

Od phishingu po sabotaż – ewolucja cyberzagrożeń wobec Polski. Wnioski z raportu CSIRT GOV za 2024 rok

Monika Stodolnik

Autorka niezależna

 <https://orcid.org/0009-0000-5319-7968>

Cyberprzestrzeń stanowiąca dziś arenę rywalizacji międzynarodowej podlega dynamicznym przemianom, a ostatnie lata pokazały jej znaczenie w kontekście państwowych działań niemilitarnych. Umożliwia ona prowadzenie operacji o charakterze wywiadowczym, sabotażowym, dezinformacyjnym, a także operacji wpływu. W tej rzeczywistości cyberbezpieczeństwo powinno być integralnym elementem odporności państwa – obok bezpieczeństwa militarnego, energetycznego czy ekonomicznego.

Polska jako członek wspólnot międzynarodowych, a przede wszystkim jako podmiot aktywnie wspierający Ukrainę w obliczu agresji Federacji Rosyjskiej, znajduje się w grupie państw szczególnie narażonych na cyberataki. *Raport o stanie bezpieczeństwa cyberprzestrzeni RP za rok 2024*, opracowany przez Zespół Reagowania na Incydenty Bezpieczeństwa Komputerowego CSIRT GOV działający w strukturach Agencji Bezpieczeństwa Wewnętrznego, stanowi cenne źródło wiedzy o aktualnych trendach,

wektorach ataków oraz poziomie przygotowania administracji publicznej i operatorów infrastruktury krytycznej.

Analiza raportu przedstawiona w artykule pozwala na sformułowanie wniosków dotyczących nie tylko technicznych aspektów ataków, lecz także zagrożeń dla instytucji i społeczeństwa związanych ze współczesnymi zjawiskami w cyberprzestrzeni.

Rola CSIRT GOV w krajowym systemie cyberbezpieczeństwa

Zespół CSIRT GOV pełni funkcję jednego z trzech krajowych zespołów powołanych do życia ustawą o krajowym systemie cyberbezpieczeństwa (dalej: ustawa o KSC)¹, odpowiedzialnych za rozpoznawanie i wykrywanie zagrożeń godzących w systemy administracji publicznej oraz infrastruktury krytycznej i zapobieganie im. CSIRT GOV realizuje zadania nałożone zarówno ustawą o KSC, jak i ustawą o Agencji Bezpieczeństwa Wewnętrznego oraz Agencji Wywiadu². Łączy tym samym kompetencje techniczno-operacyjne i analityczne, odpowiadając za monitorowanie cyberprzestrzeni Rzeczypospolitej Polskiej, reagowanie na incydenty i koordynowanie działań w zakresie jej ochrony.

CSIRT GOV jest elementem operacyjnym krajowego systemu cyberbezpieczeństwa i bezpośrednio wspiera realizację zadań państwa w obszarze ochrony informacji, przeciwdziałania zagrożeniom cybernetycznym, będącym główną częścią zagrożeń hybrydowych, oraz zapewnienia ciągłości funkcjonowania infrastruktury krytycznej. Jego umiejscowienie w strukturze ABW pozwala łączyć bieżącą analizę techniczną incydentów z oceną ich szerszego kontekstu, w tym wpływu na bezpieczeństwo narodowe, z uwzględnieniem perspektywy kontrwywiadowczej. Ocena ta obejmuje również aspekt prewencji – dla administracji państwowej i operatorów infrastruktury krytycznej.

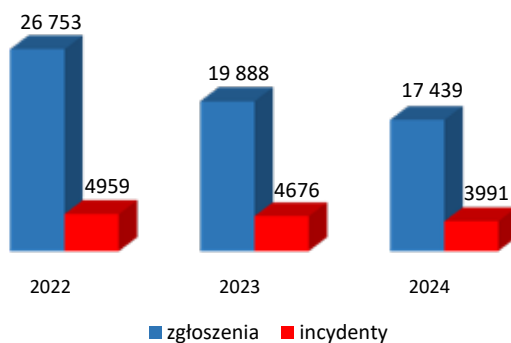
¹ Ustawa z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa (t.j. DzU z 2024 r. poz. 1077, ze zm.).

² Ustawa z dnia 24 maja 2002 r. o Agencji Bezpieczeństwa Wewnętrznego oraz Agencji Wywiadu (t.j. DzU z 2025 r. poz. 902, ze zm.).

Kontekst cyberbezpieczeństwa w 2024 roku

Przez cały rok 2024 obowiązywał podwyższony stopień alarmowy CRP (w styczniu i lutym był to CHARLIE-CRP, a od marca – BRAVO-CRP³). Wiązało się to z utrzymywaniem stałej gotowości do reagowania na potencjalne działania o charakterze terrorystycznym, zgodnie z ustawą o działaniach antyterrorystycznych⁴. W szerszym ujęciu oznaczało to stałą gotowość do reagowania na potencjalne incydenty o charakterze hybrydowym i cyberwywiadowczym, ze względu na wspólne wektory ataków wykorzystywane we wszystkich tych przypadkach.

