UNIWERSYTET Andrzeja Frycza Modrzewskiego w Krakowie

BEZPIECZEŃSTWO TEORIA I PRAKTYKA SECURITY THEORY AND PRACTICE

e-ISSN 2451-0718
ISSN 1899-6264

2025
Nr 2 (LIX)

Copyright© 2025 by the Authors
Opublikowano w wolnym dostępie (Open Access) na licencji CC BY-NC-ND 4.0

https://doi.org/10.48269/2451-0718-btip-2025-2-006
Data wpłynięcia: 28.05.2025
Data akceptacji: 21.07.2025

Analiza zagrożeń polskiej infrastruktury cybernetycznej w latach 2010–2023. Część II lata 2017–2023

Marceli Herman

dr, Uniwersytet Andrzeja Frycza Modrzewskiego w Krakowie
https://orcid.org/0009-0004-8709-4632

Michał Sitarski

dr, Uniwersytet Andrzeja Frycza Modrzewskiego w Krakowie
https://orcid.org/0009-0008-9119-9663

Wprowadzenie

Publikacja stanowi kontynuację analizy zagrożeń środowiska cybernetycznego Polski w latach 2010–2016[1]. W artykule przedstawiono statystyki incydentów prowadzone przez zespół CSIRT GOV, zidentyfikowano zagrożenia infrastruktury cybernetycznej (takie jak podszycia, kampanie phishingowe, podmiany stron internetowych), a także podatności wykryte przez zespół CSIRT GOV oraz aktywności grup APT (*Advanced Persistent Threats*). Publikacja wskazuje na występującą tendencję wzrostową i eskalację w zakresie alarmów wykrywanych przez system wczesnego ostrzegania o zagrożeniach w sieci internetowej ARAKIS 3.0 GOV.

[1] M. Herman, *Analiza zagrożeń polskiej infrastruktury cybernetycznej w latach 2010–2024. Część I: Lata 2010–2016*, „Bezpieczeństwo. Teoria i Praktyka" 2024, nr 3, s. 111–124, https://doi.org/10.48269/2451-0718-btip-2024-3-008.

Główne pytanie badawcze artykułu sformułowano następująco: Jakie rodzaje zagrożeń miały największy wpływ na pogorszenie funkcjonowania infrastruktury cybernetycznej kraju w latach 2017–2023?

Celem niniejszej publikacji jest przedstawienie zagrożeń cybernetycznych zaistniałych we wskazanym okresie, a także zwrócenie uwagi na ich zmiany i rozwój determinowany zjawiskami o charakterze społecznym, politycznym czy militarnym. Zdefiniowano zagrożenia dla infrastruktury cybernetycznej kraju, przedstawiono statystyki zgłoszeń faktycznych i potwierdzonych incydentów cybernetycznych w latach 2017–2023 oraz badania poziomu bezpieczeństwa witryn internetowych administracji publicznej z zastosowaniem systemu wczesnego ostrzegania ARAKIS GOV.

Statystyki zgłoszeń faktycznych oraz potwierdzonych incydentów cybernetycznych w latach 2017–2023

Rządowy Zespół Reagowania na Incydenty Komputerowe CERT.GOV.PL jako podmiot odpowiedzialny za monitorowanie zagrożeń cyberbezpieczeństwa i incydentów komputerowych, w roku 2017 odnotował 28 281 zgłoszeń o potencjalnym wystąpieniu incydentów komputerowych, co względem roku 2016 stanowiło wzrost o 8327 zgłoszeń. Ze wszystkich odnotowanych zgłoszeń w 2017 r. status faktycznego naruszenia bezpieczeństwa teleinformatycznego instytucji (czyli incydentu) miało 5819 przypadków, co wglądem roku 2016 stanowiło spadek o 3469 zdarzeń faktycznych[2]. W 2018 r. zaobserwowano ponad 11-proc. wzrost liczby zgłoszeń o potencjalnym wystąpieniu incydentów względem 2017 r. (31 865 zgłoszeń), a status potwierdzonego incydentu otrzymało 6236 przypadków, o 417 więcej niż w roku poprzednim[3]. Znaczny wzrost zgłoszeń incydentów teleinformatycznych przypadł w roku 2019 (226 914 zgłoszeń), co względem 2018 r. stanowiło wzrost o ponad 610%. Za przyczynę takiego stanu rzeczy uznano zwiększenie świadomości użytkowników sieci teleinformatycznych na zagrożenia, a co za tym idzie także dostosowywanie nowych form działania cyberprzestępców. Liczba zdarzeń zarejestrowanych jako faktyczny incydent wynosiła 12 405, co stanowiło wzrost o ponad 50% w porównaniu z 2018 r.[4]. W roku 2020 Zespół CSIRT GOV odnotował 246 107 zgłoszeń dotyczących potencjalnego wystąpienia incydentu teleinformatycznego, z czego 23 309 okazało się faktycznym incydentem. Powyższe wartości stanowiły tylko 8-proc wzrost liczby zgłoszeń) oraz aż 87-proc. wzrost liczby zdarzeń kwalifikowanych jako incydent faktyczny

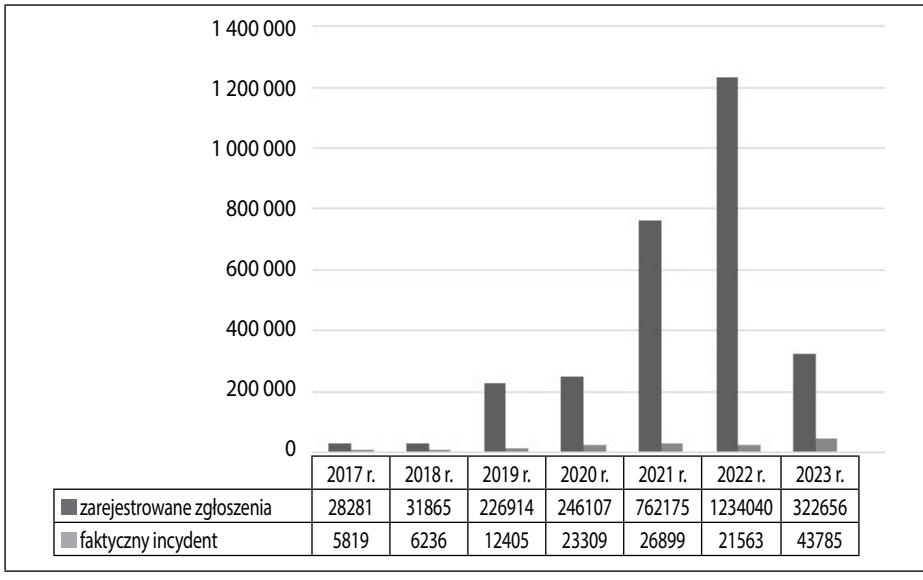
[2] Rządowy Zespół Reagowania na Incydenty Komputerowe CERT.GOV.PL [dalej: CERT.GOV.PL], *Raport o stanie bezpieczeństwa cyberprzestrzeni RP w 2017 r.*, Warszawa 2018, s. 11.

