OCHRONA OBIEKTÓW INFRASTRUKTURY KRYTYCZNEJ – W ŚWIETLE ZAGROŻEŃ WOJENNYCH

Sergiusz Parszowski

Wojna w Ukrainie spowodowała wyraźny wzrost zainteresowania sprawami ochrony infrastruktury krytycznej zlokalizowanej nie tylko na terenach objętych konfliktem zbrojnym czy w krajach regionu, lecz także w państwach znacznie oddalonych od miejsc prowadzenia działań wojennych. Z jednej strony panuje ogólna zgoda co do tego, że powinniśmy obserwować przebieg wojny na Ukrainie i wyciągać z niej wnioski. Z drugiej natomiast infrastrukturę krajów europejskich dotknęły zdarzenia, które zostały zakwalifikowane jako działania sabotażowe lub co do których istnieje uzasadnione podejrzenie, że takimi właśnie były.

Wymiar Ukraiński

Ukraińska infrastruktura cywilna niszczona jest systematycznie i metodycznie od początku października ubiegłego roku[1]. W tym celu Rosja wykorzystuje przede wszystkim pozostałe jeszcze w jej zasobach pociski precyzyjne oraz pozyskane z Iranu „drony-kamikadze". Celem jest przede wszystkim infrastruktura elektroenergetyczna (elektrownie, sieci energetyczne i stacje przesyłowe), ciepłownicza (elektrociepłownie) oraz gazowa (gazociągi). Jednocześnie celem ataków kinetycznych co do zasady nie są centra przetwarzania danych.

Według dostępnych publicznie szacunków, w skutek rosyjskich ataków, do połowy grudnia zniszczeniami objętych było do 50% infrastruktury elektroenergetycznej, w tym wszystkie duże podstacje transformatorowe oraz elektrownie wodne i cieplne. Na znacznej części terytorium Ukrainy energia dostarczana jest tylko przez niewielką

[1] Institute for the Study of War (https://www.iswresearch.org/) jako początkową datę podaje 10 października 2022 r.

część doby (głównie w nocy), podczas gdy w pozostałych regionach codziennością stały się tymczasowe wyłączenia. W systemie elektroenergetycznym odnotowuje się aktualnie 30-procentowy deficyt mocy.

Zniszczenia infrastrukturalne oraz trudności z ich naprawą przy jednoczesnym zwiększonym zapotrzebowaniu na energię podczas niskich temperatur spowodowały, że sytuacja jest na tyle poważna, że coraz częściej mówi się, iż Ukraina stoi na progu klęski humanitarnej. Miliony Ukraińców pozbawionych jest nie tylko stałych dostaw energii elektrycznej, lecz także ogrzewania i bieżącej wody. Braki energii elektrycznej to w konsekwencji także braki usług telekomunikacyjnych, w tym tak ważnych jak możliwość wezwania służb ratunkowych. Celem ataków bywają także elementy systemu wodociągowego (stacje uzdatniania wody, przepompownie).

W kontynuowanych atakach na ukraińską infrastrukturę Rosji zależy nie tyle na osiągnięciu bezpośrednich korzyści wojskowych, co osłabieniu morale żołnierzy ukraińskich oraz złamaniu odporności ludności cywilnej. Według szacunków już ponad 6,8 mln Ukraińców zmuszonych było do opuszczenia swoich domów i poszukiwania nowego miejsca zamieszkania w zachodnich, zachodnio-południowych i centralnych regionach Ukrainy.

Wymiar Europejski

Jak czytamy w biuletynie Polskiego Instytutu Spraw Międzynarodowych „*Dążąc do osiągnięcia celów na Ukrainie, Rosja będzie nasilała działania hybrydowe, w tym wojnę informacyjną, cyberataki lub akty sabotażu wymierzone w infrastrukturę krytyczną państw NATO i UE. Działania te mają spotęgować obawy europejskiej opinii publicznej przed niekontrolowaną eskalacją konfliktu i dalszym pogarszaniem sytuacji gospodarczej. W ten sposób Rosja chce osłabić jedność sojuszniczą, która jest niezbędna do dalszego wspierania Ukrainy, wdrażania nowych strategii Sojuszu i Unii oraz szybkiego reagowania na pojawiające się zagrożenia*”[2]. W minionym roku odnotowano wiele zdarzeń sabotażowych i cyberataków, o których to sprawstwo przypisano lub podejrzewano właśnie Rosję.