W 2024 r. CSIRT GOV zarejestrował 17 439 zgłoszeń o potencjalnych incydentach, z czego 3991 uznano za faktyczne naruszenia bezpieczeństwa systemów teleinformatycznych (rysunek 1)⁵. Choć te liczby wskazują na spadek względem roku 2023, to autorzy raportu zwracają uwagę, że nie wynika to ze zmniejszenia liczby zagrożeń, lecz z poprawy kompetencji i świadomości użytkowników oraz z wdrażania w instytucjach skuteczniejszych mechanizmów ochrony⁶.



Rysunek 1. Liczba zgłoszeń i incydentów zarejestrowanych przez CSIRT GOV w latach 2022–2024.

Źródło: CSIRT GOV, *Raport o stanie bezpieczeństwa cyberprzestrzeni RP w 2024 roku*, <https://csirt.gov.pl/download/3/221/RaportostaniebezpieczenstwacyberprzestrzeniRPw2024.pdf>, s. 10 [dostęp: 1 X 2025].

³ CSIRT GOV, *Raport o stanie bezpieczeństwa cyberprzestrzeni RP w 2024 roku*, <https://csirt.gov.pl/download/3/221/RaportostaniebezpieczenstwacyberprzestrzeniRPw2024.pdf>, s. 5 [dostęp: 1 X 2025].

⁴ Ustawa z dnia 10 czerwca 2016 r. o działaniach antyterrorystycznych (t.j. DzU z 2025 r. poz. 194).

⁵ CSIRT GOV, *Raport o stanie bezpieczeństwa cyberprzestrzeni...*, s. 10.

⁶ Tamże.

Te dane obrazują zwiększającą się odporność podmiotów będących we właściwości CSIRT GOV. Czynnikiem sprzyjającym wzrostowi tej odporności są:

- 1) powstrzymywanie ataków na poziomie brzegowym sieci, czyli skuteczne filtrowanie i blokowanie prób naruszeń, zanim dotrą one do właściwych systemów teleinformatycznych. W przypadku ataków socjotechnicznych z wykorzystaniem poczty elektronicznej oznacza to stosowanie zaawansowanych filtrów antyspamowych i mechanizmów reputacyjnych na bramkach pocztowych; w odniesieniu do ataków siłowych – wdrażanie rozwiązań takich jak blokowanie adresów IP (tzw. blacklisting) czy limity prób logowania, a w przypadku zagrożeń wykorzystujących znane podatności – bieżące aktualizowanie oprogramowania i eliminowanie luk bezpieczeństwa;
- 2) wzrost świadomości użytkowników i pracowników administracji, którzy coraz częściej potrafią rozpoznać i powstrzymać próby ataków, w których wykorzystuje się socjotechnikę (np. phishing, spearphishing, vishing), jeszcze na etapie kontaktu z wiadomością lub podejrzanym linkiem, przed wejściem z nimi w interakcję. To efekt rosnącej liczby szkoleń, komunikatów ostrzegawczych i wewnętrznych procedur reagowania na incydenty. W 2024 r. CSIRT GOV przeprowadził szkolenia i warsztaty dla blisko 1900 osób, co stanowi prawie czterokrotny wzrost w stosunku do roku 2023⁷;
- 3) rozwój wewnętrznych struktur odpowiedzialnych za cyberbezpieczeństwo, takich jak zespoły SOC (Security Operations Center) lub jednostki ds. bezpieczeństwa teleinformatycznego w instytucjach publicznych. Pozwala to na skuteczniejszą obsługę incydentów na poziomie lokalnym, bez konieczności angażowania CSIRT GOV;
- 4) zacieśnienie współpracy i koordynacji międzyinstytucjonalnej, zarówno w ramach trzech krajowych zespołów CSIRT (GOV, MON, NASK), jak i między administracją publiczną i operatorami infrastruktury krytycznej. Wymiana informacji o zagrożeniach i dystrybucja wskaźników kompromitacji (ang. *indicators of compromise*) umożliwiają wcześniejsze wykrywanie prób ataków oraz szybsze reagowanie na incydenty. Na podstawie zgłoszeń incydentów oraz analizy wskaźników kompromitacji z jednego przypadku

⁷ Tamże.

