# CERT.GOV.PL

# Raport o stanie bezpieczeństwa cyberprzestrzeni RP w 2017 roku


**Warszawa, kwiecień 2018 r.**

**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
tel: +48 22 58 59 373
faks: +48 22 58 58 833

## Spis treści

## Wstęp

Raport o stanie bezpieczeństwa cyberprzestrzeni RP w 2017 roku opublikowany przez Zespół CERT.GOV.PL zawiera dane statystyczne i informacje, które przede wszystkim mają dostarczyć wiedzy niezbędnej do realizacji procesów podnoszących bezpieczeństwo systemów teleinformatycznych. Raport ma na celu podnoszenie świadomości użytkowników o zagrożeniach i podatnościach, a wprowadzenie zawartych w nim rekomendacji pozwoli na osiągnięcie podstawowego akceptowalnego poziomu bezpieczeństwa systemów teleinformatycznych oraz na wdrożenie działań ograniczających możliwość eskalacji wystąpienia zagrożenia.

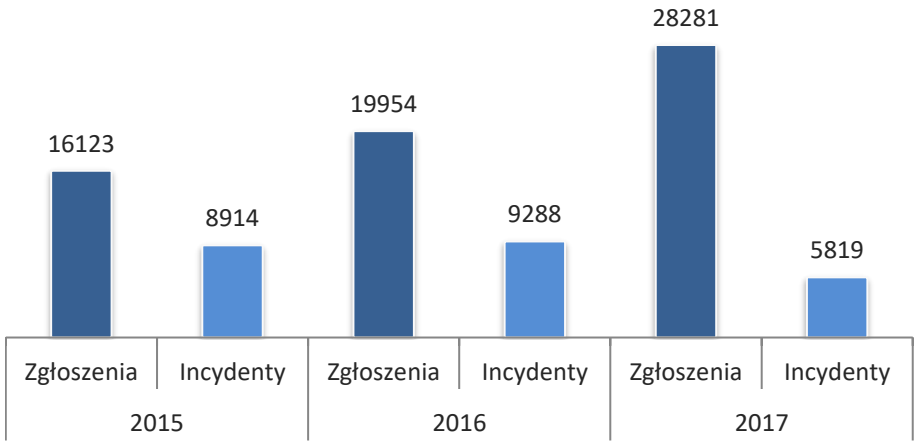
# 1. STATYSTYKI INCYDENTÓW KOORDYNOWANYCH PRZEZ ZESPÓŁ CERT.GOV.PL

W 2017 roku Rządowy Zespół Reagowania na Incydenty Komputerowe CERT.GOV.PL odnotował aż 28 281 zgłoszeń o potencjalnym wystąpieniu incydentów komputerowych w sieciach znajdujących się w obszarze kompetencyjnym Zespołu. Stanowi to znaczący wzrost względem 2016 roku, w którym zarejestrowano 19 954 zgłoszenia.

Odnotowane w Zespole CERT.GOV.PL 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.

Zespół CERT.GOV.PL weryfikuje także zgłoszenia pochodzące z systemów automatycznych jak np. N6[1].

W związku z tak prowadzonymi wstępnymi analizami zgłoszeń incydentów, w 2017 roku ustalono, iż ze zgłoszonych 28 281 incydentów faktyczne naruszenie bezpieczeństwa teleinformatycznego instytucji miało miejsce w 5 819 przypadkach, co stanowi spadek względem 2016 roku, w którym faktycznych incydentów odnotowano 9 288.




**Wykres 1 Liczba zarejestrowanych zgłoszeń oraz incydentów w latach 2015-2017**

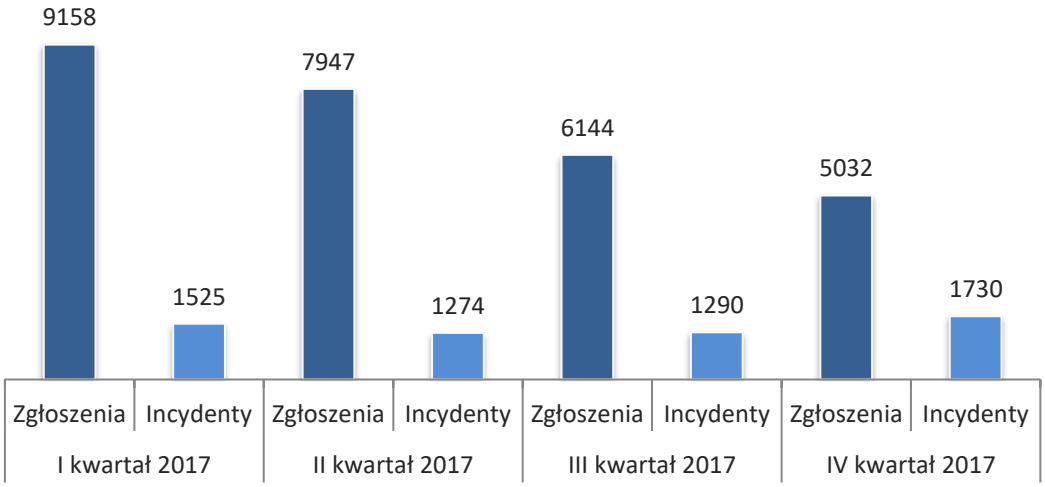
Jak widać na powyższym wykresie, tendencja zgłoszeń o potencjalnym wystąpieniu incydentów komputerowych jest stale rosnąca. Przyczyną takiego stanu rzeczy może

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

być między innymi wzrost zainteresowania potencjalnych atakujących sieciami rządowymi w Polsce oraz stosunkowy wzrost incydentów będących wynikiem błędnych konfiguracji albo braku aktualizacji.

