WRDS WOJEWÓDZKA RADA DIALOGU SPOŁECZNEGO W GDAŃSKU

Informacja Wojewódzkiej Rady Dialogu Społecznego w Gdańsku z dnia 26 września 2019 r. dotycząca cyberbezpieczeństwa

Zbudowanie pierwszych komputerów elektronicznych w latach 40-tych ubiegłego wieku rozpoczęło erę dynamicznego rozwoju nowoczesnych technologii, dzięki którym wyłonił się nowy rodzaj społeczeństwa nazwany przez Japończyka T. Umesao społeczeństwem informacyjnym (Information Society). Działalność człowieka została uzależniona od systemów i sieci teleinformatycznych tworzących nową „przestrzeń życiową" obejmującą swym zasięgiem cały świat. Przestrzeń ta została nazwana cyberprzestrzenią i stała się doskonałym środowiskiem funkcjonowania administracji publicznej, podmiotów gospodarczych oraz zaawansowanych technologicznie społeczeństw. Obszar ten, stał się także przedmiotem zainteresowania zorganizowanych grup przestępczych, organizacji terrorystycznych oraz sił zbrojnych.

Dzisiaj w sposób odpowiedzialny musimy mówić o budowaniu skutecznych mechanizmów bezpieczeństwa chroniących nas przed szkodliwą działalnością prowadzoną w globalnej sieci komputerowej. Zapewnienie cyberbezpieczeństwa, rozumianego jako odporność systemów informacyjnych na działania naruszające poufność, integralność, dostępność i autentyczność przetwarzanych danych lub związanych z nimi usług oferowanych przez te systemy (definicja zaczerpnięta z Ustawy z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa) jest jednym z najważniejszych zadań realizowanych w ostatnich latach przez administrację rządową. Zadanie to nie jest łatwe do zrealizowania ze względu na skalę problemu oraz jego złożoność.

Budując mechanizmy bezpieczeństwa w cyberprzestrzeni, w pierwszej kolejności zwrócono szczególną uwagę na konieczność ochrony elementów infrastruktury krytycznej państwa, w których systemy i sieci teleinformatyczne mają szerokie zastosowanie. Elementy te zaliczane są do takich sektorów jak: systemy zaopatrzenia w energię i paliwa, systemy łączności i sieci teleinformatycznych, systemy finansowe, systemy zaopatrzenia w żywność i wodę, systemy ochrony zdrowia, systemy transportowe i komunikacyjne, systemy ratownicze, systemy zapewniające ciągłość działania administracji publicznej, systemy produkcji, składowania, przechowywania i stosowania substancji chemicznych i promieniotwórczych, w tym rurociągi substancji niebezpieczny.

Rozpatrując problematykę cyberbezpieczeństwa, należy zdawać sobie sprawę z tego, że najsłabszym ogniwem zawsze będzie człowiek – użytkownik systemów i sieci teleinformatycznych. Bardzo często zwykli ludzie, właściciele firm, korporacji, decydenci nie zdają sobie sprawy z tego, jak łatwo uzyskać dostęp do danych w postaci cyfrowej

lub całkowicie zablokować funkcjonowanie sieci komputerowych. Nie każdy zdaje sobie sprawę o zagrożeniach, jakie mogą płynąć z „wirtualnego świata". Stosowanie zabezpieczeń w postaci zapór ogniowych i programów antywirusowych nie zawsze wystarcza. Ważna jest także odpowiednia świadomość użytkowników. Lekceważenie przedstawionego powyżej problemu może doprowadzić do przykrych w skutkach sytuacji. Statystyki, raporty, doniesienia są jednoznaczne. Hakerzy, przestępcy działający w sieci coraz częściej sięgają po dane, ukryte informacje, czyszczą konta bankowe, dokonywane są kradzieże tożsamości, zagrożone jest bezpieczeństwo państwowe. Luki w oprogramowaniu są wykorzystywane jako „furtki" do włamań. Brak świadomości o zagrożeniach to duży problem dzisiejszego świata w szczególności gdy „cyber-sieć" wnika coraz głębiej w ludzkie życie. Rozmiar tej sieci stale się powiększa. Liczba użytkowników Internetu wg danych z czerwca 2019 roku, zamieszczonych w serwisie www.internetworldstats.com, szacowana jest na ponad 4,5 miliarda, a liczba urządzeń tzw. Internetu rzeczy (Internet of things) ma osiągnąć wartość 50 miliardów w 2020 roku.