Dotychczasowe działania sabotażowe dotykały przede wszystkim fizycznej infrastruktury energetycznej (rurociągi) oraz transportowej. W tym miejscu należy wymienić chociażby eksplozje rurociągów Nord Stream 1 i 2 (26.09.2022) czy niewyjaśnione dotąd zdarzenia dotyczące rurociągów w Polsce i na Litwie. W całym 2022 roku odnotowano również wyraźny wzrost incydentów

polegających na próbach rozpoznawania infrastruktury krytycznej państw europejskich. Zdarzeniem o innym charakterze, lecz również wynikającym z prowadzonych na terenie Ukrainy działań wojennych, było uderzenie pocisku we wsi Przewodów (15.11.2022 r.) – zaledwie kilka kilometrów od linii energetycznej łączącej Polskę z Ukrainą.

Cyberataki przeprowadzane są przede wszystkim na infrastrukturę energetyczną (elektrownie, sieci przesyłowe), transportową (linie kolejowe, porty morskie) oraz cyfrową (bankowość, administracja). Z krajów europejskich najczęściej atakowanymi są Polska oraz kraje bałtyckie. Z nagłośnionych przypadków wypada chociażby wspomnieć o zeszłorocznych atakach na systemy kolejowe w Danii, Niemczech i Włoszech. Analitycy przewidują, że cyberataki mogą nasilać się na systemy tych państw, które najbardziej zaangażowane są w pomoc Ukrainie oraz tych, w których niebawem odbędą się wybory prezydenckie bądź parlamentarne (m.in. Estonii, Finlandii i Polsce). Wiadomo także, że stałym celem ataków jest infrastruktura teleinformatyczna UE i NATO.

Nowe regulacje UE

W połowie stycznia tego roku weszły w życie dwie bardzo ważne regulacje unijne dotyczące ochrony infrastruktury krytycznej.

Pierwszą z nich jest „Dyrektywa Parlamentu Europejskiego i Rady w sprawie odporności podmiotów krytycznych i uchylająca dyrektywę Rady 2008/114/WE” (Dyrektywa CER). Określa ona obowiązki państw członkowskich w zakresie identyfikowania podmiotów krytycznych oraz wspieraniu podmiotów krytycznych, obowiązki podmiotów krytycznych mające na celu zwiększenie ich odporności i zdolności do świadczenia usług, środki mające na celu osiągnięcie

[2] Działania hybrydowe Rosji przeciw państwom NATO i UE, Anna Maria Dyner, Biuletyn PISM NR 183 (2602), 25 LISTOPADA 2022, Polski Instytut Spraw Międzynarodowych (PSIM).

wysokiego poziomu odporności podmiotów krytycznych, a także przepisy dotyczące nadzoru nad podmiotami krytycznymi.

Drugą regulacją jest Dyrektywa Parlamentu Europejskiego i Rady w sprawie środków na rzecz wysokiego wspólnego poziomu cyberbezpieczeństwa na terytorium Unii, zmieniająca rozporządzenie (UE) nr 910/2014 i dyrektywę (UE) 2018/1972 oraz uchylająca dyrektywę (UE) 2016/1148 (Dyrektywa NIS 2). Określa ona między innymi obowiązki państw członkowskich dotyczące przyjęcia krajowych strategii cyberbezpieczeństwa oraz wyznaczenia lub powołania właściwych organów, środki zarządzania ryzykiem w cyberbezpieczeństwie oraz obowiązki w zakresie zgłaszania incydentów, zasady i obowiązki w zakresie wymiany informacji o cyberbezpieczeństwie, a także obowiązki w zakresie nadzoru i egzekwowania przepisów spoczywających na państwach członkowskich.

