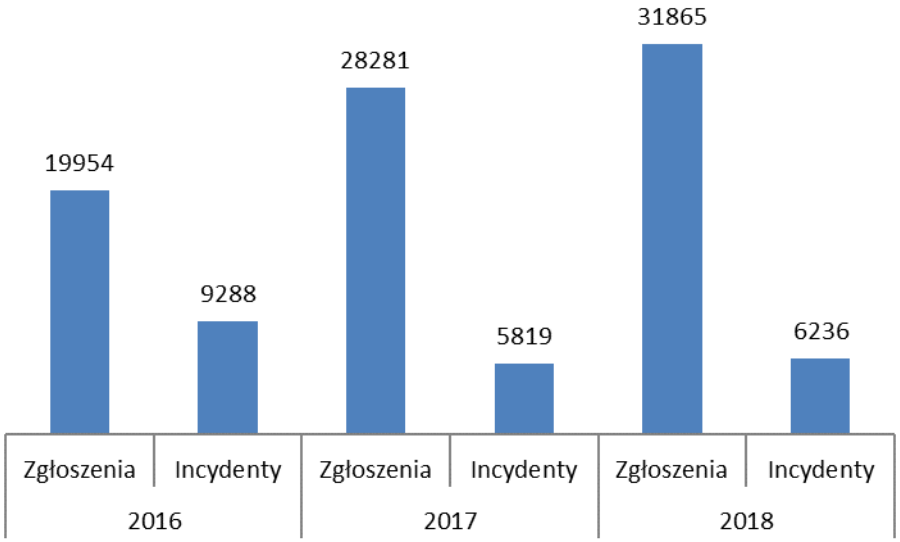
Raport o stanie bezpieczeństwa cyberprzestrzeni RP w 2018 roku opublikowany przez Zespół CSIRT GOV zawiera dane statystyczne, które mają dostarczyć wiedzy niezbędnej do realizacji procesów podnoszących bezpieczeństwo systemów teleinformatycznych. Raport ma na celu podnoszenie świadomości użytkowników o zagrożeniach i podatnościach ukierunkowane na osiągnięcie podstawowego akceptowalnego poziomu bezpieczeństwa systemów teleinformatycznych oraz na podjęcie decyzji o wdrożeniu działań ograniczających możliwość eskalacji wystąpienia zagrożenia.

1. STATYSTYKI INCYDENTÓW KOORDYNOWANYCH PRZEZ ZESPÓŁ CSIRT GOV

W 2018 roku Zespół Reagowania na Incydenty Bezpieczeństwa Komputerowego CSIRT GOV odnotował aż **31 865** zgłoszeń o potencjalnym wystąpieniu incydentów komputerowych w sieciach znajdujących się w obszarze kompetencyjnym Zespołu. Stanowi to znaczący wzrost względem 2017 roku, w którym zarejestrowano **28 281** zgłoszeń.

Odnotowane w Zespole CSIRT GOV zgłoszenia poddawane są weryfikacji, w wyniku której określa się, czy uzyskana informacja nosi znamiona faktycznego incydentu komputerowego czy też jest tzw. *false positive*. Każde przychodzące zgłoszenie wymaga również sprawdzenia, czy dotyczy incydentu zaistniałego już wcześniej, co jest szczególnie wyraźne w sytuacjach wykorzystywania systemów automatycznych oraz prowadzonych kampanii phishingowych. W takich przypadkach, ta sama złośliwa wiadomość trafia do szerokiego grona odbiorców generując wiele zgłoszeń jednego incydentu.

W związku z tak prowadzonymi wstępnymi analizami zgłoszeń incydentów, w 2018 roku ustalono, iż ze zgłoszonych **31 865** incydentów faktyczne naruszenie bezpieczeństwa teleinformatycznego instytucji miało miejsce w **6 236** przypadkach, co stanowi wzrost względem 2017 roku, w którym faktycznych incydentów odnotowano **5 819**.

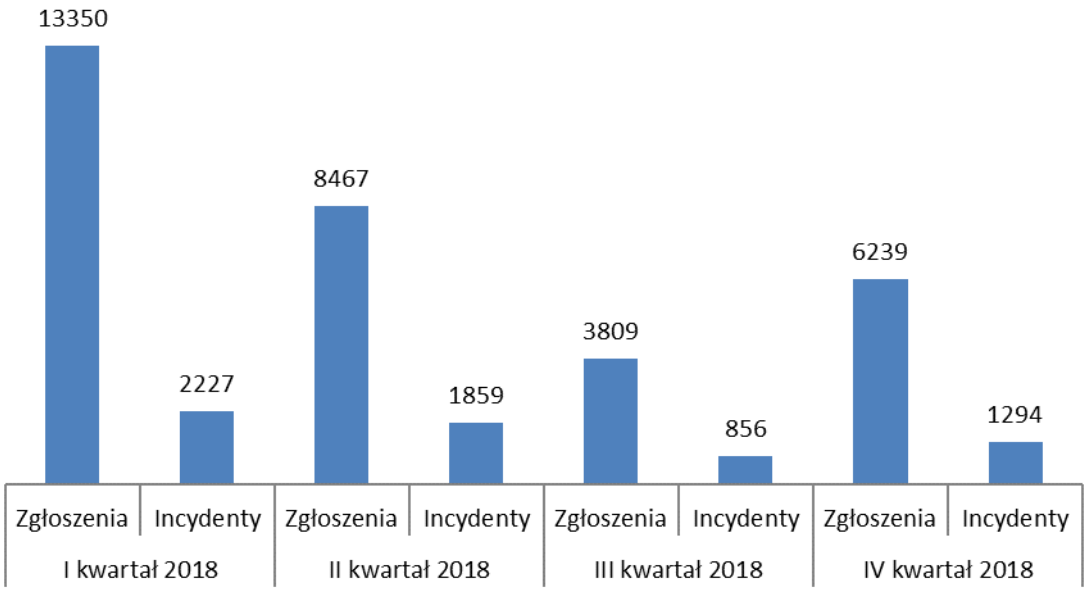


Wykres 1 Liczba zarejestrowanych zgłoszeń oraz incydentów w latach 2016-2018

Jak widać na powyższym wykresie, tendencja zgłoszeń o potencjalnym wystąpieniu incydentów komputerowych jest stale rosnąca. Przyczyną takiego stanu rzeczy może być między innymi wzrost zainteresowania potencjalnych atakujących sieciami rządowymi w Polsce oraz stosunkowy wzrost incydentów będących wynikiem błędnych konfiguracji albo braku aktualizacji.