[3] CERT.GOV.PL, *Raport o stanie bezpieczeństwa cyberprzestrzeni RP w 2018 r.*, Warszawa 2019, s. 11.

[4] CERT.GOV.PL, *Raport o stanie bezpieczeństwa cyberprzestrzeni RP w 2019 r.*, Warszawa 2020, s. 8.

względem 2019 r.[5]. Ponad trzykrotnie większe wartości zgłoszeń i potwierdzonych incydentów odnotowano w 2021 r.: 762 175 zgłoszeń dotyczących potencjalnego wystąpienia incydentu teleinformatycznego, z czego 26 899 okazało się faktycznym incydentem. Zdaniem autorów analizowanego Raportu, determinantem takiego stanu faktycznego było wzmocnienie wykrywalności zagrożeń przez system ARAKIS GOV[6]. W 2022 r. zarejestrowanych zostało łącznie 1 234 040 zgłoszeń, co stanowiło 62-proc. wzrost względem roku poprzedniego. Jako faktyczne incydenty zakwalifikowano 21 563 zdarzeń. Tak znaczny wzrost determinowany był przeprowadzoną aktualizacją bazy zagrożeń systemu ARAKIS GOV oraz Internet ARAKIS GOV, co wzmocniło ich identyfikację[7]. W roku 2023 zostało zarejestrowanych 322 656 zgłoszeń, spośród których 43 785 zakwalifikowano jako faktyczne incydenty bezpieczeństwa teleinformatycznego. Przedmiotowe wartości odzwierciedlały 73-proc. spadek w liczby zgłoszeń oraz 100-proc. wzrost liczby faktycznych incydentów względem roku 2022[8].

Wykres 1. Statystyki zgłoszeń i incydentów w latach 2017–2023



	2017 r.	2018 r.	2019 r.	2020 r.	2021 r.	2022 r.	2023 r.
zarejestrowane zgłoszenia	28281	31865	226914	246107	762175	1234040	322656
faktyczny incydent	5819	6236	12405	23309	26899	21563	43785

Źródło: opracowanie własne na podstawie Raportów o stanie bezpieczeństwa cyberprzestrzeni RP w latach 2017–2023.

[5] CERT.GOV.PL, *Raport o stanie bezpieczeństwa cyberprzestrzeni RP w 2020 r.*, Warszawa 2021, s. 4.

[6] CERT.GOV.PL, *Raport o stanie bezpieczeństwa cyberprzestrzeni RP w 2021 r.*, Warszawa 2022, s. 5.

[7] CERT.GOV.PL, *Raport o stanie bezpieczeństwa cyberprzestrzeni RP w 2022 r.*, Warszawa 2023, s. 10–11.

[8] *Ibidem*, s. 10.

Na wykresie 1 zauważalny jest ponadto systematyczny wzrost liczby wydarzeń zakwalifikowanych jako faktyczne incydenty w latach 2017–2023. Przyczyny takiego stanu faktycznego dotyczą kwestii prowadzonej polityki zagranicznej, obronnej, a także – co najważniejsze – zdarzeń geopolitycznych na arenie międzynarodowej. Powyższe czynniki wpływają na zainteresowanie podmiotów zewnętrznych (służby specjalne państw niesprzymierzonych, ugrupowania hackerskie itp.) polską bądź sojuszniczą infrastrukturą cybernetyczną.

Badanie poziomu bezpieczeństwa witryn internetowych administracji publicznej z zastosowaniem systemu wczesnego ostrzegania ARAKIS GOV (wersje 2.0 oraz 3.0)

ARAKIS 2.0 GOV (oraz późniejsza wersja 3.0) 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”[9].

W 2017 r. w sieciach teleinformatycznych podmiotów uczestniczących w projekcie ARAKIS 2.0 GOV zanotowano łącznie 323 722 095 przepływów. Wygenerowano 347 178 alarmów, wśród których odnotowano 62 292 alarmy mające priorytet pilny (wymagających natychmiastowej reakcji na zagrożenie ze strony administratorów sieci – duże ryzyko przełamania zabezpieczeń); 30 505 alarmów mających priorytet wysoki (wymagających wzmożonej uwagi na zagrożenia określone w alarmie – średnie ryzyko przełamania zabezpieczeń); 15 911 alarmów mających priorytet średni (informacje o dobrze znanym zagrożeniu – małe ryzyko przełamania zabezpieczeń); 238 470 alarmów mających priorytet niski (alarmy informacyjne dotyczące monitorowanej sieci wewnętrznej z siecią Internet)[10].

Wskazać należy, iż każdy z alarmów zawierał dokładne dane techniczne, umożliwiające jego weryfikację. Ponadto był szczegółowo klasyfikowany przez system, który wyróżniał pięć zasadniczych typów: typ 1 – komunikacja do złośliwych adresów (próba nawiązania komunikacji z adresami IP); typ 2 – skanowania (określające kierunek zainteresowania); typ 3 – wykryte znane ataki; typ 4 – wykryte nieopisane ataki; typ 5 – infekcje wewnętrzne. Zainteresowanie atakiem w 2017 r. ukierunkowane było przede wszystkim na instytucje skategoryzowane jako: „infrastruktura krytyczna” – 92%, „urzędy” – 5%, „ministerstwa” – 0,6% (alarmy typu 1). Natomiast wśród alarmów typu 5 najwięcej przepływów zanotowano w: „urzędach” – 42%, „infrastrukturze krytycznej” – 39% i „ministerstwach” – 6,5%. Najwyższe wartości

[9] CERT.GOV.PL, *Raport o stanie bezpieczeństwa cyberprzestrzeni RP w 2017 r.*, *op. cit.*, s. 19.
[10] *Ibidem*.

przepływów w 2017 r. (w celu identyfikacji/eksploitacji) dotyczyły: ataków na usługę SSH, ataków na usługę TELNET, ataków na usługę SMTP, skanowania ICMP (*echo reply*), ataków na aplikacje webowe[11].

W 2018 r. w sieciach teleinformatycznych przy wykorzystaniu systemu ARAKIS 3.0 GOV zanotowano łącznie 319 943 424 przepływów, co wygenerowało 454 207 alarmów. Wśród nich 62 365 miało priorytet pilny, 104 502 – priorytet wysoki, 15 412 – priorytet średni, oraz 271 928 – priorytet niski. Najwięcej przepływów, celem identyfikacji istniejących zasobów teleinformatycznych bądź próby ich eksploitacji, zaobserwowano w wśród alarmów typu 2 (skanowanie) skategoryzowanych jako „urzędy" – 57%, „ministerstwa" – 18%, „infrastruktura krytyczna" – 13%, „służby i wojsko" – 6%. Przepływy ukierunkowano jako: ataki na usługę SSH, skanowanie ICMP (*echo reply*), ataki na usługę TELNET, ataki na aplikacje webowe, ataki na usługę Windows SMB i inne[12].