Więcej na ten temat pisałem w poprzednim numerze czasopisma "Ochrona i Bezpieczeństwo obiektów i biznesu" (6/2022) w artykule zatytułowanym „Nowe regulacje dotyczące infrastruktury krytycznej".

Zalecenia dotyczące ochrony infrastruktury

Wdrażanie Dyrektywy CER i Dyrektywy NIS 2 zostało rozłożone na okres 3 lat, co jest okresem normalnym biorąc pod uwagę złożoność i zakres tych regulacji. Zważywszy jednak na aktualną sytuację polityczną i zmieniające się zagrożenia, takie jak rosyjska wojna napastnicza przeciwko Ukrainie i kampanie hybrydowe przeciwko państwom członkowskim UE, wzmocnienie odporności infrastruktury krytycznej powinno nastąpić jak najszybciej.

Odporność infrastruktury krytycznej to zdolności do zapobiegania zdarzeniom, które w istotny sposób zakłócają lub mogą w istotny sposób zakłócić świadczenie usług kluczowych na rynku wewnętrznym[3], a także do zdolności tej infrastruktury do ochrony przed takimi zdarzeniami, reagowania na nie, przeciwstawiania się im, łagodzenia lub amortyzowania ich skutków, przystosowywania się do nich lub przy wracania poprzedniego stanu.

W celu szybkiej poprawy ochrony infrastruktury krytycznej i płynnego przejścia do nowych regulacji Rada Europejska przygotowała zestaw rekomendacji pn. „Zalecenie Rady z dnia 8 grudnia 2022 r. w sprawie ogólnounijnego skoordynowanego podejścia do kwestii wzmocnienia odporności infrastruktury krytycznej (2023/C 20/01)". Zalecenia są skierowane przede wszystkim do organów i agencji Unii Europejskiej oraz państw członkowskich. Z formalnego punktu widzenia mają one jednak charakter niewiążący i mają być stosowane na zasadzie dobrowolności.

Kluczowe sektory

Dyrektywa CER wymienia jedenaście sektorów, w których to wyznaczane będą podmioty krytyczne, tj. energetykę (energia elektryczna, centralne ogrzewanie i chłodzenie, ropa, gaz, wodór), transport (powietrzny, kolejowy, wodny, lądowy), bankowość, infrastrukturę rynków finansowych,

[3] Usługi kluczowe to tj. usługi, które mają kluczowe znaczenie dla utrzymania niezbędnych funkcji społecznych i gospodarczych, bezpieczeństwa publicznego, zdrowia ludności lub środowiska.

zdrowie, wodę pitną, ścieki, infrastrukturę cyfrową, administrację publiczną, przestrzeń kosmiczną oraz wytwarzanie, przetwarzanie i dystrybucję żywności. Spośród wymienionych, jako kluczowe i zarazem priorytetowe, w zaleceniach uznaje się:

- energetykę;
- infrastrukturę cyfrową;
- transport;
- przestrzeń kosmiczną.

Podobnie za kluczową uważana jest infrastruktura krytyczna o istotnym znaczeniu transgranicznym, której zakłócenie mogłoby mieć znaczący wpływ na inne państwa członkowskie, i to niezależnie od sektora, do którego została ona zaliczona. Szczególna uwaga powinna być zwrócona także na infrastrukturę krytyczną znajdującą się poza terytorium państw członkowskich, taką jak podmorska infrastruktura krytyczna (m.in. podmorskie kable telekomunikacyjne) lub infrastruktura energii morskiej. Jeżeli zaś chodzi o infrastrukturę kosmiczną to priorytetem powinna być ochrona związanych z nią aktywów naziemnych, w tym obiektów produkcyjnych, i usług wykorzystujących instalacje w przestrzeni kosmicznej.