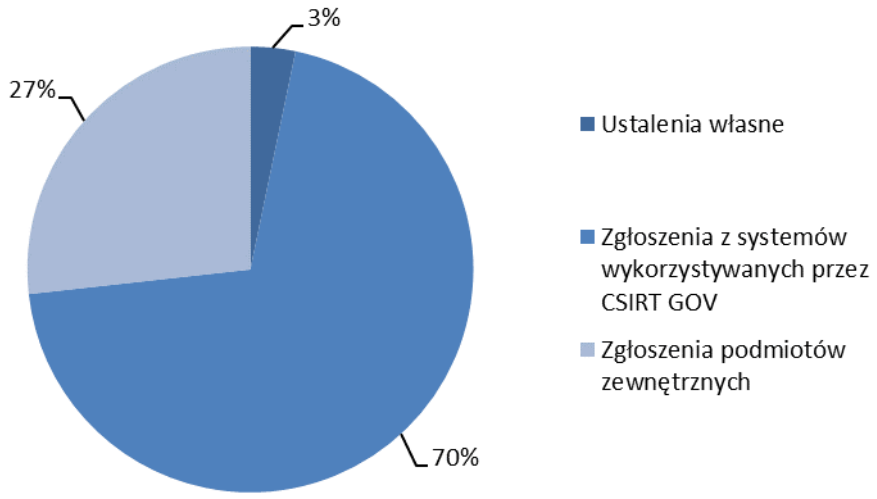
Należy zauważyć, że tematy dotyczące bezpieczeństwa cyberprzestrzeni są coraz częściej poruszane w mediach publicznych oraz portalach internetowych, a co za tym idzie - wzrasta świadomość społeczna na temat zagrożeń w cyberprzestrzeni.

Ponadto, znaczna różnica pomiędzy zgłoszeniami a faktycznie zarejestrowanymi incydentami wynika z ciągłego rozwoju systemów wspomagających pracę analityków Zespołu CSIRT GOV. Stają się one coraz bardziej precyzyjne w analizowaniu przepływów w sieci oraz w określaniu faktycznych zagrożeń dla systemów i sieci komputerowych, co istotnie wpływa na wzrost jakości analizy każdego zarejestrowanego przypadku.



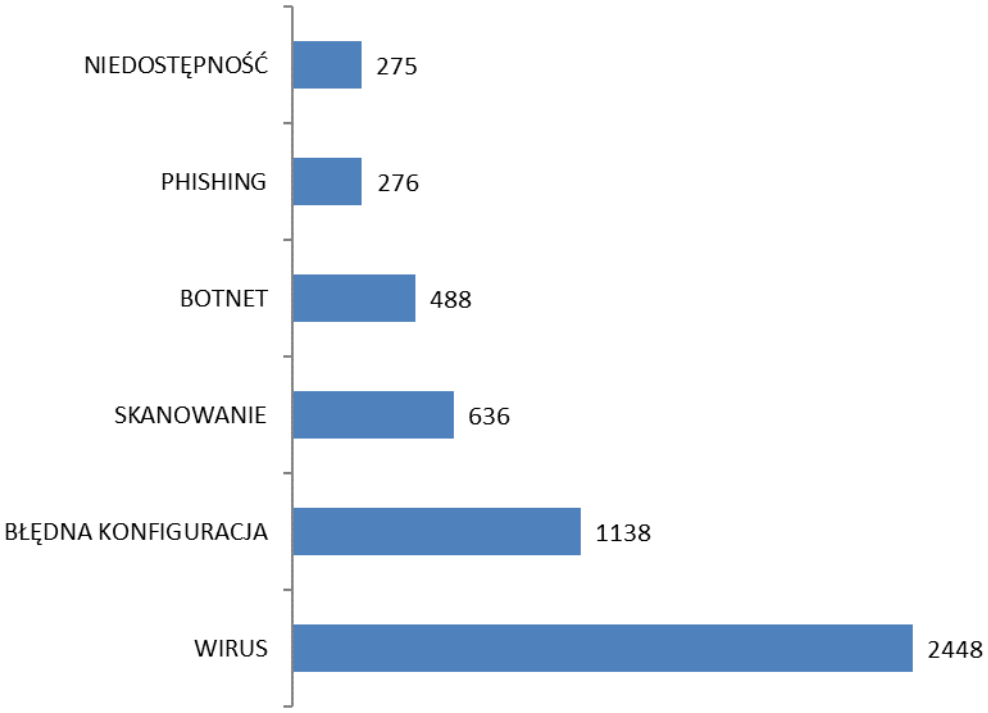
Wykres 2 Liczba zarejestrowanych zgłoszeń oraz incydentów w poszczególnych kwartałach 2018 roku

Różnica zgłoszeń incydentów w poszczególnych kwartałach 2018 roku wynika m. in. z propagacji złośliwego oprogramowania, podjętych działań przez jednostki administracji publicznej w stosunku do zgłoszeń dotyczących w szczególności błędnej konfiguracji urządzeń oraz wynika z zasięgu i intensywności kampanii phishingowych.



Wykres 3 Źródło zgłoszeń incydentów

Źródłami informacji o zaistniałych bądź potencjalnych incydentach bezpieczeństwa teleinformatycznego są wykorzystywane systemy, ustalenia własne CSIRT GOV oraz zgłoszenia od podmiotów zewnętrznych. Podobnie jak w poprzednich latach, w 2018 roku większość agregowanych informacji tj. **70%** pozyskano z wykorzystywanych przez Zespół CSIRT GOV systemów. **27%** z nich stanowiły zgłoszenia od podmiotów zewnętrznych, a **3%** to tzw. ustalenia własne Zespołu.