CSIRT GOV opracowuje ostrzeżenia i rekomendacje dla całego swojego obszaru kompetencyjnego, co pozwala zapobiegać rozprzestrzenianiu się zagrożeń⁸;

- 5) wykorzystywanie testów bezpieczeństwa i audytów jako działań proaktywnych, które w sposób bezpieczny i kontrolowany pozwalają na identyfikację słabych punktów systemów, zanim zostaną one wykorzystane przez grupy przestępcze i cyberofensywne. Tego typu działania, prowadzone przez jednostki znajdujące się w strukturze danego podmiotu, zewnętrzne firmy świadczące usługi testów penetracyjnych oraz przez CSIRT GOV, stanowią istotny element prewencji i podnoszenia ogólnej odporności cyfrowej podmiotów administracji publicznej i operatorów infrastruktury krytycznej. W 2024 r. CSIRT GOV przeprowadził serię testów penetracyjnych w instytucjach administracji publicznej. Obejmowały one m.in. ocenę konfiguracji systemów, skuteczności mechanizmów obronnych i jakości zarządzania podatnościami. Wnioski z tych testów posłużyły do opracowania zaleceń dla poszczególnych jednostek⁹.

Charakterystyka działań cyberofensywnych w kontekście cyberbezpieczeństwa Rzeczypospolitej Polskiej

Wzrost kompetencji i zdolności podmiotów pozostających we właściwości CSIRT GOV nie eliminuje wszystkich zagrożeń. Analiza incydentów odnotowanych w 2024 r. wskazuje, że mimo zauważalnej poprawy poziomu zabezpieczeń i świadomości użytkowników, cyberprzestrzeń Polski nadal pozostaje miejscem aktywności podmiotów o charakterze przestępczym, wywiadowczym i hakywistycznym¹⁰. Zdarzenia będące wynikiem działań grup wspieranych przez państwa są jednym z elementów składających się na incydenty dzielone przez CSIRT GOV na dwie kategorie określane jako „socjotechnika” oraz „atak”. Pierwsza z kategorii wskazuje głównie na phishing wymierzony w użytkowników organizacji pozostających w za interesowaniu aktorów, druga dotyczy prób oraz skutecznych incydentów

⁸ Tamże, s. 15.

⁹ Tamże, s. 96.

¹⁰ Tamże, s. 54.

przełamania zabezpieczeń infrastruktury teleinformatycznej atakowanych podmiotów¹¹.

W 2024 r. aktywność grup sponsorowanych przez państwa oraz pro-rosyjskich kolektywów hakywistycznych utrzymywała się na wysokim poziomie. Międzynarodowe raporty umieszczają Polskę wśród czołowych krajów europejskich pod względem liczby ataków sponsorowanych, motywowanych społecznie lub politycznie. Z raportu Microsoftu, firmy z sektora IT, wynika, że w 2024 r. Polska znalazła się w pierwszej trójce w Europie¹². Z kolei według analityków firmy technologicznej Radware wśród państw Europy Polska zajmowała drugie miejsce, za Ukrainą, pod względem liczby ataków DDoS¹³ inicjowanych przez prorosyjskich hakywistów¹⁴. To potwierdza, że Polska, jako aktywny sojusznik Ukrainy i wschodnia granica NATO i Unii Europejskiej, była szczególnie narażona na działania asymetryczne i hybrydowe w cyberprzestrzeni.

Raport CSIRT GOV wskazuje na dominację ataków z kierunku rosyjskiego, szczególnie przeprowadzanych przez grupę APT28 (stanowiącą jednostkę wojskową nr 26165 w 85. Głównym Centrum Zadań Specjalnych rosyjskiego wywiadu wojskowego GRU¹⁵) oraz grupę APT2916¹⁶ (podległą Służbie Wywiadu Zagranicznego Federacji Rosyjskiej)¹⁷. Omawiane przypadki odnotowane w cyberprzestrzeni RP znajdują potwierdzenie także w przywołanych w tym artykule zagranicznych publikacjach, które pokazują szerszy kontekst działalności tych grup.

¹¹ Tamże, s. 12–13.

¹² *Microsoft Digital Defense Report 2024, The foundations and new frontiers of cybersecurity*, <https://cdn-dynmedia-1.microsoft.com/is/content/microsoftcorp/microsoft/final/en-us/microsoft-brand/documents/Microsoft%20Digital%20Defense%20Report%202024%20%281%29.pdf>, s. 13 [dostęp: 19 III 2025].

¹³ Atak DDoS (ang. *distributed denial of service*, rozproszona odmowa usługi) – skoordynowane przeciążenie zasobów systemu lub usługi poprzez dużą liczbę jednoczesnych żądań pochodzących z różnych urządzeń, co ma uniemożliwić prawidłowe działanie.