Zgodnie z zaleceniami wskazanie infrastruktury krytycznej w powyższych sektorach powinno dokonać się jak najszybciej, przy czym jako infrastrukturę krytyczną rozumie się tutaj zarówno infrastrukturę krytyczną wyznaczoną na mocy dotychczasowej dyrektywy w sprawie odporności podmiotów krytycznych (2008/114/WE), jako podmioty krytyczne, które należy wskazać na mocy Dyrektywy CER, zaś w stosownych przypadkach także podmioty objęte Dyrektywą NIS 2. W kolejnym kroku priorytetem jest przyjęcie środków zwiększających odporność infrastruktury krytycznej uwzględniających odpowiednie rodzaje ryzyka, w szczególności efekty kaskadowe, zakłócenia w łańcuchu dostaw, zależności, skutki zmiany klimatu, niewiarygodnych sprzedawców i partnerów oraz zagrożenia i kampanie hybrydowe, w tym zagraniczne manipulacje informacjami i ingerencje w informacje[4].

Działania krajów członkowskich

Zawarte w zaleceniach rekomendacje, by nie czekając na wdrożenie wszystkich nowych regulacji państw członkowskich :

- nadal wzajemnie koordynowały swoją reakcję, w stosownych przypadkach, i miały ogólny obraz międzysektorowych reakcji na znaczące zakłócenia w świadczeniu usług kluczowych przez infrastrukturę krytyczną;
- zintensyfikowały wymianę informacji z ERCC (Emergency Response Coordination Centre) na szczeblu operacyjnym w ramach UMOL (Unijnego Mechanizmu Ochrony Ludności), aby usprawnić wczesne ostrzeganie i skoordynować reakcję w ramach UMOL w przypadku zakłóceń funkcjonowania infrastruktury krytycznej;
- zwiększały swoją gotowość do reagowania za pomocą istniejących narzędzi lub narzędzi, które mają zostać opracowane;
- angażowały się w dalszy rozwój odpowiednich zdolności reagowania w ramach europejskiej puli ochrony ludności (European Civil Protection Pool, ECPP) i rescEU;

[4] ZALECENIE RADY z dnia 8 grudnia 2022 r. w sprawie ogólnounijnego skoordynowanego podejścia do kwestii wzmocnienia odporności infrastruktury krytycznej (2023/C 20/01), str. 2.

- zachęcały operatorów infrastruktury krytycznej i odpowiednie organy krajowe do zwiększania ich zdolności do szybkiego przywracania podstawowego funkcjonowania usług kluczowych świadczonych przez tych operatorów infrastruktury krytycznej;
- zachęcały operatorów infrastruktury krytycznej, by przy odbudowie ich infrastruktury krytycznej dążyli do tego, by była jak najbardziej odporna na pełen zakres poważnych zagrożeń, które mogą się do niej odnosić, w tym w przypadku niekorzystnych scenariuszy klimatycznych.

Wykorzystane Unijnego Mechanizmu Ochrony Ludności powinno obejmować również możliwości dotyczące:

- stałej analizy i testowania adekwatności i gotowości operacyjnej istniejących zdolności reagowania;
- regularnego monitorowania i wskazywania potencjalnie znaczących luk w zdolnościach reagowania w ramach zdolności ECPP i rescEU;
- dalszego pogłębiania współpracy międzysektorowej oraz organizowania regularnych szkoleń lub ćwiczeń;
- dalszego rozwijania ERCC jako międzysektorowego centrum reagowania na sytuacje nadzwyczajne na szczeblu Unii służącego koordynacji wsparcia dla państw członkowskich dotkniętych sytuacją nadzwyczajną.

Państwa członkowskie powinny gromadzić ekspertów z zakresu ochrony infrastruktury krytycznej, wspierać ich szkolenia, ćwiczenia oraz wymianę najlepszych praktyk i doświadczeń między nimi.