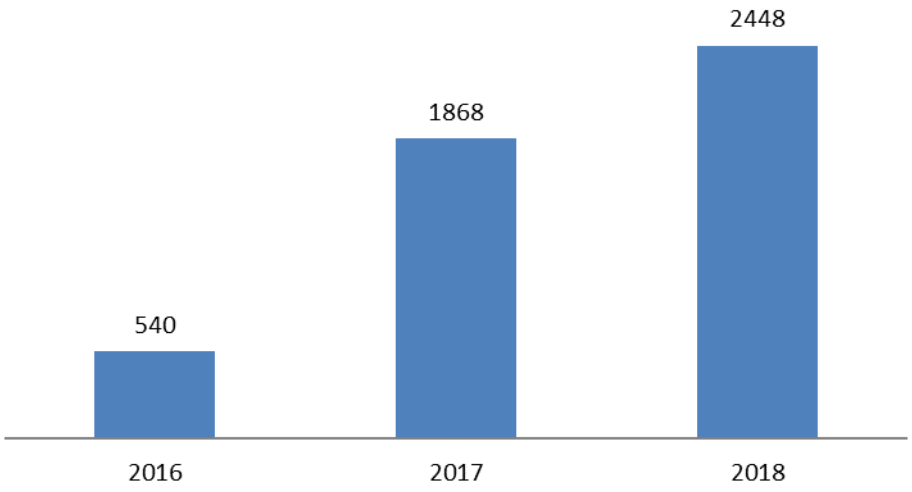
Wykres 4 Klasyfikacja najczęstszych incydentów zgłoszonych do CSIRT GOV w 2018 r.

Kolejnym istotnym zagadnieniem jest rodzaj odnotowywanych incydentów. W 2018 roku najczęściej występującymi incydentami były należące do kategorii *wirus,* definiowanej jako uzyskanie informacji na temat prawdopodobnej infekcji stacji roboczej, serwerów lub urządzeń sieciowych. Cyberprzestępcy bardzo często w celu propagacji złośliwego oprogramowania wykorzystują elementy inżynierii społecznej np. złośliwe załączniki w wiadomościach email. Takie wiadomości zaklasyfikowano do kategorii *wirus*.

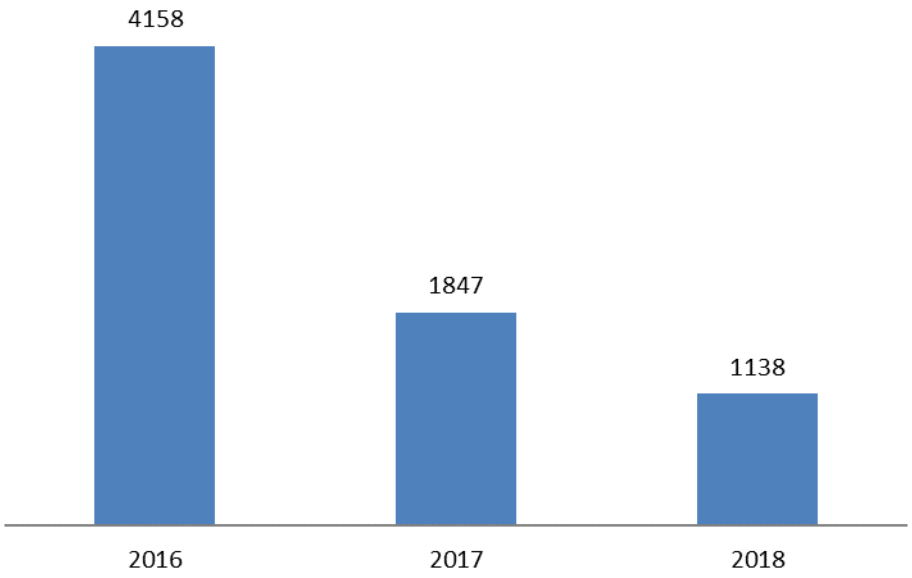
Drugą najczęściej występującą kategorią w 2018 roku była *błędna konfiguracja urządzenia*, w której odnotowano **1 138** incydentów. Należy podkreślić, iż ten rodzaj zagrożenia bezpieczeństwa, choć nie wynika z ingerencji zewnętrznej w system, w wielu przypadkach może stanowić furtkę do przeprowadzenia skutecznego ataku.

Incydenty z trzeciej najczęściej występującej kategorii *skanowanie* polega na wysyłaniu pakietów TCP do dowolnych typów urządzeń sieciowych w celu sprawdzenia otwartych portów oraz dostępnych usług. Przedmiotowe działanie może być wykorzystane do złamania zabezpieczeń systemów teleinformatycznych.

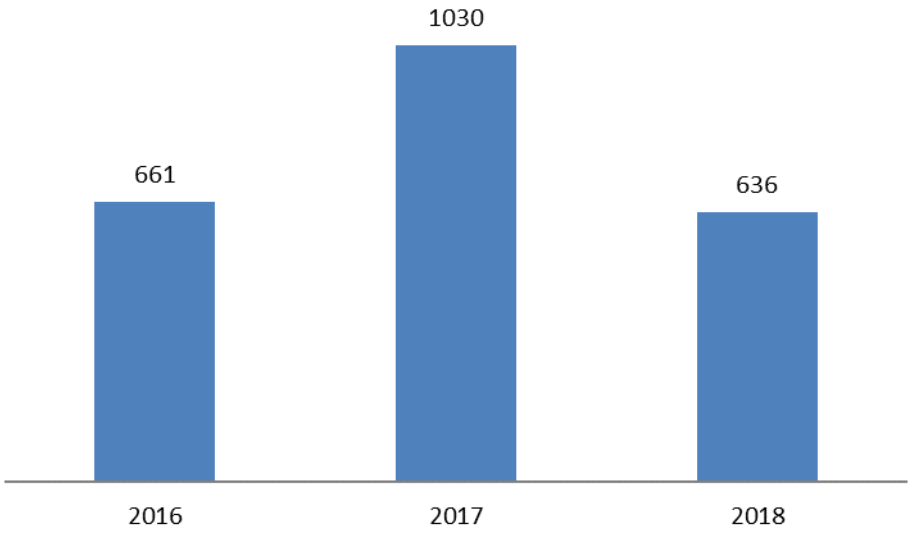
W kontekście powyższych informacji należy również zwrócić uwagę na liczbę incydentów w poszczególnych kategoriach w odniesieniu do poprzednich lat. Poniżej przedstawiono wykresy przedstawiające dane z lat 2016, 2017 oraz 2018.