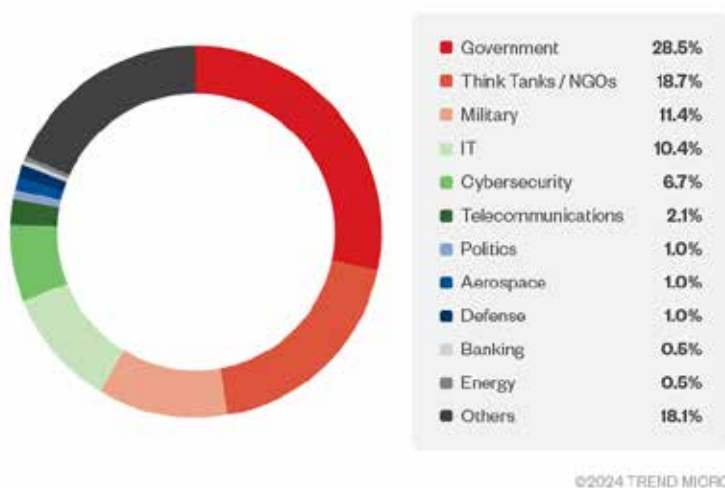
¹⁴ *2024 Global Threat Analysis Report, Executive Summary*, https://www.cisco.com/c/dam/m/en_in/events/security-conclave-2024/radware-threat-report-summary-2024.pdf, s. 9 [dostęp: 2 X 2025].

¹⁵ *Działania rosyjskiej służby specjalnej GRU wymierzone w zachodnie podmioty logistyczne oraz przedsiębiorstwa technologiczne*, <https://www.gov.pl/attachment/e9e86877-2ba0-478e-be36-f20d68474f37>, s. 4 [dostęp: 14 X 2025].

¹⁶ APT29, MITRE ATT&CK, <https://attack.mitre.org/groups/G0016/> [dostęp: 14 X 2025].

¹⁷ CSIRT GOV, *Raport o stanie bezpieczeństwa cyberprzestrzeni...*, s. 56.

Kampania grupy APT29, znanej również jako Earth Koshchei, wykorzystująca pliki konfiguracji połączenia RDP (ang. *remote desktop protocol*), z dużym prawdopodobieństwem (zgodnie z ustaleniami analityków Microsoftu dokonanymi na podstawie nazw zarejestrowanych domen¹⁸) była adresowana m.in. do podmiotów rządowych państw europejskich, szczególnie do ministerstw spraw zagranicznych i ministerstw obrony, struktur NATO, a także do ukraińskich sektorów: obrony, energii i telekomunikacji (rysunek 2). Wpisuje się to jednoznacznie w kontekst działania służby wywiadowczej państwa prowadzącego wojnę z Ukrainą oraz działalność hybrydową wobec państw NATO, a lista potencjalnych adresatów kampanii pokrywa się z dotychczas notowanymi¹⁹.



Rysunek 2. Odsetek domen zarejestrowanych przez grupę APT29 z podziałem na branże.

Źródło: *Earth Koshchei Coopts Red Team Tools in Complex RDP Attacks*, Trend Micro, 17 XII 2024 r., https://www.trendmicro.com/en_us/research/24/1/earth-koshchei.html [dostęp: 14 X 2025].

¹⁸ *Midnight Blizzard conducts large-scale spear-phishing campaign using RDP files*, Microsoft Threat Intelligence, 29 X 2024 r., <https://www.microsoft.com/en-us/security/blog/2024/10/29/midnight-blizzard-conducts-large-scale-spear-phishing-campaign-using-rdp-files/> [dostęp: 14 X 2025].

¹⁹ *Threat profile: APT29*, https://blackpointcyber.com/wp-content/uploads/2024/06/Threat-Profile-APT29_Blackpoint-Adversary-Pursuit-Group-APG_2024.pdf, s. 4 [dostęp: 2 X 2025].

Wśród zagrożeń ze strony grupy APT28 dominowały ataki socjotechniczne, w tym polegające na wyłudzeniu danych logowania do poczty elektronicznej oraz infekowaniu złośliwym oprogramowaniem wykradającym wrażliwe informacje ze stacji roboczych. Wyróżniono także ataki wykorzystujące różnego rodzaju podatności systemów teleinformatycznych²⁰. W kontekście teleinformatyki „podatności” oznaczają słabości systemów, którymi atakujący może się posłużyć do przeprowadzenia skutecznego ataku²¹. Należy jednak podkreślić, że to pojęcie nie odnosi się wyłącznie do błędów oprogramowania zarejestrowanych w bazie CVE (ang. Common Vulnerabilities and Exposures), lecz obejmuje także błędy konfiguracji, zachowania użytkowników oraz niezamierzone cechy oprogramowania, które mogą zostać wykorzystane w sposób sprzeczny z ich przeznaczeniem²².

Na przykład słabym punktem systemu może być użycie prostych lub powtarzalnych haseł, co bywa wyzyskiwane w atakach siłowych na panele logowania. Brak filtrowania ruchu pochodzącego z anonimizujących sieci VPN²³ lub TOR²⁴ również stanowi istotną słabość, ułatwiającą atakującemu ukrycie źródła działań. W analizowanych przypadkach odnotowano także wykorzystanie podatności umożliwiających przeprowadzenie ataku DCSync²⁵, który pozwala na uzyskanie poświadczeń domenowych²⁶. Z kolei pewne funkcje systemowe, takie jak mechanizmy nadawania uprawnień do folderów poczty elektronicznej w usłudze Microsoft Exchange, mogą być użyte zgodnie z ich konstrukcją, lecz w sposób złośliwy i służyć eskalacji uprawnień lub eksfiltracji danych²⁷. Tak szeroki zakres podatności

²⁰ CSIRT GOV, *Raport o stanie bezpieczeństwa cyberprzestrzeni...*, s. 57–66.