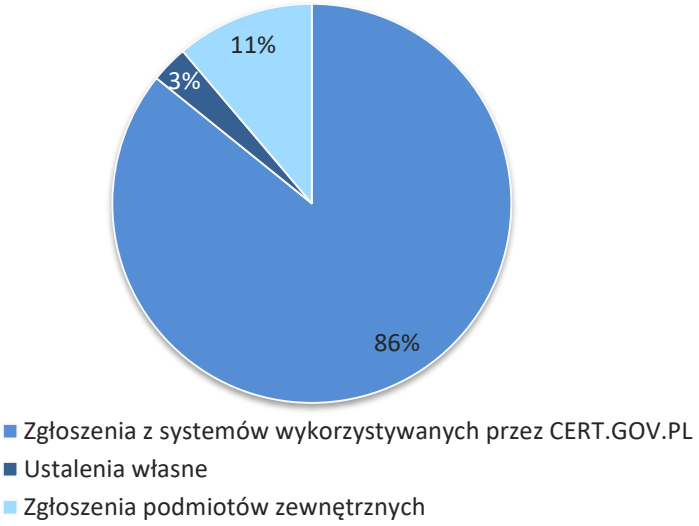
Należy zauważyć, że tematy dotyczące bezpieczeństwa cyberprzestrzeni są coraz częściej poruszane w mediach publicznych oraz portalach internetowych, a co za tym idzie - wzrasta świadomość społeczna na temat zagrożeń w cyberprzestrzeni.

Ponadto, znaczna różnica pomiędzy zgłoszeniami a faktycznie zarejestrowanymi incydentami wynika z ciągłego rozwoju systemów wspomagających pracę analityków Zespołu CERT.GOV.PL. 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.



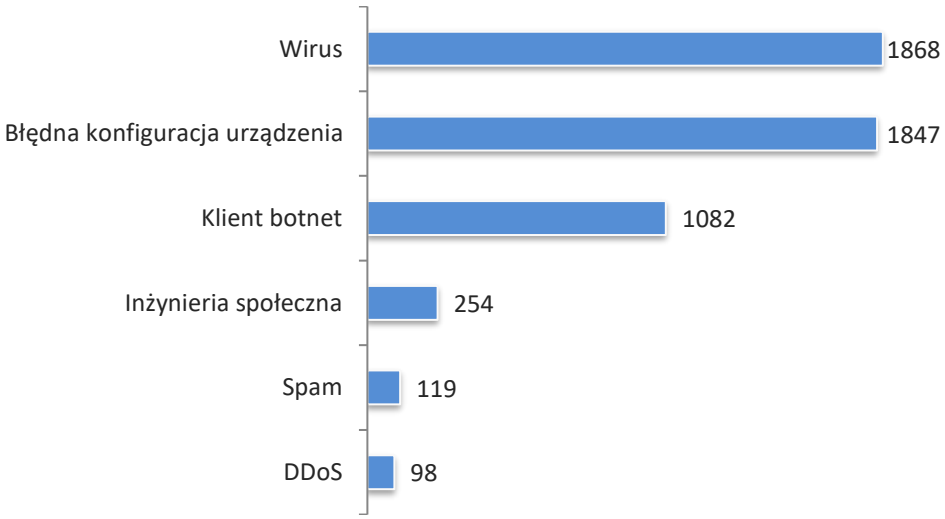

**Wykres 2 Liczba zarejestrowanych zgłoszeń oraz incydentów w poszczególnych kwartałach 2017 roku**

Różnica zgłoszeń incydentów w poszczególnych kwartałach 2017 roku wynikała m. in. z zasięgu i intensywności kampanii phishingowych/propagacji złośliwego oprogramowania oraz podjętych działań przez jednostki administracji publicznej w stosunku do zgłoszeń dotyczących w szczególności błędnych konfiguracji urządzeń oraz klientów sieci botnet.




**Wykres 3 Źródła zgłoszeń incydentów**

Źródłami informacji o zaistniałych bądź potencjalnych incydentach bezpieczeństwa teleinformatycznego są wykorzystywane systemy, ustalenia własne CERT.GOV.PL oraz zgłoszenia od podmiotów zewnętrznych. Podobnie jak w poprzednichlatach, w 2017 roku większość agregowanych informacji tj. 86% pozyskano z wykorzystywanych przez Zespół CERT.GOV.PL systemów. 11% z nich stanowiły zgłoszenia od podmiotów zewnętrznych, a 3% to tzw. ustalenia własne Zespołu.




**Wykres 4 Liczba wybranych incydentów w 2017 roku ze względu na kategorie**

Kolejnym istotnym zagadnieniem jest rodzaj odnotowywanych incydentów. W 2017 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.

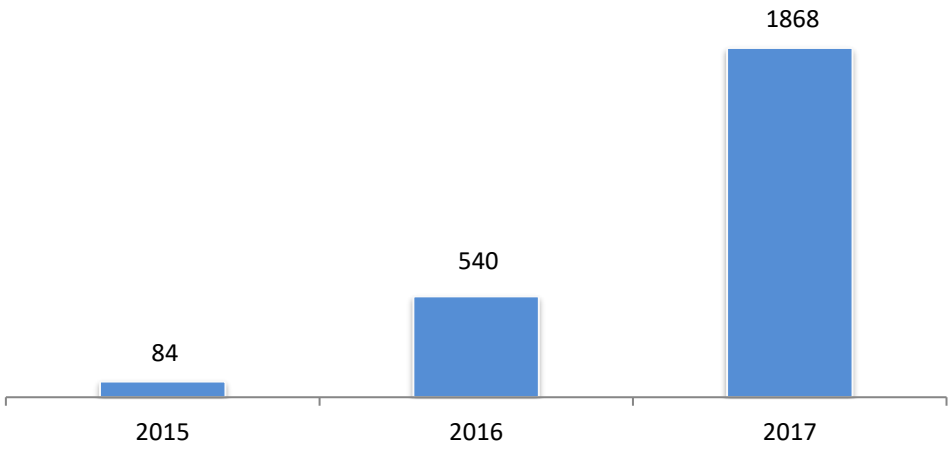
złośliwe załączniki w wiadomościach email. Takie wiadomości zaklasyfikowano do kategorii *Wirus*.