W 2019 r., odnotowano 1 052 675 641 przepływów przekładających się na wygenerowanie 844 951 alarmów, o różnych stopniach zagrożenia. Priorytet pilny miało 266 135 alarmów, priorytet wysoki – 99 612 alarmów, priorytet średni – 51 721 alarmów, priorytet niski – 427 483 alarmów. Alarmy typu 1 stanowiły 27% zainteresowania podmiotów zewnętrznych, alarmy typu 2 (skanowania) stanowiły aż 50,5% przepływów, alarmy typu 3 (wykryte złośliwe ataki) – 20,1%, alarmy typu 4 (nieopisane ataki) – 1,48%, alarmy stanowiące infekcje wewnętrzne stanowiły 0,7%[13]. Najwięcej przepływów zaobserwowano w wśród alarmów typu 2 (skanowanie) skategoryzowanych jako „urzędy" 32%, „infrastruktura krytyczna" – 31%, „ministerstwa" – 19%, „instytuty" – 10%, „służby i wojsko" – 5%. Najczęściej ataki ukierunkowane były na usługi typu: ICMP (*echo reply*), MSSQL, SMB, oraz RPC[14].

Projekt ARAKIS 3.0 GOV w 2020 r. wskazał aż 1 813 243 995 przepływów, co przekładało się na 1 758 813 wygenerowanych alarmów o zróżnicowanych priorytetach. Wśród zanotowanych alarmów wyróżniono: priorytet pilny – 187 149 alarmów, priorytet wysoki – 67 939 alarmów, priorytet średni – 140 303 alarmy, priorytet niski – 1 363 422 alarmy. Alarmy typu 1 stanowiły 7,34% wszystkich alarmów jako prób nawiązywania komunikacji z adresami IP lub domenami uznanymi za złośliwe. Skanowania (typ 2) stanowiły aż 77% wszystkich przepływów ukierunkowanych na: „urzędy" – 31%, „infrastrukturę krytyczną" – 29%, „instytuty" – 17%, „ministerstwa" – 13,5%, „służby i wojsko" – 5%. Alarmy typu 3 i 4 stanowiły odpowiednio 7,80% oraz 7,22% przepływów. W roku 2020 najczęściej wykorzystywanym elementem rekonesansu był protokół ICMP (*echo reply*), duże zainteresowanie

[11] *Ibidem*, s. 20–21.
[12] CERT.GOV.PL, *Raport o stanie bezpieczeństwa cyberprzestrzeni RP w 2018 r.*, *op. cit.*, s. 20–22.
[13] CERT.GOV.PL, *Raport o stanie bezpieczeństwa cyberprzestrzeni RP w 2019 r.*, *op. cit.*, s. 24.
[14] *Ibidem*, s. 27.

wzbudzała usługa MSSQL powiązaną z portem 1433 oraz port 445 powiązany z usługą SMB, posiadającą wiele znanych podatności[15].

W rok 2021 odnotowano łącznie 1 758 708 908 przepływów, w tym 3 366 360 wygenerowanych przez system alarmów. Wśród zanotowanych alarmów: 1 170 136 o priorytecie pilnym, 99 207 o priorytecie wysokim, 416 987 o priorytecie średnim, oraz 1 680 030 o priorytecie niskim. W 2021 r. alarmy systemu ARAKIS GOV typu 1 (komunikacja do złośliwych adresów) stanowiły 32%, typu 2 (skanowania) – 49% (w tym skategoryzowanych jako „infrastruktura krytyczna" – 31%, „urzędy" – 26%, „instytuty" – 16%, „ministerstwa" – 15%, „służby i wojsko" – 5%). Alarmy typu 3 i 4 (wykryte znane ataki, wykryte nieopisane ataki) stanowiły odpowiednio 4,94% oraz 13,04%. W roku 2021 najczęściej wykorzystywanym elementem rekonesansu był protokół ICMP (*echo reply/request*), a także FTP, SSH, SMB, TELNET.

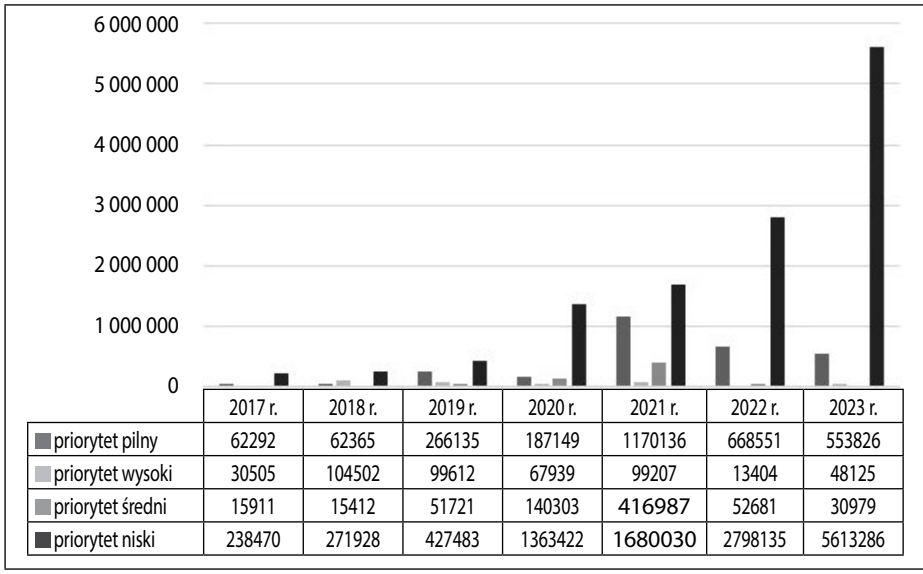
W 2022 r. w sieciach teleinformatycznych projektu ARAKIS GOV odnotowano 2 193 855 851 przepływów, co stanowi 24-proc. wzrost względem roku 2021. Przepływy przełożyły się na wygenerowanie 3 532 771 alarmów o zróżnicowanej skali zagrożenia (4-proc. wzrost względem 2021 r.). Alarmy podzielono zgodnie ze skalą zagrożenia: 668 551 alarmów o priorytecie pilnym, 13 404 o priorytecie wysokim, 52 681 o priorytecie średnim, 2 798 135 o priorytecie niskim[16]. Alarmy charakteryzujące się próbami nawiązywania komunikacji z adresami IP lub domenami uznanymi za złośliwe (typu 1) stanowiły 18%. Ze względu na rozmieszczanie systemu ARAKIS GOV w wielu instytucjach administracji państwowej, wśród alarmów typu 2 najwięcej przepływów zostało zanotowanych w instytucjach skategoryzowanych jako: „urzędy" 30%, „infrastruktura krytyczna" 27%, „służby" 15%, „ministerstwa" 14%, „instytuty" 10%. Nikły wskaźnik procentowy stanowiły alarmy Typu 3 i 4 odpowiednio 0,6% oraz 1% ze wszystkich przepływów. Determinantem powyższego zjawiska może być wygenerowanie sygnatury IDS w oparciu o obserwowaną komunikację do sygnatury IDS która była niewidoczna w systemie. W roku 2022 najczęściej wykorzystywanym elementem rekonesansu był także protokół ICMP (*echo reply/request*), TELNET, SSH, SMB, HTTP[17].