Wykres 5 Liczba zarejestrowanych incydentów w kategorii *Wirus* w latach 2016 - 2018



Wykres 6 Liczba zarejestrowanych incydentów w kategorii *Błędna konfiguracja urządzenia* w latach 2016– 2018



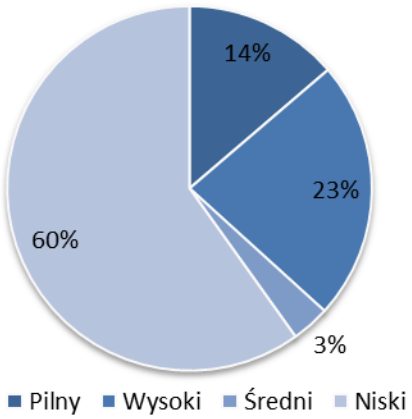
Wykres 7 Liczba zarejestrowanych incydentów w kategorii *Skanowanie* w latach 2016 - 2018

2. ANALIZA ALARMÓW NA PODSTAWIE SYSTEMU ARAKIS 3.0 GOV

System ARAKIS 3.0 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 2018 roku w sieciach teleinformatycznych podmiotów uczestniczących w projekcie ARAKIS 3.0 GOV zanotowano łącznie **319 943 424** przepływów, co przełożyło się na **454 207** wygenerowanych przez system alarmów[1]. Wśród zanotowanych alarmów:

- **62 365** alarmów miało priorytet pilny, tzn. wymagało natychmiastowej reakcji na zagrożenie ze strony administratorów, niosło duże ryzyko przełamania zabezpieczeń;
- **104 502** alarmów miało priorytet wysoki, tzn. wymagało wzmożonej uwagi w kontekście zagrożenia wskazanego w alarmie, niosło średnie ryzyko przełamania zabezpieczeń;
- **15 412** alarmów miało priorytet średni, tzn. były to alarmy informujące o dobrze znanym zagrożeniu, które niosły małe ryzyko przełamania zabezpieczeń;
- **271 928** alarmów miało priorytet niski, tzn. były to alarmy czysto informacyjne dot. aktualnej sytuacji na styku sieci wewnętrznej z siecią Internet.

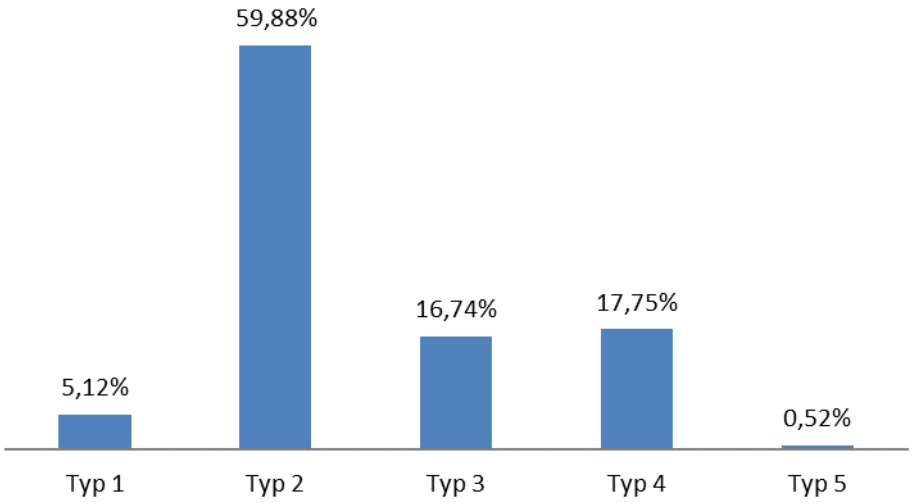


Wykres 8 Procentowy rozkład alarmów systemu ARAKIS 3.0 GOV ze względu na priorytet

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

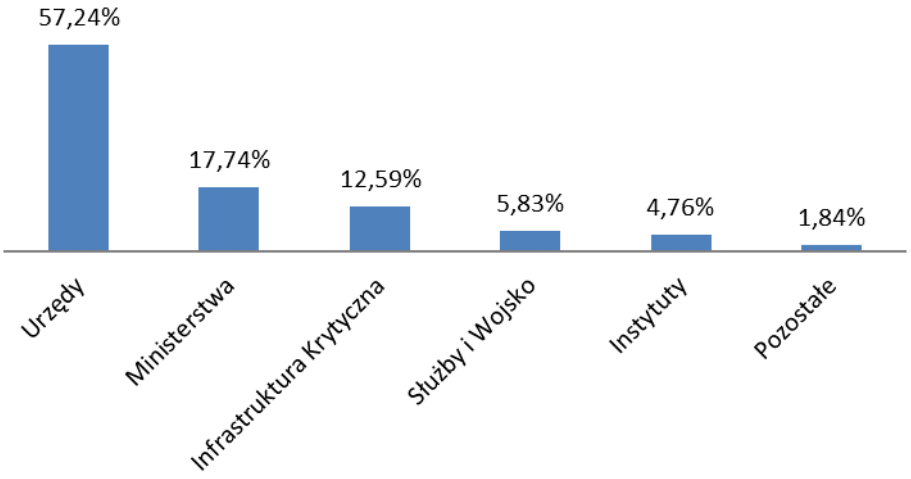
Każdy z zanotowanych alarmów posiada dokładne dane techniczne, pozwalające na jego weryfikację oraz jest szczegółowo klasyfikowany przez system. W ramach klasyfikacji każdy alarm może zostać przypisany do jednego z pięciu podstawowych typów:

- 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 systemu ARAKIS 3.0 GOV ze względu na typ

Wśród alarmów typu 2 w 2018 roku najwięcej przepływów zostało zanotowanych w instytucjach skategoryzowanych jako *Urzędy* (57,24%), co może wynikać bezpośrednio z ilości wysyłanych pakietów TCP lub UDP do systemów teleinformatycznych dostępnych przez sieć TCP/IP w celu sprawdzenia otwartych portów i dostępnych usług.