Drugą najczęściej występującą kategorią w 2017 roku była *Błędna konfiguracjaurządzenia*, w której odnotowano 1 847 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.

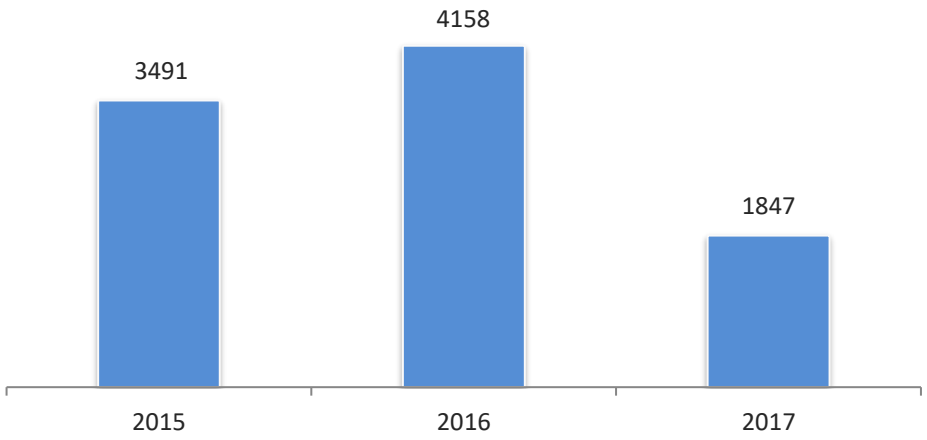
Incydenty z trzeciej najczęściej występującej kategorii *Klient sieci botnet* to zdarzenia, w których, z wykorzystaniem systemów wspomagających, zaobserwowano próby połączenia (bardzo często udane) stacji roboczych z adresami/domenami sklasyfikowanymi jako serwery C&C lub charakterystyka ruchu sieciowego odpowiadała wskaźnikom IoC znanych sieci Botnet. Mimo, iż nadal ta kategoria incydentów znajduje się na pozycji trzeciej to jednakże należy zauważyć, odnotowywaną w ostatnich latach wyraźnie spadkową tendencję w tym zakresie. Wynika to m.in. z prowadzonych na całym świecie działań skierowanych przeciwko systemom kierującym grupami zarażonych komputerów, czyli tzw. serwerami C&C.

Zdarzenia o charakterze *Inżynierii społecznej* to wiadomości, które w związku z brakiem złośliwej zawartości bez większych problemów trafiały do odbiorców i miały na celu wyłudzenie wrażliwych danych lub wykonanie nieautoryzowanej czynności np. transakcji finansowej na zagraniczny rachunek.

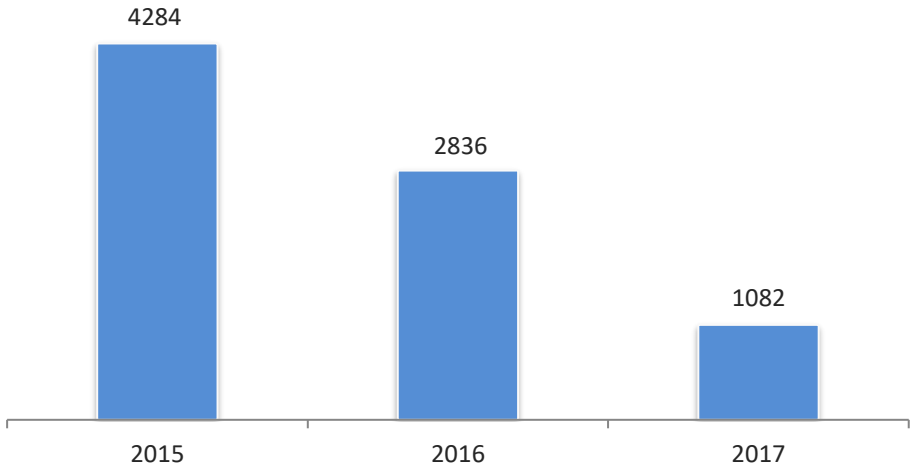
W kontekście powyższych informacji należy również zwrócić uwagę na liczbę incydentów w poszczególnych kategoriach w odniesieniu do poprzednich lat. Poniżej przedstawiono wykresy przedstawiające dane z lat 2015, 2016 oraz 2017.