Spadek liczby przepływów w sieciach teleinformatycznych podmiotów uczestniczących w projekcie ARAKIS GOV (o 31% względem roku poprzedzającego) odnotowano w 2023 r. Na 1 501 466 173 przepływów wygenerowano łącznie 6 246 216 alarmów, co stanowi 76-proc. wzrost w stosunku do 2022 r. Priorytet pilny miało 553 826 alarmów, priorytet wysoki – 48 125 alarmów, priorytet średni – 30 979 alarmów, priorytet niski – 5 613 286 alarmów. W 2023 r. alerty systemu ARAKIS GOV typu 1 stanowiły 4% ogółu zarejestrowanych alarmów. Najwięcej przepływów wśród alarmów typu 2 zostało zanotowanych w systemach podmiotów skategoryzowanych

[15] CERT.GOV.PL, *Raport o stanie bezpieczeństwa cyberprzestrzeni RP w 2020 r.*, *op. cit.*, s. 38–43.
[16] CERT.GOV.PL, *Raport o stanie bezpieczeństwa cyberprzestrzeni RP w 2022 r.*, *op. cit.*, s. 80.
[17] *Ibidem*, s. 82–84.

jako: „instytucje" – 42%, „operatorzy infrastruktury krytycznej" – 35%, „urzędy" – 30%, „ministerstwa" – 11%, „służby" – 5%. Alarmy typu 3 i 4 stanowiły odpowiednio 1% oraz 0,1% przepływów. W roku 2023 najczęściej wykorzystywanym elementem rekonesansu były protokoły typu: SSH, TELNET, FTP, SMB, HTTP[18].

Wykres 2. Analiza alarmów wygenerowanych przez system ARAKIS GOV w latach 2017–2023



	2017 r.	2018 r.	2019 r.	2020 r.	2021 r.	2022 r.	2023 r.
priorytet pilny	62292	62365	266135	187149	1170136	668551	553826
priorytet wysoki	30505	104502	99612	67939	99207	13404	48125
priorytet średni	15911	15412	51721	140303	416987	52681	30979
priorytet niski	238470	271928	427483	1363422	1680030	2798135	5613286

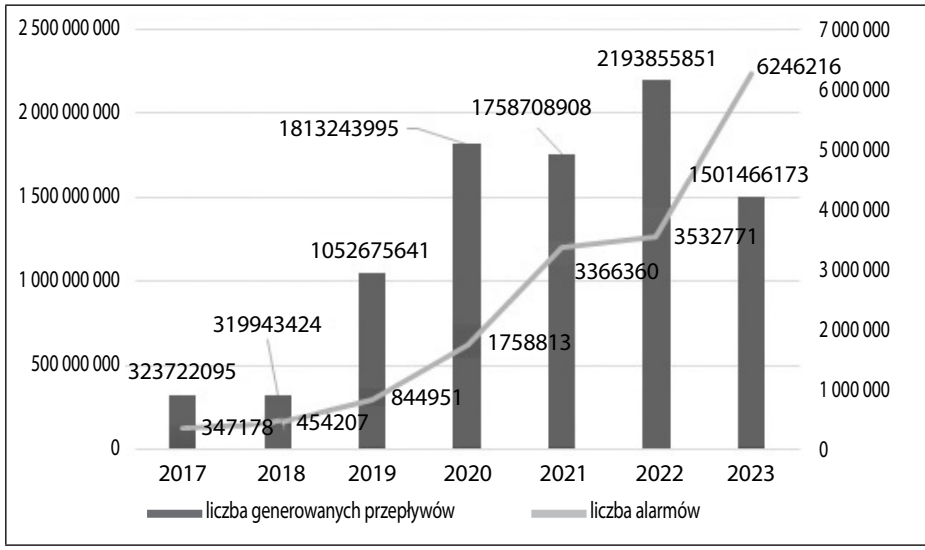
Źródło: opracowanie własne na podstawie Raportów o stanie bezpieczeństwa cyberprzestrzeni RP w latach 2017–2023.

Wykres 2 pokazuje tendencję wzrostową alarmów o niskim priorytecie. Liczba alarmów w pozostałych rodzajach priorytetowości wykazuje skoki, które mogą być warunkowane zdarzeniami geopolitycznymi na świecie, polityką bezpieczeństwa RP, a także modernizacją techniczną oprogramowania i systemów infrastruktury cybernetycznej w kraju.

Na wykresie 3 przedstawiony został stosunek liczby alarmów do liczby odnotowanych przepływów w infrastrukturze cybernetycznej. Wykres wskazuje zdecydowany wzrost liczby alarmów w badanym okresie, z zaznaczeniem dużego skoku na przestrzeni lat 2022 i 2023. Liczby generowanych przepływów w latach 2017 i 2018, a także w latach 2020 i 2021 były zbliżone. W 2023 r. nastąpił ponad 30-proc. spadek wykrywalności przepływowej względem roku 2022, mający związek ze zmianą sposobu tworzenia alarmów i zmniejszeniem liczby alarmów typu *false positive*.

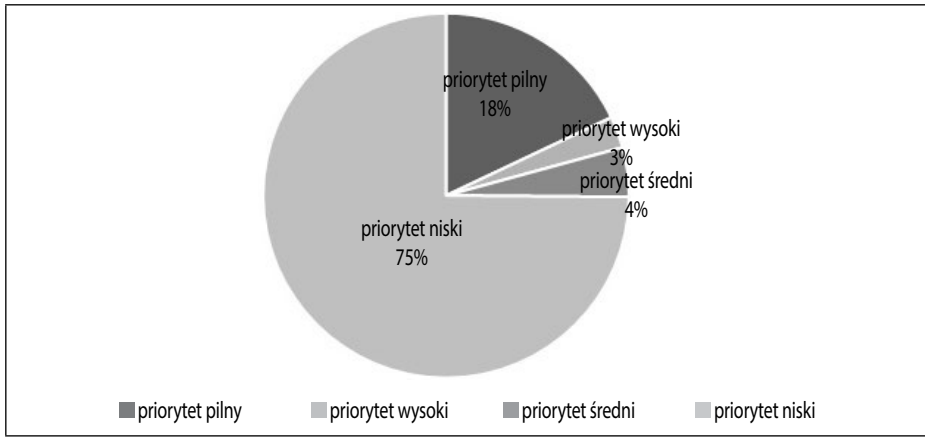
[18] CERT.GOV.PL, *Raport o stanie bezpieczeństwa cyberprzestrzeni RP w 2023 r.*, Warszawa 2024, s. 80–84.