Monitorowanie sieci pod kątem identyfikacji zagrożeń i przeciwdziałania nim staje się coraz trudniejsze i wymaga ogromnych nakładów. Podejmowane są działania mające na celu ocenę podatności systemów i sieci teleinformatycznych na zagrożenia oraz prowadzące do wskazania słabych punktów. Administratorzy systemów wyposażani są w narzędzia wykrywające szkodliwe działania prowadzone w nadzorowanych przez nich systemach teleinformatycznych. Zalecane są szkolenia i warsztaty uświadamiające użytkowników o znaczeniu ochrony informacji.

Budowanie skutecznych mechanizmów cyberbezpieczeństwa wymaga przygotowania solidnych regulacji prawnych. Niewątpliwie dużym osiągnięciem administracji rządowej w Polsce było opracowanie i przyjęcie wspominanej już Ustawy o krajowym systemie cyberbezpieczeństwa. Ustawa ta weszła w życie 28 sierpnia 2018 r. i daje podstawy do stworzenia w Polsce krajowego systemu cyberbezpieczeństwa. System ten będzie obejmował m.in. instytucje administracji rządowej i samorządowej oraz największych przedsiębiorców z kluczowych sektorów gospodarki. W ustawie wskazano operatorów usług kluczowych i zaliczono do nich największe banki, firmy z sektora energetycznego, przewoźników lotniczych i kolejowych, armatorów oraz szpitale. W ustawie wskazano instytucje publiczne, w których kompetencjach znajdzie się nadzór nad danym istotnym sektorem dla naszej gospodarki np. dla firm zajmujących się transportem lotniczym organem właściwym jest Minister Infrastruktury. Zgodnie z ustawą Zespoły Reagowania na Incydenty Bezpieczeństwa Komputerowego zostaną utworzone w trzech instytucjach: Agencji Bezpieczeństwa Wewnętrznego, Naukowej i Akademickiej Sieci Komputerowej – Państwowym Instytucie Badawczym oraz Ministerstwie Obrony Narodowe. Podmioty te będą współpracować ze sobą, z organami właściwymi do spraw cyberbezpieczeństwa, ministrem właściwym do spraw informatyzacji oraz Pełnomocnikiem Rządu ds. Cyberbezpieczeństwa.

Podsumowując, należy stwierdzić, że znaczenie systemów i sieci teleinformatycznych we współczesnym świecie jest tak wielkie, że stały się ona bardzo wrażliwym elementem

funkcjonalnym całego państwa. Systemy te mają również kluczowe znaczenie w funkcjonowaniu elementów infrastruktury krytycznej. Szybkie tempo rozwoju technologii informacyjnych w wymiarze sprzętowym jak i oprogramowania spowodowało, że obecne mechanizmy oraz procedury bezpieczeństwa są niewystarczające. Jest to znaczący problemem, który powoduje wielkie starty firm oraz instytucji państwowych. Kłopot również stanowi globalna sieć komputerowa, której tak intensywny rozwój trudny był do przewidzenia. Łączy ona ze sobą miliardy urządzeń stając się doskonałym środowiskiem do prowadzenia działalności przestępczej.

W ostatnich latach odczuwalne jest również zaangażowanie sił zbrojnych różnych państwa w prowadzeniu działań pasywnych jak i aktywnych w cyberprzestrzeni. Należy się również liczyć z tym, że w przyszłości nowoczesne armie będą coraz częściej wykorzystywać cyberprzestrzeń do prowadzenia działań mających na celu unieszkodliwienie infrastruktury krytycznej innych państw, w tym również infrastruktury morskiej. Jedyną receptą na zmianę takiego stanu rzeczy jest konsekwentne i rygorystyczne budowanie mechanizmów cyberbezpieczeństwa w wymiarze krajowym oraz międzynarodowym, opartych na solidnych podstawach prawnych.

Przewodniczący
Wojewódzkiej Rady Dialogu Społecznego
w Gdańsku
Zbigniew Canowiecki