²¹ *Vulnerability management, Understanding vulnerabilities*, National Cyber Security Centre, <https://www.ncsc.gov.uk/collection/vulnerability-management/understanding-vulnerabilities> [dostęp: 10 X 2025].

²² Tamże.

²³ Virtual Private Network – usługa szyfrowanego tunelu pomiędzy urządzeniem użytkownika a serwerem pośredniczącym, maskująca rzeczywisty adres IP i lokalizację użytkownika.

²⁴ The Onion Router – sieć anonimizująca, przekierowująca ruch sieciowy przez dużą liczbę szyfrowanych węzłów.

²⁵ Atak DCSync – technika, w której atakujący podszywa się pod kontroler domeny Active Directory i żąda synchronizacji danych, uzyskując w ten sposób skróty kryptograficzne poświadczeń do wszystkich kont w domenie.

²⁶ CSIRT GOV, *Raport o stanie bezpieczeństwa cyberprzestrzeni...*, s. 65.

²⁷ Tamże.

oznacza, że cyberodporność organizacji zależy nie tylko od bieżącej aktualizacji oprogramowania, lecz także od właściwej konfiguracji środowiska, dyscypliny użytkowników oraz rozumienia, w jaki sposób funkcjami systemowymi może posłużyć się przeciwnik.

Grupa APT28 wykorzystywała te środki w atakach zarówno na podmioty w Polsce, jak i w innych państwach, w tym należących do NATO. W maju 2025 r. zostało to zaraportowane we wspólnym dokumencie służb Stanów Zjednoczonych, Wielkiej Brytanii, Niemiec, Czech, Polski, Australii, Kanady, Danii, Estonii, Francji i Holandii²⁸. Dokument ten stanowi rozwinięcie opisu przedstawionej przez CSIRT GOV aktywności GRU wobec podmiotów realizujących zadania na rzecz wsparcia Ukrainy w wojnie z Rosją, a także przedsiębiorstw technologicznych i jednocześnie prezentuje inny – obok działalności sabotażowej²⁹ – wymiar obecności GRU w państwach zachodnich oraz w Ukrainie (rysunek 3).



Rysunek 3. Lokalizacja geograficzna podmiotów, w które były wymierzone działania GRU.

Źródło: *Działania rosyjskiej służby specjalnej GRU wymierzone w zachodnie podmioty logistyczne oraz przedsiębiorstwa technologiczne*, Serwis Rzeczypospolitej Polskiej, <https://www.gov.pl/attachment/e9e-86877-2ba0-478e-be36-f20d68474f37>, s. 7 [dostęp: 14 X 2025].

²⁸ *Działania rosyjskiej służby specjalnej GRU...*, s. 7.

²⁹ A. Jawor, „Agenci jednorazowego użytku” rosyjskiego GRU. „Tajna” kampania sabotażu w Europie, *CyberDefence24*, 3 X 2025 r., <https://cyberdefence24.pl/armia-i-sluzby/agenci-jednorazowego-uzytku-rosyjskiego-gru-tajna-kampania-sabotazu-w-europie> [dostęp: 14 X 2025].

Wśród zagrożeń analizowanych przez CSIRT GOV wskazano również aktywność grup powiązanych z Chińską Republiką Ludową, które w 2024 r. prowadziły działania wywiadowcze wobec państw członkowskich Unii Europejskiej. Koncentrowała się ona na pozyskiwaniu informacji z obszarów: naukowo-technologicznego, energetycznego oraz administracji publicznej. Ataki odnotowane w Polsce zostały przeprowadzone przez dwie grupy – Volt Typhoon³⁰ oraz APT15³¹. Ponadto zidentyfikowano sieć przejętych przez chińskich cyberprzestępców urządzeń sieciowych firmy TP-Link. Użyto jej do anonimizacji ruchu w atakach na usługi Microsoftu³². Działania te wpisują się w długofalową strategię pozyskiwania w sposób ukryty informacji o dużym znaczeniu dla przemysłu i gospodarki, realizowaną w celu wzmocnienia potencjału technologicznego i konkurencyjności Chin na arenie międzynarodowej.