Wykres 3. Porównanie liczby odnotowanych przepływów i generowanych alarmów w sieci cybernetycznej w latach 2017–2023



Źródło: opracowanie własne na podstawie Raportów o stanie bezpieczeństwa cyberprzestrzeni RP w latach 2017–2023.

Wykres 4. Procentowy rozkład skali zagrożeń cybernetycznych w latach 2017–2023.



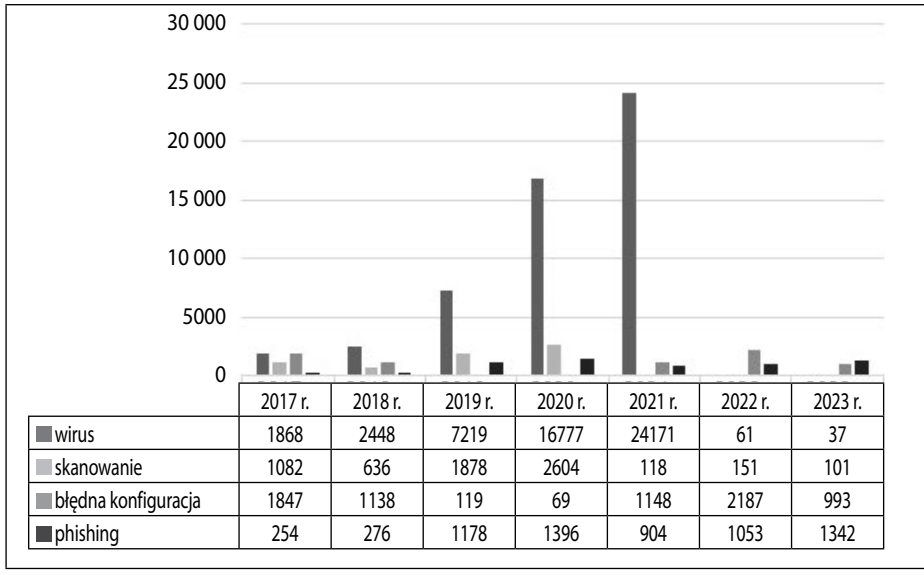
Źródło: opracowanie własne na podstawie Raportów o stanie bezpieczeństwa cyberprzestrzeni RP w latach 2017–2023.

Wykres 4 obrazuje procentowy rozkład skali zagrożeń cybernetycznych w latach 2017–2023 wg kategorii priorytetowości. Jak widać najliczniejszymi zagrożeniami dla infrastruktury cybernetycznej są zagrożenia o niskim priorytecie, a najrzadziej występują najbardziej realne i znaczące zagrożenia cybernetyczne, mające priorytet wysoki.

Zagrożenia polskiej infrastruktury cybernetycznej w latach 2017–2023

W 2017 r. zasadnicze zagrożenie infrastruktury cybernetycznej w Polsce stanowiły wirusy, czyli infekcje urządzeń (stacji roboczej, serwerów, sieci). Ataki z zastosowaniem zainfekowanych załączników do wiadomości e-mail wykorzystywały elementy inżynierii społecznej. Błędna konfiguracja urządzenia stanowiła kolejne zagrożenie dla poprawności działania systemów komputerowych wykazane w 2017 r. – odnotowano 1847 takich incydentów. Innym rodzajem zagrożeń były próby nawiązania połączeń sieciowych z sieciami botnet (tzw. klient sieci botnet). Polegało to na odpowiednim wykorzystaniu systemów wspomagających, przeprowadzeniu próby połączenia urządzenia roboczego z skompromitowanymi adresami lub domenami, np. serwerów C&C. Inną formą ataków cybernetycznych z wykorzystaniem inżynierii społecznej były próby wyłudzenia wrażliwych danych lub wykonania nieautoryzowanej czynności (np. transakcji bankowej na podany rachunek zagraniczny)[19].

Wykres 5. Statystyka incydentów w latach 2017–2023.



	2017 r.	2018 r.	2019 r.	2020 r.	2021 r.	2022 r.	2023 r.
wirus	1868	2448	7219	16777	24171	61	37
skanowanie	1082	636	1878	2604	118	151	101
błędna konfiguracja	1847	1138	119	69	1148	2187	993
phishing	254	276	1178	1396	904	1053	1342

Źródło: opracowanie własne na podstawie Raportów o stanie bezpieczeństwa cyberprzestrzeni RP w latach 2017–2023.

Wykres 5 przedstawia statystykę występowania rodzajów zagrożeń i incydentów w latach 2017–2023 r. Duży spadek w kategorii „wirus" odnotowany w latach 2022 i 2023 mógł być warunkowany wprowadzeniem i utrzymywaniem

[19] CERT.GOV.PL, *Raport o stanie bezpieczeństwa cyberprzestrzeni RP w 2017 r.*, *op. cit.*, s. 13–14.

stopnia alarmowego CHARLIE-CRP w przestrzeni cybernetycznej. Powyższe wynikało z przeprowadzonej analizy zagrożeń w napiętej sytuacji geopolitycznej w regionie, której konsekwencją było wzmocnienie działań cyberprzestępczych wykonywanych przez grupy bądź inne podmioty powiązane ze służbami państw obcych.