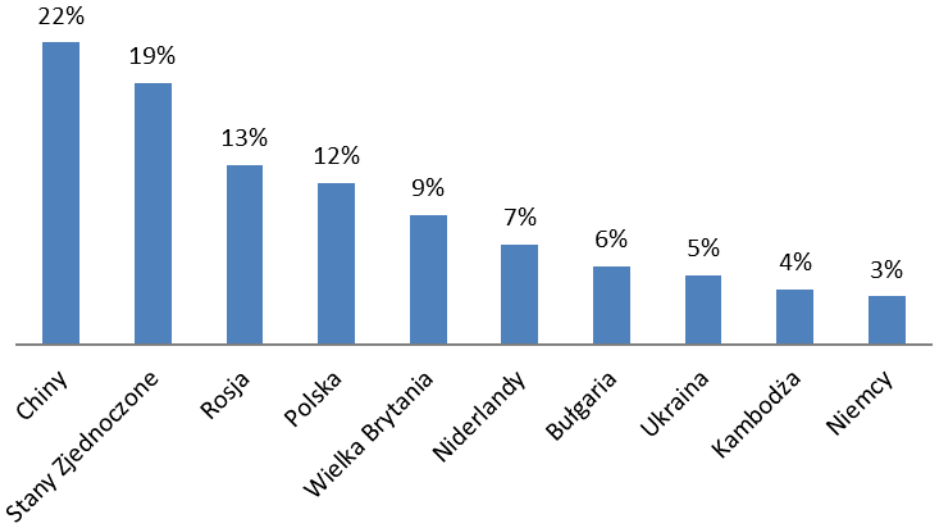


Wykres 10 Procentowy podział przepływów alarmów typu 2 w instytucjach

Wśród alarmów typu 3 i 4 zanotowano 16,74% (typ 3) oraz 17,75% (typ 4) ze wszystkich przepływów, co wprost wynika z wygenerowania sygnatury IDS w oparciu o obserwowane komunikacje lub dopasowania do sygnatury IDS nie widzianej w systemie od pewnego czasu. Ma to miejsce zarówno przy wygenerowaniu nowej sygnatury IDS jak i przy aktualizacji uprzednio wygenerowanej sygnatury lub w przypadku gdy Honeypot zaraportował, że w wyniku interakcji został pobrany nowy, unikalny złośliwy plik.

Do najbardziej aktywnych krajów pod kątem liczby generowanych przepływów w 2018 roku należały Chiny (22% przepływów) oraz Stany Zjednoczone (19% przepływów). Należy zwrócić uwagę na duży stosunek przepływów pochodzących z adresów należących do Rosji (13% przepływów) oraz Polski (12% przepływów). Na przestrzeni ostatnich 6 lat Polska pojawiła się w pierwszej dziesiątce tego zestawienia dopiero drugi raz. Pierwszy raz miał miejsce w 2015 roku - przepływy pochodzące z Polski stanowiły wtedy 0,9% wszystkich odnotowanych.

Warto też zaznaczyć, iż liczba przepływów z poszczególnych krajów należących do grupy TOP 10 stanowi 71% wszystkich wygenerowanych przepływów zanotowanych przez System ARAKIS 3.0 GOV w 2018 roku.



Wykres 11 Rozkład źródeł ataków na sieci monitorowane przez system ARAKIS 3.0 GOV pod kątem liczby generowanych przepływów

Biorąc pod uwagę specyfikę sieci Internet (tzw. *brak granic*), infrastruktura teleinformatyczna podmiotów generujących przepływy w stronę systemu ARAKIS 3.0 GOV może być rozproszona oraz zlokalizowana na terytorium dowolnych państw na całym świecie. W związku z powyższym zaprezentowaną powyżej statystykę należy traktować podglądowo.

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

L.p.	Docelowy port/protokół	Liczba przepływów	Opis
1	22/TCP	37 548 696	Ataki na usługę SSH
4	0/ICMP	26 118 497	Skanowanie ICMP (Echo Replay)
3	23/TCP	25 013 268	Ataki na usługę telnet
4	80/TCP	18 082 458	Ataki na aplikacje webowe
5	445/TCP	17 404 976	Ataki na usługę Windows SMB
6	5060/UDP	6 162 989	Ataki na usługę SIP VoIP
7	8291/TCP	5 496 725	Ataki na usługę MikroTik
8	7547/TCP	5 387 039	Nasłuchiwania przezprotokół zarządzania CWMP

			(TR-069)
9	3306/TCP	4 257 425	Ataki na bazę danych MySQL
10	25/TCP	3 968 325	Ataki na usługę SMTP

Tabela 1 Zidentyfikowane w 2018 roku skanowania i próby eksploitacji usług na podstawie danych z systemu ARAKIS 3.0 GOV

Od kilku lat niezmiennie najczęściej atakowanymi usługami są usługi zapewniające zdalny dostęp do danego zasobu teleinformatycznego (SSH). Najczęstszym scenariuszem próby przełamania zabezpieczeń w tym przypadku są ataki słownikowe (*brute-force*). Dużą liczbę przepływów można zauważyć również na porcie 23/TCP należącym do usługi telnet, zastępowanym przez SSH.

L.p.	Liczba przepływów	Reguła SNORT
1	6146501	"ET SCAN Potential SSH Scan OUTBOUND"
2	4558171	"ET SCAN Suspicious inbound to MSSQL port 1433"
3	4 157751	"ET SCAN SSH BruteForce Tool with fake PUTTY version"
4	2688328	"GPL NETBIOS SMB-DS IPC$ unicode share access"
5	2 159089	"ET SCAN Sipvicious User-Agent Detected (friendly-scanner)"
6	1471774	"ET SCAN Potential SSH Scan"
7	1389999	"ET INFO Potentially unsafe SMBv1 protocol in use"
8	1 148079	"GPL NETBIOS SMB-DS IPC$ share access"
9	1144315	"ET SCAN Sipvicious Scan"
10	967806	"ET SCAN Suspicious inbound to mySQL port 3306"

Tabela 2 Najczęściej dopasowane reguły do ruchu sieciowego widzianego przez system ARAKIS 3.0 GOV