Na uwagę zasługuje także aktywność podmiotów powiązanych z Republiką Białorusi, które z dużym prawdopodobieństwem działają we współpracy ze służbami Federacji Rosyjskiej. W 2024 r. obserwowano działania grupy UNC1151, prowadzącej dwa rodzaje działalności – dezinformacyjną oraz wywiadowczą³³. Jej kampanie obejmowały wiadomości phishingowe podszywające się pod panele logowania do poczty elektronicznej najpopularniejszych polskich dostawców – Interii, Onetu, Wirtualnej Polski. Chodziło o wyłudzenie danych logowania, przejęcie kont i zbudowanie infrastruktury potrzebnej do akcji dezinformacyjnych. Aby prowadzić działalność szpiegowską, infekowano komputery szkodliwym oprogramowaniem pozwalającym na przejęcie pełnej kontroli nad urządzeniem. Dokonywano tego za pośrednictwem wiadomości e-mail. Aktywność tej grupy jest obserwowana od co najmniej 2017 r.³⁴, co świadczy o długotrwałym, rozpoznawczym charakterze działań i ukierunkowaniu na destabilizację informacyjną państwa.

³⁰ Volt Typhoon – grupa o atrybucji wskazującej na Chińską Armię Ludowo-Wyzwoleńczą, atakująca infrastrukturę krytyczną państw zachodnich w celu prowadzenia działań wywiadowczych.

³¹ APT15 – grupa cyberofensywna o atrybucji chińskiej, realizująca strategiczne cele wywiadowcze Chin.

³² CSIRT GOV, *Raport o stanie bezpieczeństwa cyberprzestrzeni...*, s. 72–73, 75.

³³ Tamże, s. 69–72.

³⁴ *Ghostwriter Update: Cyber Espionage Group UNC1151 Likely Conducts Ghostwriter Influence Activity*, https://services.google.com/fh/files/misc/ghostwriter_update_report.pdf, s. 8 [dostęp: 14 X 2025].

W raporcie odnotowano także działania prorosyjskich grup hakiwistycznych Beregini i Zarya. Opublikowały one zmanipulowane dane wykradzione z Polskiej Agencji Antydopingowej, aby podważyć wiarygodność polskich sportowców podczas igrzysk olimpijskich w Paryżu³⁵. Działania te są określane jako operacje *hack-and-leak*. Łączą one cyberatak z manipulacją informacyjną, której celem jest wywarcie wpływu na opinię publiczną³⁶.

W przypadku infrastruktury przemysłowej (Operational Technology/Industrial Control Systems) działalność hakiwistyczna coraz częściej obejmuje cele związane z instalacjami użyteczności publicznej, takimi jak oczyszczalnie ścieków, sieci wodociągowe czy przepompownie³⁷. Jest to trend międzynarodowy, obserwowany także w Stanach Zjednoczonych³⁸, Holandii, Francji³⁹ czy Norwegii⁴⁰. W raporcie CSIRT GOV nie podano konkretnych przypadków, wskazano jedynie na nasilenie takich działań. Wśród najbardziej aktywnych kolektywów, pokazujących rezultaty przeprowadzonych ataków na dedykowanych kanałach na platformie Telegram, należy wskazać: Cyber Army of Russia Reborn (CARR), Z-Pentest⁴¹, Sector16 oraz TwoNet⁴². Trzy ostatnie są częścią sojuszu działającego pod przewodnictwem OverFlame (rysunek 4).

³⁵ CSIRT GOV, *Raport o stanie bezpieczeństwa cyberprzestrzeni...*, s. 6.

³⁶ S. Palczewski, *Kampanie hack-and-leak. Czy namieszkają przed wyborami w Polsce?*, Demagog, 17 VIII 2023 r., https://demagog.org.pl/analizy_i_raporty/kampanie-hack-and-leak-czy-namieszkaja-przed-wyborami-w-polsce/ [dostęp: 13 X 2025].

³⁷ CSIRT GOV, *Raport o stanie bezpieczeństwa cyberprzestrzeni...*, s. 55.

³⁸ *Defending OT Operations Against Ongoing Pro-Russia Hactivist Activity*, <https://www.cisa.gov/sites/default/files/2024-05/defending-ot-operations-against-ongoing-pro-russia-hactivist-activity-508c.pdf>, s. 1 [dostęp: 1 X 2025].

³⁹ *Cyber Insight, Sector 16 group*, https://www.orangecyberdefense.com/fileadmin/global/CyberIntelligenceBureau/Gangs_Investigations/Sector16/Sector16Group.pdf, s. 10 [dostęp: 1 X 2025].

⁴⁰ M. Bryant, *Russian hackers seized control of Norwegian dam, spy chief says*, The Guardian, 14 VIII 2025 r., <https://www.theguardian.com/world/2025/aug/14/russian-hackers-control-norwegian-dam-norway> [dostęp: 14 X 2025].

⁴¹ CSIRT GOV, *Raport o stanie bezpieczeństwa cyberprzestrzeni...*, s. 74.

⁴² *Anatomy of a Hactivist Attack: Russian-Aligned Group Targets OT/ICS*, Forescout, 9 X 2025 r., <https://www.forescout.com/blog/anatomy-of-a-hactivist-attack-russian-aligned-group-targets-otics/> [dostęp: 12 X 2025].



Rysunek 4. Grupy hakywistyczne skupione w ramach kolektywu OverFlame.