Podsumowanie

Optymalizację bezpieczeństwa cybernetycznego w Polsce zasadniczo wzmocniło opracowanie i przyjęcie ustawy z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa, wskazującej podmioty odpowiedzialne za zapewnienie bezpieczeństwa infrastruktury oraz nakładającej obowiązki i prawa na operatorów, dostawców oraz podmioty publiczne w zakresie cyberbezpieczeństwa. Ustawa stanowi zasadniczy akt prawny regulujący problematykę cyberbezpieczeństwa w kraju. Jej zapisy dokonały przeobrażenia (funkcjonującego już) Zespołu Reagowania na Incydenty Komputerowe CERT.GOV.PL w Zespół Reagowania na Incydenty Bezpieczeństwa Komputerowego CSIRT GOV, i stworzyły dodatkowo CSIRT MON[20] (prowadzony przez Ministra Obrony Narodowej) oraz CSIRT NASK[21] (prowadzony przez Naukową i Akademicka Sieć Komputerową)[22]. Odpowiadając na postawione pytanie badawcze (tj. jakie rodzaje zagrożeń miały największy wpływ na pogorszenie funkcjonowania infrastruktury cybernetycznej kraju w latach 2017–2023), zaznaczyć należy, że najczęściej występującymi zagrożeniami cybernetycznymi były incydenty należące do kategorii wirus (wzrost względem 2017 r. o 31%), błędna konfiguracja urządzenia, w której odnotowano 1138 incydentów (spadek względem 2017 r. o 38%) oraz skanowanie (spadek względem 2017 r. o 41%). Ostatni rodzaj incydentów polegał na wysyłaniu pakietów TCP do dowolnych typów urządzeń sieciowych w celu weryfikacji dostępności portów oraz usług, co było ukierunkowane na przeprowadzenie złamania zabezpieczeń systemów teleinformatycznych[23]. W 2019 r. Zespół Reagowania na Incydenty Bezpieczeństwa Komputerowego CSIRT GOV jako zasadnicze incydenty naruszające bezpieczeństwo infrastruktury wskazał kampanie APT oraz Botnet Qbot/Mirai. Zaawansowane długotrwałe ataki – APT (*Advanced Persistent Threats*) polegały

[20] Zespół Reagowania na Incydenty Bezpieczeństwa Komputerowego działający na poziomie krajowym, prowadzony przez Ministra Obrony Narodowej, funkcjonujący w ramach Dowództwa Komponentu Wojsk Obrony Cyberprzestrzeni.

[21] Zespół Reagowania na Incydenty Bezpieczeństwa Komputerowego działający na poziomie krajowym, prowadzony przez Naukową i Akademicką Sieć Komputerową – Państwowy Instytut Badawczy.

[22] Ustawa z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa, tekst jedn. Dz.U. z 2024 r., poz. 1077.

[23] CERT.GOV.PL, *Raport o stanie bezpieczeństwa cyberprzestrzeni RP w 2018 r.*, *op. cit.*, s. 14.

na przesyłaniu zainfekowanego pliku pakietu Microsoft Office pocztą elektroniczną. Przesłany plik wykorzystywał podatność CVE-2017-0199 i w efekcie końcowym uruchamiał plik wykonywalny w formacie EXE, będący tak naprawdę oprogramowaniem typu RAT (*Remote Access Trojan*). Inną możliwością ataku przy zastosowaniu APT było przesyłanie wiadomości phishingowych lub tworzenie skompromitowanych witryn internetowych w celu gromadzenia haseł do poczty lub systemu ofiary/celu ataku. Ponadto w 2019 r. przełamano zabezpieczenia routerów CISCO użytkowanych przez instytucje administracji rządowej. Przeprowadzona analiza danych urządzeń sieciowych wykazała nieautoryzowane połączenia wychodzące z routera brzegowego, a także infekcję złośliwym oprogramowaniem typu Botnet Qbot/Mirai. Atak charakteryzował się wyszukiwaniem otwartych portów i usług tj. SSH, TELNET, HTTP na różnorodnych urządzeniach (router, switch, kamera itp.) dostępnych w sieci WAN. Po zalogowaniu na urządzeniu z wykorzystaniem domyślnych loginów lub podatności następowało dalsze pobieranie zainfekowanego oprogramowania. Ostatnim etapem było oczekiwanie na polecenia wysyłane z serwerów C&C w celu rozpoczęcia ataków np. w formie DoS/DDoS ukierunkowanych na adres IP celu[24]. Jednym z modułów ataku było zablokowanie protokołu TELNET oraz stałe wyszukiwanie i usuwanie procesów konkurencyjnego malware'u[25].

W roku 2020 pojawiały się incydenty sklasyfikowane podobnie jak w 2019 r., tj.: wirus (wzrost o 132%), skanowanie (wzrost o 39%), phishing (wzrost o 18%). Zagrożenia wirusowe stanowiły aż 72% ogółu wszystkich incydentów, co spowodowane było zwiększeniem skuteczności identyfikacji złośliwego oprogramowania przy zastosowaniu systemów detekcji, sygnatury oraz przepływów sieciowych. Incydenty zaklasyfikowane jako skanowanie wynikały z alarmów ARAKIS 3.0 GOV dotyczących złośliwego lub podejrzanego ruchu skierowanego na adresację podmiotów podległych CSIRT GOV. Kolejnym rodzajem zagrożeń były kampanie phishingowe, prowadzone z wykorzystaniem metod socjotechnicznych i mogące stanowić fazę inicjującą bardziej zaawansowanych i rozleglejszych ataków, ukierunkowanych na przejecie kontroli i uzyskanie dostępu do określonej infrastruktury teleinformatycznej celu. Słabość systemu teleinformatycznego była kolejnym zagrożeniem, a wynikała z błędów konfiguracyjnych lub braku zaimplikowanych procedur bezpieczeństwa (aktualizacji oraz weryfikacji poprawnie wdrożonych rozwiązań teleinformatycznych)[26].

Główne rodzaje zagrożeń dla sieci instytucji państwowych w roku 2021 sklasyfikowano jako wirusy (wzrost o 44% względem 2020 r.), podatność oraz socjotechnikę. W tym roku odnotowano kilka krytycznych podatności, tj. ProxyLogon

[24] CERT.GOV.PL, *Raport o stanie bezpieczeństwa cyberprzestrzeni RP w 2019 r.*, *op. cit.*, s. 36–40.

[25] *Analiza bota Mirai oraz jego wariantów*, CERT Polska, https://cert.pl/posts/2020/03/analiza-bota-mirai-oraz-jego-wariantow [dostęp: 2.03.2025].

[26] CERT.GOV.PL, *Raport o stanie bezpieczeństwa cyberprzestrzeni RP w 2020 r.*, *op. cit.*, s. 12–13.

i Proxyshell (dotyczące oprogramowania Microsoft Exchange) oraz Apache Log4j. Podatność dotyczyła umieszczenia na serwerze webowym spreparowanego pliku ASPX, działającego jako *webshell*. Przekazywane parametry w wysyłanym żądaniu używane były do wykonywania kodu po stronie serwera. Zespół CSIRT GOV realizował zadania polegające na identyfikacji podatności, obsłudze incydentów, publikacji ostrzeżeń oraz wydawaniu rekomendacji specjalistycznych[27].