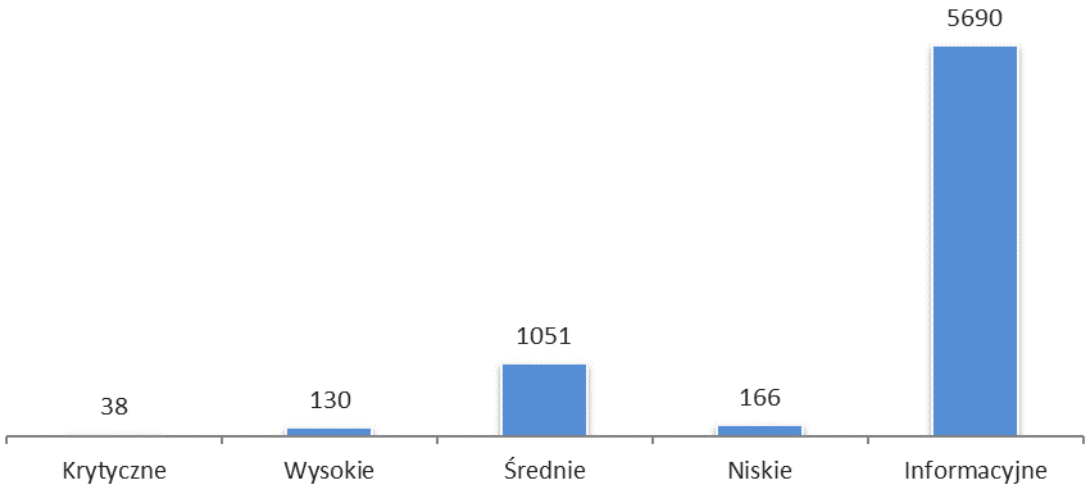
W 2018 roku zidentyfikowano 27 107 981 dopasowań reguł SNORT do obserwowanego ruchu sieciowego. Przedmiotowe dopasowania mają odzwierciedlenie m.in. w ruchu zaprezentowanym w poprzedniej tabeli na poszczególne porty docelowe – najczęściej wykrywane są reguły dotyczące prób nieuprawnionego wykorzystania usług SSH oraz prób skanowania usług MSSQL.

3. OCENA BEZPIECZEŃSTWA SYSTEMÓW TI

W 2018 roku Zespół Reagowania na Incydenty Bezpieczeństwa Komputerowego CSIRT GOV na mocy art. 32a *Ustawy z dnia 24 maja 2002 r. o Agencji Bezpieczeństwa Wewnętrznego oraz Agencji Wywiadu* (Dz. U. z 2016 r. poz. 1897, z późn. zm.) oraz *Rozporządzenia Rady Ministrów z dnia 19 lipca 2016 r. w sprawie przeprowadzania oceny bezpieczeństwa związanej z zapobieganiem zdarzeniom o charakterze terrorystycznym*, dokonał oceny bezpieczeństwa systemów teleinformatycznych instytucji administracji rządowej oraz infrastruktury krytycznej.

W ramach przeprowadzonych ocen bezpieczeństwa Zespół CSIRT GOV przeprowadził szereg testów mających na celu identyfikację istotnych podatności wpływających na bezpieczeństwo infrastruktur teleinformatycznych instytucji. Do rzeczonych testów należało pasywne, półpasywne oraz aktywne zbieranie informacji, identyfikacja podatności architektury systemów i usług sieciowych, wykorzystywanie podatności oraz analiza wpływu wykorzystania czynników inżynierii społecznej.

W wyniku przeprowadzonych ocen bezpieczeństwa Zespół CSIRT GOV dokonał identyfikacji szeregu podatności od stopnia informacyjnego poprzez błędy należące do kategorii krytyczne. Poniższy wykres przedstawia zestawienie zidentyfikowanych podatności.



Wykres 12 Liczba podatności ze względu na kategorię

Do najistotniejszych (krytycznych oraz wysokich) podatności zidentyfikowanych w ramach przeprowadzonych ocen bezpieczeństwa systemów teleinformatycznych należały:

- serwery FTP umożliwiające anonimowe logowanie oraz nieograniczony dostęp do zgromadzonych na nich danych;
- hosty akceptujące połączenia z wykorzystaniem szyfrowania SSL 2.0 i/lub 3.0, co pozwala na przeprowadzenie ataków typu Man-in-the-middle;

- podatności typu XSS pozwalające atakującego na wysłanie złośliwego kodu poprzez podatną aplikację WWW do innego użytkownika;
- niewspierana przez producenta wersja systemu operacyjnego zainstalowanego na zdalnym hoście;
- podatność na ataki typu BREACH;
- wersja wykorzystywanego PHP nie jest wspierana przez producenta;
- wersja serwera Web: Oracle GlassFish Server posiadające liczne podatności;
- wersja Apache podatna na liczne CVE;
- serwer WWW wspierający metody TRACE i/lub TRACK wykorzystywane do debugowania połączeń serwera;
- możliwość zamontowania zasobu NFS udostępnianego przez zdalny host;
- zdalny serwer X akceptujący zdalne połączenia TCP;
- wersja HP System Management Homepage (SMH) zawierająca podatności;
- na serwerze NTP występująca podatność typu *odmowa usługi* spowodowana nieprawidłową weryfikacją kwerend mrulist;
- wykorzystanie hosta zewnętrznego oraz polecenia PORT dające możliwość wykonania operacji na zdalnym serwerze FTP;
- serwer VNC zainstalowany na zdalnym hoście umożliwiający atakującemu połączenie z zdalnym hostem;
- dostępnym panel administracyjny do phpmyadmin;
- błąd SQL Injection mogący pozwalać atakującemu podmienić strukturę logiczną zapytania SQL kierowanego do produkcyjnej bazy danych, z której korzysta witryna WWW;
- możliwość wstrzyknięcia w podatny system dowolnego nagłówka HTTP typu Host I przepisania adresów na każdej stronie tak, aby kierowały do jego spreparowanych zasobów;
- znalezienie kodu źródłowego aplikacji wraz z plikiem konfiguracyjnym, które mogą zawierać wrażliwe informacje takie jak połączenia do bazy danych;
- podatność pozwalająca na zastosowaniu ataku man-in-the-middle w komunikacji HTTPS wykorzystującej bibliotekę Open SSL;
- włączony tryb (devMode) programisty w Struts 2 (false lub true w struts.properties);
- serwlety ‘EBJInvokerServlet’ oraz ‘JMXInvokerServlet’ hostowane na zdalnej maszynie, dostępne są dla nieuwierzytelnionych użytkowników;
- wersja system posiada sterownik HTTP.sys w podatnej wersji;
- serwer JBoss umożliwia nieuwierzytelniony dostęp do serwletów JMX i/lub zdanej konsoli pozwalających na zdalne zarządzenie serwerem I jego usługami;
- directory traversal pozwala atakującemu uzyskać dostęp do plików.