Źródło: *Anatomy of a Hacktivist Attack: Russian-Aligned Group Targets OT/ICS*, Forescout, 9 X 2025 r., <https://www.forescout.com/blog/anatomy-of-a-hacktivist-attack-russian-aligned-group-targets-otics/> [dostęp: 12 X 2025].

Aktywność tych kolektywów charakteryzuje się wysoką dynamiką. Dochodzi do częstej dezaktywacji kanałów, powstawania nowych grup i sojuszy, a także konfliktów. Jednocześnie wiele wskazuje na to, że za wieloma kolektywami stoi niewielka grupa tych samych osób, które działają na zlecenie rosyjskich służb. Ukraiński instytut Molfar (Molfar Intelligence Institute) opublikował w styczniu 2025 r. dane administratorów i członków grup NoName057(16) oraz DDoSia, prowadzących ataki DDoS przeciwko stronom i usługom internetowym w państwach sprzeciwiających się polityce Federacji Rosyjskiej⁴³. Zidentyfikowana tam Julia Vladimirovna Pankratova wraz z Denisem Olegovichem Dekgtyarenko znaleźli się na liście osób, na które Stany Zjednoczone nałożyły sankcje w związku z rolą, jaką odegrały w atakach grupy hakerskiej CARR na amerykańską infrastrukturę krytyczną⁴⁴. Analitycy Mandiant, amerykańskiej firmy z branży cyberbezpieczeństwa, w swoim raporcie dotyczącym grupy Sandworm

⁴³ *Russian Cyber Army. Who is it?*, Molfar Intelligence Institute, 23 I 2025 r., <https://www.molfar.institute/en/russian-cyber-army/> [dostęp: 12 X 2025].

⁴⁴ *Treasury Sanctions Leader and Primary Member of the Cyber Army of Russia Reborn*, U.S. Department of the Treasury, 19 VII 2024 r., <https://home.treasury.gov/news/press-releases/jy2473> [dostęp: 11 X 2025].

(identyfikowanej jako jednostka wojskowa 74455 Centrum Technologii Specjalnych GRU) wskazali na jej powiązania z kolektywami XakNet, Solntsepek oraz CARR⁴⁵. Z dużym prawdopodobieństwem może to oznaczać, że CARR i grupy działające z nią w sojuszu realizują zadania na zlecenie służb Federacji Rosyjskiej, co podaje w wątpliwość oddolny charakter haktywizmu.

Bezpieczeństwo łańcucha dostaw

Jednym z najważniejszych wniosków raportu CSIRT GOV jest zwrócenie uwagi na rosnące ryzyko związane z podmiotami trzecimi – dostawcami usług IT, firmami outsourcingowymi i wykonawcami (w branży IT nazywanymi kontraktorami, z ang. *contractor*). Incydenty dotyczące łańcucha dostaw pokazują, że bezpieczeństwo organizacji jest tak silne jak najslabsze ogniwo w jej ekosystemie. Restrykcyjne procedury wewnętrzne nie gwarantują bezpieczeństwa, jeśli partnerzy zewnętrzni nie utrzymują odpowiedniego poziomu ochrony⁴⁶. W 2024 r. do incydentów polegających na kompromitacji systemów, eksfiltracji danych i ich publikacji doszło w firmach świadczących usługi z zakresu informatyki i automatyki, np. AIUT Sp. z o.o.⁴⁷ czy Atende S.A.⁴⁸ W 2025 r. były to EuroCert Sp. z o.o.⁴⁹ – dostawca usługi podpisu kwalifikowanego oraz firma ochroniarska Ekotrade Sp. z o.o.⁵⁰ Skutkiem tych działań było upublicznienie danych wrażliwych o pracownikach, klientach i umowach.

⁴⁵ G. Roncone, D. Black, J. Wolfram, T. McLellan, N. Simonian, R. Hall, A. Prokopenkov, D. Perez, L. Aytes, A. Wahlstrom, *APT44: Unearthing Sandworm*, <https://services.google.com/fh/files/misc/apt44-unearthing-sandworm.pdf>, s. 12–13 [dostęp: 19 III 2025].

⁴⁶ CSIRT GOV, *Raport o stanie bezpieczeństwa cyberprzestrzeni...*, s. 113.

⁴⁷ *Incydent bezpieczeństwa, Aiut*, <https://aiut.com/incydent-bezpieczenstwa/> [dostęp: 12 X 2025].

⁴⁸ *Komunikat Atende w związku z upublicznieniem ukradzionych danych*, Atende, 22 X 2024 r., <https://atende.pl/pl/aktualnosci/komunikat-atende-w-zwiazku-z-upublicznieniem-ukradzionych-danych> [dostęp: 12 X 2025].

⁴⁹ *Atak na EuroCert – oświadczenie*, EuroCert, 15 I 2025 r., <https://eurocert.pl/atak-na-eurocert-oswiadczenie/> [dostęp: 12 X 2025].