Wszelkie zagrożenia infrastruktury cybernetycznej w 2022 r. warunkowane były niestabilną sytuacja geopolityczną w Europie, w szczególności konfliktem zbrojnym w Ukrainie. Determinacja Rzeczpospolitej Polskiej w kwestii pomocy Ukrainie potęgowała potencjalny i faktyczny poziom zagrożeń bezpieczeństwa cyberprzestrzeni RP. Zidentyfikowane agresywne działania w obszarze cyberprzestrzeni i ryzyko wystąpienia zdarzenia o charakterze terrorystycznym wymusiły na organach administracji państwowej wprowadzenie na obszarze całego terytorium RP pierwszego stopnia alarmowego ALFA-CRP[28]. W związku z dalszą eskalacją zagrożeń wprowadzony został trzeci stopień alarmowy w obszarze cyberbezpieczeństwa – CHARLIE-CRP[29]. Obecnie (stan na grudzień 2025) obowiązuje drugi stopień alarmowy w obszarze cyberbezpieczeństwa – BRAVO-CRP, wprowadzony 1 marca 2024 r.[30] i następnie przedłużony do 28 lutego 2026 r.[31]. W 2022 r. odnotowano znaczny wolumen kampanii DDoS realizowanych przez grupy haktywistyczne (m.in. NoName057(16), Killnet, CyberArmia Ludowa). Ataki ukierunkowane były na ograniczenie dostępności witryn internetowych atakowanych podmiotów oraz świadczonych przez nie usług. Powyższe zjawisko stanowiło element kampanii propagandowych (informacje rozpowszechniane za pośrednictwem mediów społecznościowych), co wzmacniało oddziaływanie i skuteczność grup przy jednoczesnej próbie wskazania słabości atakowanych celów. Celem ataków DDoS w 2022 r. były także strony internetowe Narodowego Banku Polskiego, Policji czy operatorów sieci komórkowych[32]. W roku 2023 dominowały dwie kategorie zasadniczych zagrożeń: kampanie socjotechniczne oraz ataki DDoS, mające cyberprzestępczy oraz cyberofensywny charakter. Motywem cyberprzestepczym była chęć uzyskania nieuprawnionego dostępu do danych wrażliwych użytkowników, dostępu do sieci i systemów celem dalszej eksploitacji czy eksfiltracji danych. Działania cyberofensywne

[27] *Ibidem*, s. 11–21.

[28] Zarządzenie Prezesa Rady Ministrów nr 3 z dnia 18 stycznia 2022 r. w sprawie wprowadzenia stopnia alarmowego CRP.

[29] Zarządzenie Prezesa Rady Ministrów nr 40 z dnia 21 lutego 2022 r. w sprawie wprowadzenia stopnia alarmowego CRP.

[30] Zarządzenie Prezesa Rady Ministrów nr 17 z dnia 29 lutego 2024 r. w sprawie wprowadzenia stopnia alarmowego CRP.

[31] Zarządzenie Prezesa Rady Ministrów nr 69 z dnia 18 listopada 2025 r. w sprawie wprowadzenia stopnia alarmowego CRP.

[32] CERT.GOV.PL, *Raport o stanie bezpieczeństwa cyberprzestrzeni RP w 2022 r.*, *op. cit.*, s. 24–27.

dotyczyły realizacji ataków typu *state-sponsored*, wykorzystujących podatności typu *zero-day*. Zespół CSIRT GOV odnotowywał wysoką intensywność kampanii socjotechnicznych z wektorem ataku ukierunkowanym na podmioty administracji państwowej, podmioty świadczące usługi publiczne czy operatorów infrastruktury krytycznej[33]. Zwiększona liczba ataków typu DDoS warunkowana była działalnością grup haktywistycznych.

Bibliografia

Opracowania

Analiza bota Mirai oraz jego wariantów, CERT Polska, https://cert.pl/posts/2020/03/analiza-bota-mirai-oraz-jego-wariantow [dostęp: 2.03.2025].

Banasiński C., Rojszczak M., *Cyberbezpieczeństwo*, Wolters Kluwer, Warszawa 2020.

Chmielewski Z., *Polityka publiczna w zakresie ochrony cyberprzestrzeni w UE i państwach członkowskich*, „Studia z Polityki Publicznej" 2016, nr 2, s. 103–128, https://doi.org/10.33119/KSzPP.2016.2.5.

Czaplicki K. *et al.*, *Ustawa o krajowym systemie cyberbezpieczeństwa – komentarz*, Wolters Kluwer, Warszawa 2019.

Czym jest PHISHING i jak nie dać się nabrać na podejrzane wiadomości e-mail oraz SMS-y?, GOV.pl, https://www.gov.pl/web/baza-wiedzy/czym-jest-phishing-i-jak-nie-dac-sie-nabrac-na-podejrzane-widomosci-e-mail-oraz-sms-y [dostęp: 3.05.2025].

Herman M., *Analiza zagrożeń polskiej infrastruktury cybernetycznej w latach 2010–2024. Część I: Lata 2010–2016*, „Bezpieczeństwo. Teoria i Praktyka" 2024, nr 3, s. 111–124, https://doi.org/10.48269/2451-0718-btip-2024-3-008.

Kuc B., Ścibiorek Z., *Zarys metodologii nauk o bezpieczeństwie*, Wydawnictwo Adam Marszałek, Toruń 2018.

Liderman K., *Bezpieczeństwo informacyjne. Nowe wyzwania*, PWN, Warszawa 2017.

Stallings W., Brown L., *Bezpieczeństwo systemów informatycznych. Zasady i praktyka*, t. 1–2, tłum. Z. Płoski, R. Meryk, Helion, Gliwice 2019.

Tanner N.H., *Blue Team i cyberbezpieczeństwo. Zestaw narzędzi dla specjalistów od zabezpieczeń w sieci*, tłum. A. Łapuć, Helion, Warszawa 2021.

Akty prawne i dokumenty

Ustawa z dnia 10 czerwca 2016 r. o działaniach antyterrorystycznych, tekst jedn. Dz.U. z 2024 r., poz. 92.

Rozporządzenie Prezesa Rady Ministrów z dnia 25 lipca 2016 r. w sprawie zakresu przedsięwzięć wykonywanych w poszczególnych stopniach alarmowych i stopniach alarmowych CRP, tekst jedn. Dz.U. z 2022 r., poz. 2065.

Ustawa z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa, tekst jedn. Dz.U. z 2024 r., poz. 1077.

Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2019/881 z dnia 17 kwietnia 2019 r. w sprawie ENISA (Agencji Unii Europejskiej ds. Cyberbezpieczeństwa) oraz certyfikacji cyberbezpieczeństwa w zakresie technologii informacyjno-komunikacyjnych oraz uchylenia rozporządzenia (UE) nr 526/2013 (akt o cyberbezpieczeństwie), Dz.U. L 151 z 7.06.2019.

[33] CERT.GOV.PL, *Raport o stanie bezpieczeństwa cyberprzestrzeni RP w 2023 r.*, *op. cit.*, s. 17–19.