W przypadku podatności o mniejszej wadze (średnie, niskie oraz wysokie) do najczęściej identyfikowanych przez Zespół CSIRT GOV można zaliczyć:

- logowanie do panelu administracyjnego serwera Apache Tomcat przy pomocy nieszyfrowanego protokołu http;
- hasła użytkowników podatne na atak typu *brute-force*;
- posiadanie nieaktualnych wersji bibliotek jQuery;
- aktywna metoda OPTIONS na serwerze;
- usługa rsh działająca na zdalnym hoście – podatna na atak;
- możliwość uzyskania domyślnej nazwy zdalnego serwera SNMP;
- usługa rlogin działająca na zdalnym hoście, podatna na uszkodzenia;
- panel logowania do usługi dostępny z sieci TOR;
- błędnie skonfigurowany mechanizm CORS;
- nieaktualna wersja serwera IIS;
- standard szyfrowania XML W3C, zaimplementowany w JBossWS posiadający podatność;
- błędnie wpisany rekord DNS.

W ramach prowadzonych ocen bezpieczeństwa Zespół CSIRT GOV przeprowadził również analizę źródeł otwartych w ramach czynności typu OSINT. Czynności te pozwoliły na określenie ilości danych zawartych jako *metadata* w dokumentach publikowanych w ramach publicznych serwerów WWW oraz portalach społecznościowych, na których pracownicy posiadali aktywne konta.

4. USTAWA O KRAJOWYM SYSTEMIE CYBERBEZPIECZEŃSTWA

W dniu 28 sierpnia 2018 roku weszła w życie *ustawa o ksc*, która określa organizację krajowego systemu oraz zadania i obowiązki podmiotów wchodzących w jego skład. Odnosi się to także do funkcjonującego od ponad dekady Zespołu Reagowania na Incydenty Komputerowe CERT.GOV.PL, który od dnia wejścia w życie przedmiotowej ustawy przeobraził się w Zespół Reagowania na Incydenty Bezpieczeństwa Komputerowego CSIRT GOV stając się jednym z trzech CSIRTów poziomu krajowego. Pozostałe dwa zespoły zaliczone do danego poziomu to CSIRT MON prowadzony przez Ministra Obrony Narodowej, oraz CSIRT NASK prowadzony przez Naukową i Akademicka Sieć Komputerową.

Ustawa o ksc wprowadziła również rozróżnienie zgłaszanych incydentów na incydent: poważny, krytyczny, istotny oraz incydent w podmiocie publicznym. Rozróżnienie uzależnione zostało od kategorii podmiotu zgłaszającego incydent. Tak jest w przypadku incydentu poważnego, istotnego i incydentu w podmiocie publicznym. W odniesieniu do incydentu poważnego ustawodawca dodatkowo określił progi uznania zdarzenia za incydent poważny, które znajdziemy w akcie wykonawczym do ustawy tj. *Rozporządzeniu Rady Ministrów z dnia 31 października 2018 r. w sprawie progów uznania incydentu za poważny* (DZ.U.2018.2180). Inaczej natomiast przedstawia się sytuacja w przypadku kategorii incydentu sklasyfikowanego jako krytyczny – jest to incydent skutkujący znaczną szkodą dla bezpieczeństwa lub porządku publicznego, interesów międzynarodowych, interesów gospodarczych, działania instytucji publicznych, praw i wolności obywatelskich lub życia i zdrowia ludzi, klasyfikowany przez właściwy CSIRT MON, CSIRT NASK lub CSIRT GOV (art. 2 pkt 6). W tym przypadku mamy więc do czynienia z sytuacją, podczas której klasyfikację nakłada właściwy zespół reagowania na incydenty bezpieczeństwa komputerowego poziomu krajowego.

Przyporządkowanie podmiotów do konkretnych CSIRTów poziomu krajowego znajduje się w art. 26 ust 5, 6, 7. Ustawodawca do CSIRT GOV przypisał:

1) jednostki sektora finansów publicznych, o których mowa w art. 9 pkt 1, 8 i 9 *ustawy z dnia 27 sierpnia 2009 r. o finansach publicznych*, z wyjątkiem przypisanych do innych CSIRTów krajowych;

2) jednostki podległe Prezesowi Rady Ministrów lub przez niego nadzorowane;

3) Narodowy Bank Polski;

4) Bank Gospodarstwa Krajowego;

5) inne niż wyżej wymienione podmioty, których systemy teleinformatyczne lub sieci teleinformatyczne objęte są jednolitym wykazem obiektów, instalacji, urządzeń i usług wchodzących w skład infrastruktury krytycznej;

6) podmioty wymienione przy CSIRT NASK jeżeli incydent dotyczy systemów teleinformatycznych lub sieci teleinformatycznych objętych jednolitym wykazem obiektów, instalacji, urządzeń i usług wchodzących w skład infrastruktury krytycznej.

Biorąc pod uwagę zakresy przypisane do CSIRTów krajowych uznać należy, iż dotychczasowo funkcjonujące rozróżnienie na gov.pl – CERT.GOV.PL, pl – CERT.PL i mil.pl – MIL-CERT przestało obowiązywać z dniem wejścia w życie *ustawy o ksc*.

Wykaz kompetencji Zespołów CSIRT znajduje się w art. 26 *ustawy o ksc*, gdzie poza reagowaniem na zgłoszone incydenty, prowadzeniem zaawansowanej analizy złośliwego oprogramowania czy monitorowaniem wskaźników zagrożeń cyberbezpieczeństwa i podatności znalazły się również m.in.:

1) szacowanie ryzyka związanego z ujawnionym zagrożeniem cyberbezpieczeństwa oraz zaistniałymi incydentami, w tym prowadzenie dynamicznej analizy ryzyka;
2) wydawanie komunikatów o zidentyfikowanych zagrożeniach cyberbezpieczeństwa;
3) przeprowadzanie w uzasadnionych przypadkach badania urządzenia informatycznego lub oprogramowania w celu identyfikacji podatności, której wykorzystanie może zagrozić w szczególności integralności, poufności, rozliczalności, autentyczności lub dostępności przetwarzanych danych, które może mieć wpływ na bezpieczeństwo publiczne lub istotny interes bezpieczeństwa państwa, oraz składanie wniosków w sprawie rekomendacji dla podmiotów krajowego systemu cyberbezpieczeństwa dotyczących stosowania urządzeń informatycznych lub oprogramowania, w szczególności w zakresie wpływu na bezpieczeństwo publiczne lub istotny interes bezpieczeństwa państwa;
4) współpraca z sektorowymi zespołami cyberbezpieczeństwa w zakresie koordynowania obsługi incydentów poważnych, w tym dotyczących dwóch lub większej liczby państw członkowskich Unii Europejskiej, i incydentów krytycznych oraz w zakresie wymiany informacji pozwalających przeciwdziałać zagrożeniom cyberbezpieczeństwa;
5) przekazywanie do innych państw, w tym państw członkowskich Unii Europejskiej, i przyjmowanie z tych państw informacji o incydentach poważnych i incydentach istotnych dotyczących dwóch lub większej liczby państw członkowskich, a także przekazywanie do Pojedynczego Punktu Kontaktowego zgłoszenia incydentu poważnego i istotnego dotyczącego dwóch lub większej liczby państw członkowskich Unii Europejskiej;
6) opracowywanie i przygotowywanie materiałów analityczno-informacyjnych na rzecz ministra właściwego do spraw informatyzacji/Pełnomocnika