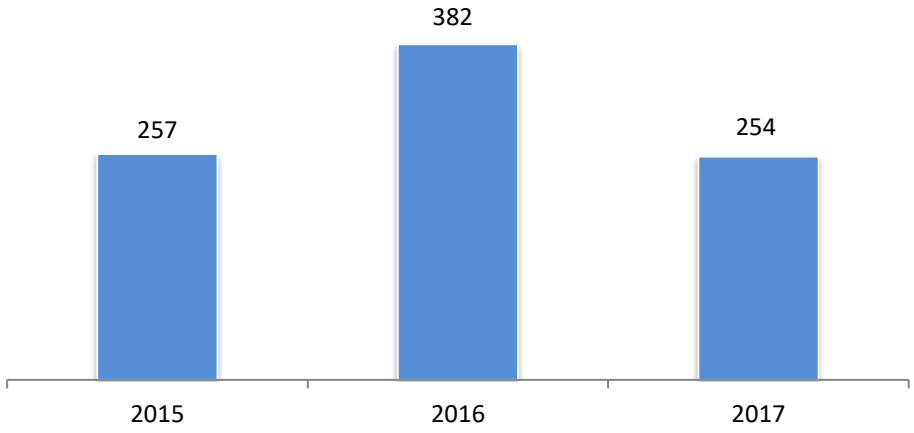

**Wykres 5 Liczba zarejestrowanych incydentów w kategorii *Wirus* w latach 2015 - 2017**




**Wykres 6 Liczba zarejestrowanych incydentów w kategorii *Błędna konfiguracja urządzenia* w latach 2015 - 2017**




**Wykres 7 Liczba zarejestrowanych incydentów w kategorii *Klient botnet* w latach 2015 - 2017**



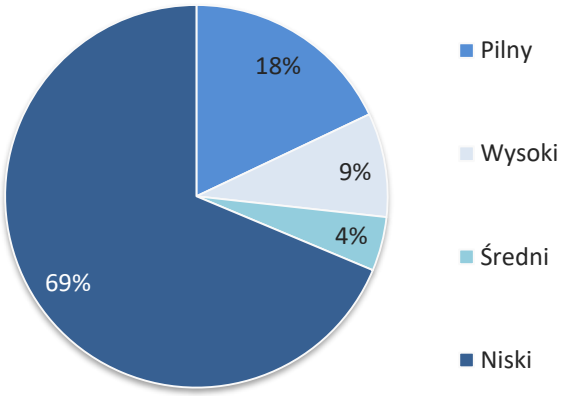

**Wykres 8 Liczba zarejestrowanych incydentów w kategorii *Inżynieria społeczna* w latach 2015 - 2017**

# 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 2017 roku w sieciach teleinformatycznych podmiotów uczestniczących w projekcie ARAKIS 2.0 GOV zanotowano łącznie 323 722 095przepływów, co przełożyło się na 347 178 wygenerowanych przez system alarmów[2]. Wśród zanotowanych alarmów:

- 62 292 alarmów miało priorytet pilny tzn. wymagało natychmiastowej reakcji na zagrożenie ze strony administratorów, niosło duże ryzyko przełamania zabezpieczeń;
- 30 505 alarmów miało priorytet wysoki tzn. wymagało wzmożonej uwagi w kontekście zagrożenia wskazanego w alarmie, niosło średnie ryzyko przełamania zabezpieczeń;
- 15 911 alarmów miało priorytet średni tzn. były to alarmy informujące o dobrze znanym zagrożeniu, które niosły małe ryzyko przełamania zabezpieczeń;
- 238 470 alarmów miało priorytet niski tzn. były to alarmy czysto informacyjne dot. aktualnej sytuacji na styku sieci wewnętrznej z siecią Internet.

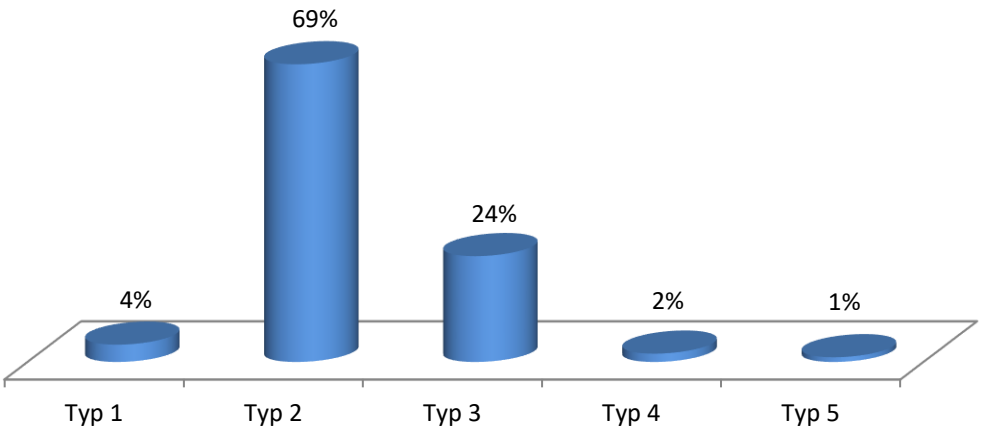



**Wykres 9 Procentowy rozkład alarmów systemu ARAKIS 2.0 GOV ze względu na priorytet**

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

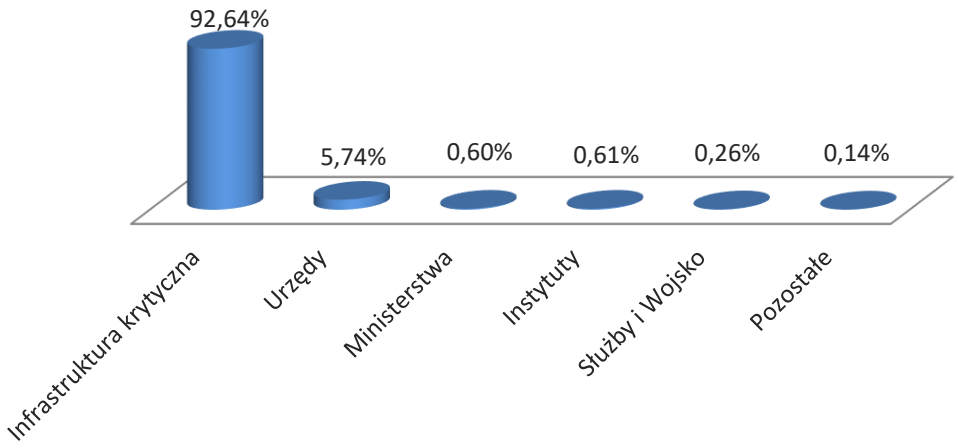
Każdy z zanotowanych alarmów posiada dokładne dane techniczne, pozwalające na jego weryfikację oraz jest szczegółowo klasyfikowany przez system. W ramach klasyfikacji każdy alarm może zostać przypisany do jednego z pięciu podstawowych typów:

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



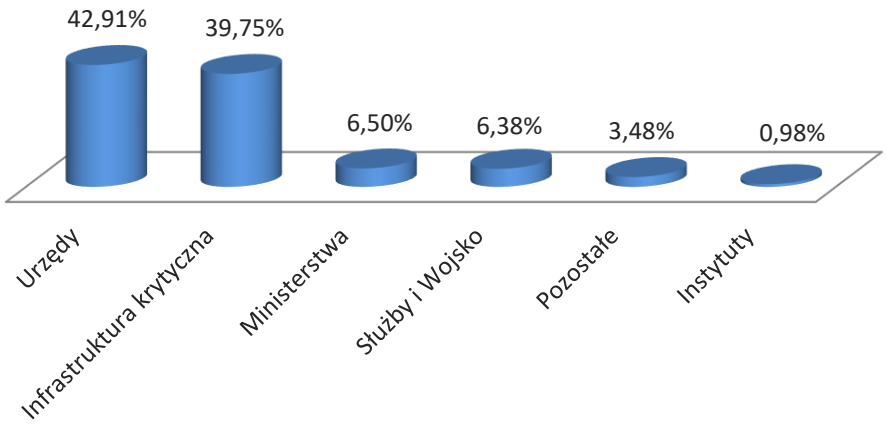

**Wykres 10 Procentowy podział alarmów systemu ARAKIS 2.0 GOV ze względu na typ**

Wśród alarmów typu 1 w 2017 roku najwięcej przepływów zostało zanotowanych w instytucjach skategoryzowanych jako „Infrastruktura Krytyczna" (92,64%), co może wynikać bezpośrednio z ilości generowanego przez podmioty ruchu sieciowego.




**Wykres 11 Procentowy podział przepływów alarmów typu 1 w instytucjach**

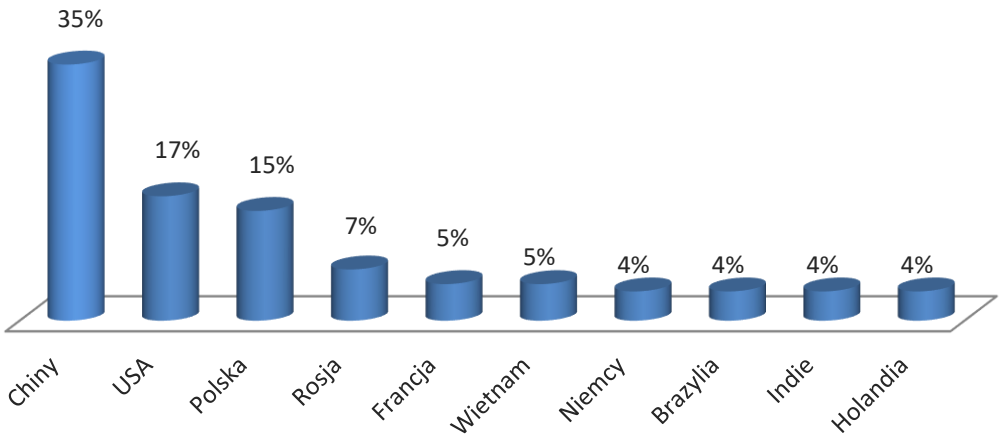
Wśród alarmów typu 5 najwięcej przepływów zostało zanotowanych w instytucjach skategoryzowanych jako „Urzędy" (42,91%) oraz „Infrastruktura krytyczna" (39,75%), co wprost wynika z liczby posiadanych urządzeń końcowych.




**Wykres 12 Procentowy podział przepływów alarmów typu 5 w instytucjach**

Do najbardziej aktywnych krajów pod kątem liczby generowanych przepływów w 2017 roku należały Chiny (35% przepływów) oraz Stany Zjednoczone (17% przepływów). Należy zwrócić uwagę na duży stosunek przepływów pochodzących z adresów należących do Polski (15% przepływów). Na przestrzeni ostatnich 5 lat Polska pojawiła się w pierwszej dziesiątce tego zestawienia tylko raz - w 2015 roku (przepływy pochodzące z Polski stanowiły wtedy 0,9 % wszystkich odnotowanych).

Warto też zaznaczyć, iż liczby przepływów z poszczególnych krajów należących do grupy TOP 10 stanowi 70% wszystkich wygenerowanych przepływów zanotowanych przez System ARAKIS 2.0 GOV w 2017 roku.