⁵⁰ *Komunikat dotyczący ataku hakerskiego na infrastrukturę informatyczną Ekotrade Sp. z o.o.*, <https://ekotrade.com.pl/img/rodo/KOMUNIKAT-EKOTRADE-dla-pracownikow.pdf> [dostęp: 12 X 2025].

W kontekście bezpieczeństwa narodowego oznacza to konieczność traktowania łańcucha dostaw jako integralnej części systemu bezpieczeństwa państwa. Regularne audyty bezpieczeństwa, kontrola dostępu zdalnego, zabezpieczenie danych w ruchu i w spoczynku, weryfikacja umów z dostawcami oraz opracowanie planów ciągłości działania powinny być standardem w instytucjach publicznych i przedsiębiorstwach o znaczeniu strategicznym, w tym wśród operatorów infrastruktury krytycznej⁵¹.

Podsumowanie

Analizując raport CSIRT GOV w szerszym kontekście, należy zauważyć, że cyberataki coraz częściej stanowią element prowadzenia konfliktów poniżej progu wojny, czym wpisują się w rosyjską koncepcję wojny nowej generacji. Służą rozpoznaniu, dezinformacji i destabilizacji bez konieczności użycia siły militarnej. W tym sensie cyberbezpieczeństwo jest już nie tylko domeną technologiczną, lecz także strategiczną i polityczną, stanowi bowiem płaszczyznę, na której przecinają się interesy państw, sektora prywatnego i społeczeństwa. Ataki na administrację państwową, infrastrukturę krytyczną czy media publiczne mają wymiar symboliczny i psychologiczny – podważają zaufanie do instytucji państwa, odsłaniając jego słabości, i wywołują szum medialny. Zdolność do szybkiego reagowania, informowania opinii publicznej zgodnie z przyjętymi scenariuszami komunikacji strategicznej oraz przywracania ciągłości działania organizacji jest jednym z najważniejszych wymiarów obronności.

Raport CSIRT GOV potwierdza, że bezpieczeństwo cybernetyczne RP stanowi dziś integralny element bezpieczeństwa narodowego, a jego utrzymanie wymaga synergii działań technicznych, prawnych i organizacyjnych państwa. Skala zagrożeń dla Polski nie maleje, dlatego tak istotne jest, aby zdolność instytucji do ich identyfikacji, ograniczania skutków i budowania odporności stale rosła. Bardzo ważne są współpraca i wymiana informacji. Stale zmieniający się krajowy system cyberbezpieczeństwa, rozszerzany o sektorowe zespoły CSIRT, wraz z zespołami krajowymi, organami właściwymi do spraw cyberbezpieczeństwa, operatorami usług kluczowych oraz pozostałymi instytucjami, musi stanowić tarczę skutecznie chroniącą przed zagrożeniami o charakterze międzynarodowym. Bezpieczeństwo

⁵¹ CSIRT GOV, *Raport o stanie bezpieczeństwa cyberprzestrzeni...*, s. 116.

to proces ciągły, wymagający stałej weryfikacji, audytów i zachowania elastyczności w celu adaptacji do zmieniających się warunków technologicznych i geopolitycznych. Pojawiające się z każdym dniem nowe podatności, techniki ataków, a przede wszystkim rozwój sztucznej inteligencji, która będzie wspierać atakujących w tworzeniu treści phishingowej oraz kolejnych wersji złośliwego oprogramowania, sprawiają, że trzeba zwiększać swoją odporność i zdolność reakcji na pojawiające się zagrożenia. Jest to istotne jak nigdy wcześniej.

Dynamicznie zmieniający się charakter zagrożeń w cyberprzestrzeni unaocznia pilną potrzebę rezygnacji z modelu reaktywnego na rzecz działań ukierunkowanych na budowanie odporności cyberprzestrzeni RP. Powinny one polegać przede wszystkim na wdrażaniu kompleksowych rozwiązań o charakterze systemowym, a także na doskonaleniu wewnętrznych regulacji organizacyjnych. Kierunek ten znajduje odzwierciedlenie w projektowanych zmianach legislacyjnych, zwłaszcza w nowelizacji ustawy o KSC oraz ustawy o zarządzaniu kryzysowym. Ich wejście w życie w 2025 r. ma na celu poprawę koordynacji działań i wymiany informacji, uwzględnienie wrażliwości łańcuchów dostaw oraz podniesienie ogólnej odporności instytucjonalnej państwa na incydenty w cyberprzestrzeni. Skuteczność tych rozwiązań będzie w dużej mierze zależeć od stopnia ich wdrożenia oraz od zdolności do adaptacji w obliczu dalszej ewolucji cyberzagrożeń.

Monika Stodolnik

Funkcjonariusz Agencji Bezpieczeństwa Wewnętrznego.

Kontakt: monika.stodolnik@abw.gov.pl