ds. cyberbezpieczeństwa, Kolegium ds. cyberbezpieczeństwa, zespołu ds. incydentów krytycznych czy Pojedynczego Punktu Kontaktowego;

7) zapewnienie zaplecza analitycznego oraz badawczo-rozwojowego, które w szczególności:
   - rozwija narzędzia i metody do wykrywania i zwalczania zagrożeń cyberbezpieczeństwa,
   - prowadzi analizy i opracowuje standardy, rekomendacje i dobre praktyki w zakresie cyberbezpieczeństwa,
   - wspiera podmioty krajowego systemu cyberbezpieczeństwa w budowaniu potencjału i zdolności w obszarze cyberbezpieczeństwa,
   - prowadzi działania z zakresu budowania świadomości w obszarze cyberbezpieczeństwa,
   - współpracuje w zakresie rozwiązań edukacyjnych w obszarze cyberbezpieczeństwa.

Zgodnie z obowiązkiem wynikającym z *ustawy o ksc* CSIRT GOV przygotował i zamieścił na stronach www.csirt.gov.pl oraz www.bip.abw.gov.pl formularze do zgłoszenia incydentu oraz dedykowany do zgłoszenia wyznaczonych osób odpowiedzialnych za utrzymywanie kontaktów z podmiotami krajowego systemu cyberbezpieczeństwa. Przypomnieć również należy, iż zgłoszenie incydentu powinno nastąpić niezwłocznie jednak nie później niż w ciągu 24 godzin od momentu jego wykrycia. W przypadku osób wyznaczonych do kontaktów zgłoszenia należy dokonać w terminie 14 dni od dnia jej wyznaczenia, analogiczne zasady mają zastosowanie w przypadku zmiany danych osób wyznaczonych. Wskazać należy, iż do dnia 31 grudnia 2018 r roku do CSIRT GOV wpłynęło ok. 40 zgłoszeń o wyznaczonych osobach.

Kolejnym nowym uprawnieniem przypisanym Agencji Bezpieczeństwa Wewnętrznego jest prowadzenie, koordynowanie funkcjonowania a także wdrażanie w określonej kategorii podmiotach systemu wczesnego ostrzegania o zagrożeniach występujących w sieci Internet (art. 79 oraz art. 91 *ustawy o ksc*, wprowadzające do *ustawy z dnia 24 maja 2002 r o Agencji Bezpieczeństwa Wewnętrznego oraz Agencji Wywiadu*. Wdrożenie elementów systemu ostrzegania w podmiotach, następuje zgodnie z rocznym planem wdrożenia, opracowywanym przez Szefa ABW w terminie do dnia 30 września roku poprzedzającego. Po zatwierdzeniu planu Agencja Bezpieczeństwa Wewnętrznego informuje o tym fakcie podmioty w nim ujęte. Podmiot ma obowiązek przystąpić do systemu ostrzegania oraz przekazać ABW niezbędne informacje umożliwiające wdrożenie systemu ostrzegania w tym podmiocie.

Do pełnego wdrożenia Systemu niezbędne jest:

- sondy systemu muszą być wdrożone przed wszelkimi systemami bezpieczeństwa na styku sieci wewnętrznej z siecią Internet;
- dysponowanie wolnymi adresami z publicznej puli;
- zapewnienie braku ograniczeń dla ruchu wychodzącego i przychodzącego dla sond;
- brak NATowania dla adresacji sond;
- doprowadzenie kopii ruchu produkcyjnego do sondy;
- dostęp do platformy sprzętowej i programowej separowany od innych systemów produkcyjnych.

Na System ARAKIS 3.0 GOV składają się następujące moduły, które realizują przypisane im funkcjonalności:

Moduł Reflector (REF) - moduł odpowiedzialny za obserwację ruchu sieciowego występującego na posiadanych przez Uczestnika lecz niewykorzystywanych przez niego czynnie do obsługi produkcyjnego ruchu sieciowego publicznych adresów IP. Moduł generuje sygnatury podejrzanego ruchu sieciowego, automatycznie przesyłając je z sond zainstalowanych u uczestników Projektu do Centrum Systemu;

Moduł Forwarder (FWD) moduł odpowiedzialny za odbieranie oraz interpretację danych przesyłanych przez źródła dodatkowe (np. oprogramowanie firewall, oprogramowanie antywirusowe serwera pocztowego, oprogramowanie serwera WWW) oraz przesyłanie ich do Centrum Systemu;

Moduł APTDetect Sensor (APTDetect) - moduł odpowiedzialny za monitoring produkcyjnego ruchu sieciowego generowanego przez Uczestnika oraz wykrywania niepożądanego ruchu w oparciu o analizę protokołów warstwy aplikacyjnej.

W uzasadnionych przypadkach, na wniosek podmiotu, wdrożenie elementów systemu ostrzegania może zostać przeprowadzone z pominięciem planu. Podmiot, który do dnia wejścia w życie *ustawy o ksc* przystąpił do realizowanego przez Agencję Bezpieczeństwa Wewnętrznego programu ARAKIS-GOV, uznaje się za podmiot, który przystąpił do systemu ostrzegania, w rozumieniu ww. zapisów. W przypadku instytucji, które nie wdrożyły Systemu ARAKIS GOVw pełnej konfiguracji obowiązkiem jest uzupełnienie wdrożenia wszystkich modułów przedmiotowego systemu w terminie roku od dnia wejścia w życie *ustawy o ksc*.

Spis Tabel

Spis Wykresów