**Wykres 13 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 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 | 63 575 377 | Ataki na usługę SSH |
| 2 | 23/TCP | 54 613 131 | Ataki na usługę telnet |
| 3 | 25/TCP | 21 950 320 | Atak na usługę SMTP |
| 4 | 0/ICMP | 16 257 198 | Skanowanie ICMP (Echo Replay) |
| 5 | 80/TCP | 13 657 103 | Ataki na aplikacje webowe |
| 6 | 1433/TCP | 11 723 197 | Ataki na bazę danych MSSQL |
| 7 | 445/TCP | 10 525 182 | Ataki na usługę Windows SMB |
| 8 | 5060/UDP | 6 252 863 | Ataki na usługę SIP VoIP |
| 9 | 3306/TCP | 5 299 442 | Ataki na bazę danych MySQL |
| 10 | 2323/TCP | 4 578 093 | Ataki na usługę telnet |

**Tabela 1 Zidentyfikowane w 2017 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). Dużą liczbę przepływów można zauważyć również na porcie 25/TCP należącym do usługi SMTP. Udany atak może spowodować w efekcie wysyłanie niechcianych wiadomości e-mail.

| L.p. | Liczba przepływów | Reguła SNORT |
|---|---|---|
| 1 | 11163101 | "ET SCAN Potential SSH Scan OUTBOUND" |
| 2 | 7434039 | "ET SCAN SSH BruteForce Tool with fake PUTTY version" |
| 3 | 3170171 | "ET SCAN Sipvicious User-Agent Detected (friendly-scanner)" |
| 4 | 2 565581 | "ET SCAN Potential SSH Scan" |

| | | |
|---|---|---|
| 5 | 1633184 | "ET SCAN Sipvicious Scan" |
| 6 | 1557710 | "GPL NETBIOS SMB-DS IPC$ unicode share access" |
| 7 | 739990 | "ET INFO Potentially unsafe SMBv1 protocol in use" |
| 8 | 656254 | "GPL NETBIOS SMB-DS IPC$ share access" |
| 9 | 245807 | "ET SCAN LibSSH Based Frequent SSH Connections Likely BruteForce Attack" |
| 10 | 195433 | "ET SCAN SipCLI VOIP Scan" |

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

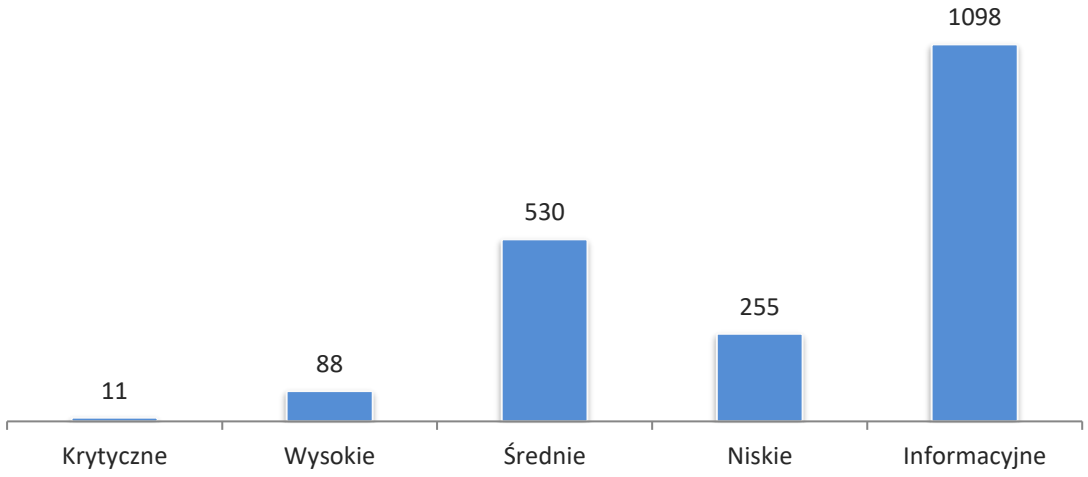
W 2017 roku zidentyfikowano 30 484 678 dopasowań reguł SNORT do obserwowanego ruchu sieciowego. Przedmiotowe dopasowania mają odzwierciedlenie m.in. w ruchu zaprezentowanym w poprzedniej tabeli na poszczególne porty docelowe – najczęściej wykrywane są reguły dotyczące prób nieuprawnionego wykorzystania usług SSH, SIP VoIP oraz ataków na usługi webowe.

# 3. OCENA BEZPIECZEŃSTWA SYSTEMÓW TI

W 2017 roku Rządowy Zespół Reagowania na Incydenty Komputerowe CERT.GOV.PL na mocy art. 32a Ustawy z dnia 24 maja 2002 r. o Agencji Bezpieczeństwa Wewnętrznego oraz Agencji Wywiadu oraz Rozporządzeniem 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 CERT.GOV.PL 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 CERT.GOV.PL dokonał identyfikacji szeregu podatności od stopnia informacyjnego poprzez błędy należące do kategorii krytyczne. Poniższy wykres przedstawia zestawienie zidentyfikowanych podatności.




**Wykres 14 Liczba podatności ze względu na kategorię**

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

- Drupal - pre Auth SQL Injection,
- wersja OpenSSL pozwalająca na przeprowadzenie ataktu man-in-the-middle,
- Oracle TNS Listener Poison Attack,
- Eternalblue Windows SMBv1,
- PHP w wersji 7.0.18, 5.4.16,

- podatność SQL Injection poprzez aplikację CGI,
- podatność BREACH (Browser Reconnaise and Exfiltration via Adaptive Compression of Hypertext),
- nieprawidłowa konfiguracja CORS,
- aktywna funkcja allow_url_fopen,
- nieaktualna wersja biblioteki jQuery pozwalająca na atak typu XSS,
- podatność typu File Path Manipulation,
- podatności typu XSS,
- podatność Directory Traversal w Spring Framework,
- podatność typu RCE (Remote Code Execution) w Secure Channel.

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

- podpisanie certyfikatu SSL algorytmem szyfrowania SSH-1 podatnym na kolizje,
- stosowanie certyfikatów niezaufanych oraz z wygaśniętą datą ważności,
- podatności typu SWEET oraz POODLE,
- wsparcie dla słabych algorytmów szyfrowania SSL,
- niewłaściwe wartości atrybutu 'commonName' certyfikatów,
- słabe szyfrowanie komunikacji RDP,
- wsparcie dla słabej grupy szyfrów Diffie-Hellman,
- możliwość identyfikacji typów oraz wersji serwerów WWW,
- brak wprowadzonych nagłówków HSTS,
- podatność na atak typu Slowloris.