Zarządzenie Prezesa Rady Ministrów nr 3 z dnia 18 stycznia 2022 r. w sprawie wprowadzenia stopnia alarmowego CRP.
Zarządzenie Prezesa Rady Ministrów nr 40 z dnia 21 lutego 2022 r. w sprawie zmiany stopnia alarmowego CRP.
Zarządzenie Prezesa Rady Ministrów nr 17 z dnia 29 lutego 2024 r. w sprawie wprowadzenia stopnia alarmowego CRP.
Zarządzenie Prezesa Rady Ministrów nr 69 z dnia 18 listopada 2025 r. w sprawie wprowadzenia stopnia alarmowego CRP.
Strategia Cyberbezpieczeństwa Rzeczypospolitej Polskiej na lata 2019–2024, Ministerstwo Cyfryzacji, GOV.pl, 30.12.2019, https://www.gov.pl/web/cyfryzacja/strategia-cyberbezpieczenstwa-rzeczypospolitej-polskiej-na-lata-2019-2024 [dostęp: 03.05.2025].
Rządowy Zespół Reagowania na Incydenty Komputerowe CERT.GOV.PL, *Raport o stanie bezpieczeństwa cyberprzestrzeni RP w 2017 r.*, Warszawa 2018.
Rządowy Zespół Reagowania na Incydenty Komputerowe CERT.GOV.PL, *Raport o stanie bezpieczeństwa cyberprzestrzeni RP w 2018 r.*, Warszawa 2019.
Rządowy Zespół Reagowania na Incydenty Komputerowe CERT.GOV.PL, *Raport o stanie bezpieczeństwa cyberprzestrzeni RP w 2019 r.*, Warszawa 2020.
Rządowy Zespół Reagowania na Incydenty Komputerowe CERT.GOV.PL, *Raport o stanie bezpieczeństwa cyberprzestrzeni RP w 2020 r.*, Warszawa 2021.
Rządowy Zespół Reagowania na Incydenty Komputerowe CERT.GOV.PL, *Raport o stanie bezpieczeństwa cyberprzestrzeni RP w 2021 r.*, Warszawa 2022.
Rządowy Zespół Reagowania na Incydenty Komputerowe CERT.GOV.PL, Raport o stanie bezpieczeństwa cyberprzestrzeni RP w 2022 r., Warszawa 2023.
Rządowy Zespół Reagowania na Incydenty Komputerowe CERT.GOV.PL, Raport o stanie bezpieczeństwa cyberprzestrzeni RP w 2023 r., Warszawa 2024.

Analiza zagrożeń polskiej infrastruktury cybernetycznej w latach 2010–2023. Część II lata 2017–2023

Streszczenie

Rzeczpospolita Polska jako kraj członkowski Unii Europejskiej, NATO, Organizacji Narodów Zjednoczonych, Organizacji Bezpieczeństwa i Współpracy w Europie, Światowej Organizacji Handlu oraz innych, w tym polsko-ukraińskiej współpracy wojskowej, jest narażona na liczne i wszechstronne zagrożenia cybernetyczne, jak również znajduje się w kręgu zainteresowania podmiotów zewnętrznych (grup hakerskich, służb specjalnych itp.). Dlatego w celu optymalizacji bezpieczeństwa cybernetycznego w Polsce konieczne jest wypracowanie zmian o charakterze prawnym, organizacyjnym i technologicznym, zapewniających pożądany poziom bezpieczeństwa cyberprzestrzeni oraz jej użytkowników i gwarantujących przy tym odpowiednią kooperację poszczególnych elementów systemu bezpieczeństwa państwa.

Główne pytanie badawcze artykułu sformułowano następująco: Jakie rodzaje zagrożeń miały największy wpływ na pogorszenie funkcjonowania infrastruktury cybernetycznej kraju w latach 2017–2023?

Celem niniejszej publikacji jest przedstawienie zagrożeń cybernetycznych zaistniałych we wskazanym okresie, a także zwrócenie uwagi na ich zmiany i rozwój determinowany zjawiskami o charakterze społecznym, politycznym czy militarnym. Zdefiniowano zagrożenia dla infrastruktury cybernetycznej kraju, przedstawiono statystyki zgłoszeń

faktycznych i potwierdzonych incydentów cybernetycznych w latach 2017–2023 oraz badania poziomu bezpieczeństwa witryn internetowych administracji publicznej z zastosowaniem systemu wczesnego ostrzegania ARAKIS GOV.

Słowa kluczowe: cyberbezpieczeństwo, cyberprzestrzeń, incydent cybernetyczny, infrastruktura cybernetyczna, system bezpieczeństwa państwa, zagrożenie cybernetyczne

An Analysis of Threats to the Polish Cybersecurity Infrastructure Between the Years 2010 and 2023. Part II: The Years 2017–2023

Abstract

As a member state of the European Union, the collective security institutions of NATO, the UN, the OSCE, the WTO and other organizations, which include its involvement in Polish-Ukrainian military cooperation, the Republic of Poland faces numerous and multilateral cybersecurity threats. It is also exposed to the activity of external bodies (such as hacker groups and intelligence agencies). In order to optimize cybersecurity in Poland, it is necessary to introduce changes of a legal, organizational and technical nature that will provide cyberspace and its users with the desired level of security, alongside a guarantee of appropriate cooperation in individual elements of the security system of the state.

This study is a continuation of an analysis of the threats to Poland's cyber environment presented in the article *An analysis of threats to the Polish cybersecurity infrastructure between the years 2010 and 2023. Part I: the years 2010–2016* published in 2024 in issue 3 of the quarterly "Bezpieczeństwo. Teoria i Praktyka".The aim of this paper is to describe cybersecurity threats that arose between the years 2017 and 2023, and also to pay attention to their transformation and development, the latter being shaped by social, political and military factors.

The main research question is of a descriptive nature and numerous threats to the cybersecurity infrastructure of the country are mentioned. Special attention is paid to three fundamental issues, namely, threats to Polish cybersecurity between the years 2017 and 2023, statistics concerning cybersecurity incidents that were actually reported and confirmed during this period, as well as investigations into the level of security of government websites using the early warning system ARAKIS-GOV. Statistical and comparative research methods are employed in order to analyze quantitative data and the features of the phenomena under investigation, with the aim of identifying similarities and differences.

A comparative method was used to compare types of cybersecurity threat, the number of cybersecurity incidents that were actually reported and confirmed, and the level of security of websites, paying attention to the amount of traffic recorded in relation to previous years. A statistical method was used to analyze quantitative changes in the number of reports and incident alerts generated by the ARAKIS-GOV system, the amount of traffic recorded compared to the alerts generated in the network, as well as changes in the incident statistics for the years 2017–2023. The main research issue was to determine what types of threat had the greatest influence on the deterioration in the functioning of Poland's cybersecurity infrastructure between the years 2017 and 2023.

Keywords: cybersecurity, cyberspace, cyber incident, cyber infrastructure, state security system, cyber threat