Zalecenia podkreślają także rosnącą współzależność infrastruktury fizycznej i cyfrowej, gdzie z jednej strony szkodliwe działania w cyberprzestrzeni mogą powodować zakłócenia lub szkody w infrastrukturze fizycznej, a sabotaż infrastruktury fizycznej może sprawić, że niedostępne staną się usługi cyfrowe. Jednym z priorytetów krajowych powinno być zwiększenie zdolności krajowych CSIRT oraz współpraca z zaufanymi sprzedawcami i partnerami. Ponadto wskazuje się na potrzebę prowadzenia proaktywnej komunikacji strategicznej w kontekście przeciwdziałania zagrożeniom i kampaniom hybrydowym.

Wykorzystanie możliwości

Zalecenia dotyczące infrastruktury krytycznej zawierają także szereg rekomendacji dotyczących lepszego wykorzystania już istniejących mechanizmów i narzędzi mogących wzmocnić odporność infrastruktury krytycznej, m.in.:

- wykorzystanie przez państwa członkowskie oraz operatorów infrastruktury krytycznej potencjalnych możliwości finansowania na szczeblu unijnym i krajowym;
- wykorzystywanie projektów badawczych i innowacyjnych finansowanych przez Unię;
- przyśpieszenie przez grupę współpracy ds. bezpieczeństwa sieci i informacji (wezwanie z Nevers) prac nad ukierunkowaną oceną ryzyka i scenariuszy ryzyka w cyberprzestrzeni oraz jak najszybszego przedstawienia pierwszych zaleceń;
- pełne korzystanie z usług w zakresie gotowości do reagowania w obszarze cyberbezpieczeństwa oferowanych w ramach realizowanego przez Komisję krótkoterminowego programu wsparcia wdrażanego wraz z ENISA (np. testowania penetracyjnego);
- pełne wykorzystanie Europejskiego Centrum Kompetencji w dziedzinie Cyberbezpieczeństwa (ECCC);
- pełne wdrożenie środków zalecanych we wspólnym unijnym zestawie narzędzi na potrzeby cyberbezpieczeństwa sieci 5G, a w szczególności wprowadzenie ograniczeń wobec dostawców wysokiego ryzyka;
- wspierania Centrum Koordynacji Reagowania Kryzysowego (ERCC) w osiągnięciu gotowości operacyjnej i w reagowaniu na zakłócenia infrastruktury krytycznej;
- rozwijanie wykorzystania programu Copernicus oraz systemu Galileo i europejskiego systemu wspomagania satelitarnego (EGNOS) do celów nadzoru;
- efektywne wykorzystanie możliwości oferowane przez unijną rządową łączność satelitarną (Govsatcom) w ramach unijnego programu kosmicznego w celu monitorowania

infrastruktury krytycznej i wspierania przewidywania kryzysów i reagowania na nie;
- wzmocnienie dialogu i współpracy między wyznaczonymi ekspertami państw członkowskich oraz z Komisją, aby zwiększyć fizyczną odporność infrastruktury krytycznej, w szczególności poprzez przygotowanie metod i scenariuszy ryzyka, wspierania przeprowadzania testów warunków skrajnych, a także gromadzenia, podsumowywania i wymiany najlepszych praktyk, wniosków wyciągniętych z doświadczeń krajowych i innych informacji dotyczących odporności.

Zaangażowanie europejskie

W końcu w zaleceniach wzywa się agencje i inne właściwe organy Unii do udzielania wsparcia w kwestiach związanych z odpornością infrastruktury krytycznej, w szczególności w następujący sposób:
- Agencję Unii Europejskiej ds. Współpracy Organów Ścigania (Europol) – w zakresie wsparcia w gromadzeniu informacji, analizie kryminalnej i wsparciu dochodzeniowym na rzecz transgranicznych działań organów ścigania; oraz, w razie potrzeby i w stosownych przypadkach, dzieleniu się wynikami z państwami członkowskimi;
- Europejską Agencję Bezpieczeństwa Morskiego (EMSA) – w zakresie wsparcia w obszarze ochrony i bezpieczeństwa sektora morskiego w Unii, w tym usług nadzoru morskiego odnoszących się do kwestii związanych z ochroną na morzu i bezpieczeństwem morskim;
- Agencję Unii Europejskiej ds. Programu Kosmicznego (EUSPA) i Centrum Satelitarne UE (SatCen) – w zakresie możliwości wsparcia poprzez operacje w ramach unijnego programu kosmicznego;
- ECCC – w zakresie wsparcia w odniesieniu do działań związanych z cyberbezpieczeństwem, również we współpracy z ENISA, możliwość wspierania innowacji i polityki przemysłowej w dziedzinie cyberbezpieczeństwa.