W ramach prowadzonych ocen bezpieczeństwa Zespół CERT.GOV.PL 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. REKOMENDACJE

Wychodząc na przeciw zainteresowaniu instytucji rekomendacjami dotyczącymi cyberbezpieczeństwa, Rządowy Zespół Reagowania na Incydenty Komputerowe CERT.GOV.PL dokonał przeglądu i aktualizacji zaleceń zawartych w Raporcie o stanie bezpieczeństwa cyberprzestrzeni RP w 2015 roku. Opracowane rekomendacje mają na celu podniesienie szeroko pojętego bezpieczeństwa teleinformatycznego w jawnych systemach instytucji administracji państwowej.

Rekomendacje zostały podzielone na trzy kategorie: organizacyjne, techniczne oraz edukacyjno-informacyjne. Powinny być traktowane jako baza do wypracowania szczegółowych mechanizmów bezpieczeństwa dla działalności instytucji administracji państwowej w kontekście realizowanych przez nią działań.

Celem osiągnięcia minimalnego akceptowalnego poziomu bezpieczeństwa systemów teleinformatycznych oraz wdrożenia działań mających na celu ograniczenie możliwości eskalacji ewentualnego wystąpienia zagrożenia/podatności na inne jednostki, Zespół CERT.GOV.PL rekomenduje wprowadzenie niżej wymienionych zaleceń.

## REKOMENDACJE ORGANIZACYJNE

**REKOMENDACJA 1**: Określenie kluczowych z punktu widzenia instytucji danych, które należy poddać szczególnej ochronie.

**REKOMENDACJA 2**: Identyfikacja kluczowych systemów teleinformatycznych w instytucji, które należy poddać szczególnej ochronie.

**REKOMENDACJA 3**: W przypadku określonych kluczowych systemów teleinformatycznych odpowiednie dobieranie rozwiązań sprzętowych, które będą w jak najbardziej zaufany i bezawaryjny sposób realizować zadania z zakresu zabezpieczenia systemów. Wybór rozwiązań powinien być planowany już na etapie planowania zakupów.

**REKOMENDACJA 4**: Opracowanie wewnętrznego katalogu zagrożeń oraz incydentów, uwzględniającego specyfikę działalności instytucji.

**REKOMENDACJA 5**: Stworzenie przejrzystych zasad użytkowania sieci wewnętrznej przez pracowników np. poprzez wytworzenie regulaminów (np. użytkowania komputera wyłącznie do celów służbowych), procedur (np. postępowania z incydentami bezpieczeństwa) oraz instrukcji (np. bezpiecznego budowania haseł).

**REKOMENDACJA 6:** Powołanie osób odpowiedzialnych za bezpieczeństwo teleinformatyczne w instytucji oraz przypisanie im konkretnych zakresów obowiązków.

**REKOMENDACJA 7**: Przygotowanie przejrzystej procedury oraz mechanizmu zgłaszania incydentów przez pracowników do osób odpowiedzialnych za bezpieczeństwo

teleinformatyczne (np. stworzenie skrzynki pocztowej na wzór *incydent@instytucja.gov.pl*).

**REKOMENDACJA 8**: Ujęcie Zespołu CERT.GOV.PL w procedurach reagowania na incydenty komputerowe. Wyznaczenie osób kontaktowych do nawiązywania współpracy i bieżącej wymiany informacji. Stworzenie dedykowanego adresu mailowego, stanowiącego punkt kontaktowy dla Rządowego Zespołu Reagowania na Incydenty Komputerowe CERT.GOV.PL w sprawach związanych z incydentami bezpieczeństwa (np. *incydent@instytucja.gov.pl*).

**REKOMENDACJE TECHNICZNE**

**REKOMENDACJA 1**: Dokonywanie cyklicznych przeglądów infrastruktury sieciowej. 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.

**REKOMENDACJA 2**: Wdrożenie dedykowanych maszyn z systemami firewall (w tym także warstwy aplikacji), IDS/IPS, monitoringu. Przygotowanie infrastruktury do eliminacji ruchu anonimizowanego w przypadku wystąpienia zagrożenia (np. TOR, Open-Proxy, Anon-Proxy, Anon-VPN). Wymuszenie ciągłej aktualizacji mechanizmów bezpieczeństwa.

**REKOMENDACJA 3**: Systematyczne dokonywanie przeglądu konfiguracji kluczowych urządzeń sieciowych znajdujących się w infrastrukturze instytucji oraz bieżące aktualizowanie rozwiązań sprzętowych i programowych.

**REKOMENDACJA 4**: Ustanowienie dostępu do wewnętrznej poczty wyłącznie z określonych i zaufanych adresów IP lub z wykorzystaniem rozwiązań VPN. Eliminacja lub, w wyjątkowych i uzasadnionych przypadkach, ograniczenie dostępu do poczty wewnętrznej poprzez stronę znajdującą się w sieci Internet.

**REKOMENDACJA 5**: Ustanowienie dostępu do funkcji administracyjnych posiadanych zasobów oraz do elektronicznego systemu obiegu dokumentów wyłącznie lokalnie lub w wyjątkowych i uzasadnionych przypadkach poprzez dostęp zdalny przy użyciu rozwiązań VPN.

**REKOMENDACJA 6**: Wprowadzenie na urządzeniach sieciowych blokowania dostępu do złośliwych domen i adresów.

**REKOMENDACJA 7**: Wprowadzenie blokady bezpośredniego dostępu stacji roboczych do sieci Internet - zapewnienie pełnej rozliczalności działań użytkowników oraz możliwości pełnej kontroli nad administrowanym środowiskiem.