Wykorzystane powinny być także możliwości jakie zapewnia Europejska Służba Działań Zewnętrznych (ESDZ), w szczególności poprzez swoje Centrum Analiz Wywiadowczych UE i Komórkę UE ds. Syntezy Informacji o Zagrożeniach Hybrydowych, w zakresie dostarczania odpowiednich informacji w formie briefingów, niewiążących podręczników i wytycznych.

Testy warunków skrajnych

Jednym z priorytetowych środków wzmacniających odporność infrastruktury krytycznej w świetle aktualnych zagrożeń wojennych mają być przeprowadzane na szczeblu krajowym testy warunków skrajnych. Ich głównym celem jest ocena odporności infrastruktury krytycznej na zagrożenia typu antagonistycznego spowodowane przez człowieka. W pierwszej kolejności, jeszcze w 2023 roku, testami objęty ma być sektor energetyczny oraz towarzysząca mu infrastruktura cyfrowa.

Na poziomie europejskim, z udziałem naukowców i służb wywiadowczych, opracowanych zostało kilkadziesiąt potencjalnych incydentów charakteryzujących się tym, że przy niewielkim nakładzie ponoszonym przez przeciwnika możliwe jest wywołanie rozległego i długotrwałego kryzysu. Wszystkie kraje członkowskie, na podstawie otrzymanych opisów możliwych incydentów, mają przygotować nie mniej niż cztery wielopodmiotowe i wieloetapowe scenariusze ćwiczeń, a następnie wskazać odpowiednią infrastrukturę krytyczną i wspólnie z jej operatorami przeprowadzić stosowne testy.

Podsumowanie

Dyrektywa CER wymaga, by w każdym państwie członkowskim powołany został co najmniej jeden organ odpowiedzialny za prawidłowe stosowanie i egzekwowanie przepisów unijnych, który będzie miał uprawnienia do przeprowadzania kontroli, zaś w przypadku stwierdzenia naruszeń będzie mógł nakazać podmiotom krytycznym podjęcie koniecznych i proporcjonalnych działań oraz nałożyć sankcje (skuteczne, proporcjonalne i odstraszające). Zalecenia rekomendują zatem państwom członkowskim, by przeznaczały one wystarczające zasoby finansowe na wzmocnienie zdolności swoich odpowiednich organów krajowych i do wspierania ich w działaniach mających na celu zwiększenie odporności infrastruktury krytycznej.

W tym samym czasie w Polsce procedowane są prace nad ustawą o ochronie ludności i stanie klęski żywiołowej[5], której to projekt zakłada między innymi likwidację dzisiejszego systemu zarządzania kryzysowego, w tym także Rządowego Centrum Bezpieczeństwa będącego głównym organem zajmującym się sprawami infrastruktury krytycznej. Jakkolwiek projekt ustawy przewiduje przekazanie dotychczasowych zadań RCB ministrowi właściwemu do spraw wewnętrznych, to jednak w jego obecnym brzmieniu w żaden sposób nie przygotowuje naszego państwa do nowych regulacji i nowych wyzwań w zakresie ochrony infrastruktury krytycznej. Jest to o tyle niezrozumiałe, gdy weźmie się pod uwagę, iż treści nowych unijnych dyrektyw były znane już o wiele wcześniej. ■

Sergiusz Parszowski
Lider zespołu eksperckiego Instin.pl
Prezes think tanku ObserwatoriumBezpieczenstwa.pl

[5] https://legislacja.rcl.gov.pl/projekt/12363754