**REKOMENDACJA 8**: Usunięcie, w jak najszerszym możliwym zakresie środowisk stwarzających poprzez swoją specyfikę duże zagrożenie (np. środowiska JAVA, Flash), ze stacji roboczych lub ograniczenie do stacji roboczych, gdzie korzystanie z tego środowiska jest niezbędne.

**REKOMENDACJA 9**: Prowadzenie analizy nieudanych prób logowania oraz analiza anomalii sieciowych.

**REKOMENDACJA 10**: Wprowadzenie polityk użytkowania kont o różnych poziomach uprawnień (zarówno administracyjnych jak i użytkowych).

**REKOMENDACJA 11**: Prowadzenie przeglądów oprogramowania użytkowanego na stacjach roboczych w sieci instytucji (odinstalowanie oprogramowania służącego do celów innych niż służbowe), a także wdrożenie mechanizmów kontrolujących w trybie ciągłym list oprogramowania dopuszczonego do stosowania w sieci.

**REKOMENDACJA 12**: Wdrożenie systemu identyfikacji użytkowników w oparciu o certyfikaty elektroniczne.

**REKOMENDACJA 13**: Wdrożenie centralnego systemu antywirusowego i antyspamowego oraz wymuszanie ich ciągłej aktualizacji na stacjach roboczych lub serwerach na podstawie list RBL czy też aktualizacji wydawanych przez wytwórcę użytkowanego oprogramowania.

**REKOMENDACJA 14**: Wdrożenie centralnego systemu korelacji danych tzw. SIEM, który m.in. umożliwia centralne zarządzanie bezpieczeństwem TI oraz pozwala na wykrywanie ataków poprzez analizę anomalii.

**REKOMENDACJA 15**: Stworzenie i właściwa konfiguracja środowisk izolowanych tzw. sandbox, które m.in. pozwalają na izolację potencjalnie niebezpiecznych plików.

**REKOMENDACJA 16**: Wprowadzenie stosownych polityk bezpieczeństwa w stosunku do stacji komputerowych użytkowników np. polityki nośników pamięci (ograniczenie wyłącznie do nośników służbowych) lub innych urządzeń podłączanych do komputera.

**REKOMENDACJA 17**: Wprowadzenie polityki użytkowania oprogramowania wyłącznie w najnowszej wersji. Dbałość o regularną aktualizację oprogramowania poprzez stosowanie odpowiednich aktualizacji oraz poprawek bezpieczeństwa. Tam gdzie to możliwe, wymuszenie aktualizacji automatycznych oprogramowania na stacjach roboczych użytkowników.

**REKOMENDACJA 18**: Wdrożenie mechanizmów mających na celu ograniczenie użytkowania służbowych stacji roboczych do celów prywatnych (np. korzystanie z prywatnej poczty e-mail, portali społecznościowych itp.), z wyjątkiem uzasadnionych przypadków biznesowych (np. public relations, human resources itp.).

**REKOMENDACJA 19**: Wprowadzenie odpowiedniej polityki konstruowania „silnych" haseł dla użytkowników nieobjętych identyfikacją o certyfikaty elektroniczne. Wymuszenie okresowej zmiany haseł.

**REKOMENDACJA 20**: Wdrożenie systemu logowania zdarzeń w sieci teleinformatycznej i wypracowanie procedury archiwizacji zebranych logów (co najmniej za okres 6 miesięcy wstecz). W przypadku korzystania z usług outsourcingowych (np. hosting witryny WWW) należy zobowiązać usługodawcę do wdrożenia wyżej wymienionych zaleceń.

**REKOMENDACJA 21**: Precyzyjne uregulowanie kwestii dotyczących dokonywania okresowych testów bezpieczeństwa oraz audytów. Określenie wymogów oraz zasad przeprowadzania testów bezpieczeństwa na systemach przygotowanych do wdrożenia w instytucji i/lub przed wprowadzaniem istotnych zmian do systemów już funkcjonujących. Podjęcie działań mających na celu wdrożenie wniosków poaudytowych.

**REKOMENDACJA 22:** Uregulowanie kwestii wykonywania oraz magazynowania kopii zapasowych danych, których utrata może zakłócić lub uniemożliwić funkcjonowanie instytucji oraz kopii zapasowych infrastruktury teleinformatycznej, która może zostać uruchomiona w przypadku awarii infrastruktury podstawowej.

**REKOMENDACJE EDUKACYJNO-INFORMACYJNE**

**REKOMENDACJA 1**: Opracowanie systemu szkoleń dla wszystkich użytkowników kont w sieci Instytucji w celu podnoszenia ogólno pojętego bezpieczeństwa korzystania z komputera oraz sieci Internet w tym:

- obowiązkowo dla nowo przyjmowanych pracowników z obowiązujących procedur w firmie związanych z bezpiecznym użytkowaniem systemów TI;
- okresowo dla wszystkich pracowników.

**REKOMENDACJA 2**: Prowadzenie kampanii edukacyjnych dostępnych dla wszystkich użytkowników. Zapewnienie mechanizmu wysyłki wiadomości pocztowych do wszystkich pracowników posiadających konta w systemie celem np. ostrzeżenia przed niebezpieczeństwem.

**REKOMENDACJA 3**: Opracowanie systemu szkoleń specjalistycznych dla osób odpowiedzialnych za bezpieczeństwo teleinformatyczne.

**REKOMENDACJA 4**: Stworzenie modelu komunikacji z zarządem instytucji w celu okresowego informowania o stanie bezpieczeństwa infrastruktury TI.

## Spis Tabel



## Spis Wykresów