ANDRZEJ LIMAŃSKI
IRENEUSZ DRABIK
ZBIGNIEW GRZYWNA
Wyższa Szkoła Zarządzania Marketingowego i
Języków Obcych w Katowicach

ZARZĄDZANIE BEZPIECZEŃSTWEM INFORMACYJNYM W WARUNKACH GLOBALIZACJI

Jednostki i podmioty zbiorowe funkcjonują obecnie w warunkach globalizacji, którą można określić jako proces narastającej współzależności między państwami, dużymi regionami oraz podmiotami gospodarczymi i niekomercyjnymi (non-profit). Wielowymiarowość, a jednocześnie złożoność i wielowątkowość globalizacji oznacza, że przebiega ona równolegle w różnych obszarach życia społecznego: w gospodarce, polityce, wojskowości, kulturze. Rosnąca współzależność jest tak silna, że wywiera presję na integrację we wszystkich praktycznie sferach życia społecznego [1].

Jednym z czynników globalizacji jest gwałtowny postęp technologiczny, związany z kształtowaniem się tzw. społeczeństwa informacyjnego. Rozwój technologii informacyjnych radykalnie zmienia funkcjonowanie jednostek i podmiotów zbiorowych, a jednocześnie traktowany jest jako fundamentalny czynnik rozwoju społeczeństw i państw w XXI wieku. Powstające globalne społeczeństwo informacyjne można traktować jako konglomerat wzajemnych związków pomiędzy technikami i technologiami informacyjnymi, przemianami struktur gospodarczych w mikro- i makroskali, a polityką poszczególnych państw i organizacji międzynarodowych oraz celami różnych grup interesów, od producentów technologii informacyjnych, poprzez nowo powstałe społeczności wirtualne, aż do społeczności lokalnych i grup broniących się przed dokonującymi się zmianami [2]. W powyżej zarysowanych warunkach wzrasta znaczenie zarządzania bezpieczeństwem coraz bardziej rozbudowanych i złożonych systemów gromadzenia, przetwarzania i wykorzystania informacji.

W ogólnym znaczeniu bezpieczeństwo można określić jako pewność istnienia i przetrwania, posiadania oraz funkcjonowania i rozwoju danego podmiotu. Pewność jest wynikiem nie tylko braku zagrożeń (ich niewystępowania lub wyeliminowania), ale także powstaje wskutek kreatywnej działalności podmiotu i jest zmienna w czasie, czyli ma naturę procesu społecznego. W analizach teoretycznych bezpieczeństwa wyodrębnia się trzy podstawowe ujęcia (wymiary) [3]:

- podmiotowe – dotyczy odpowiedzi na pytanie o czyją pewność istnienia i przetrwania chodzi;
- przedmiotowe – dotyczy treści bezpieczeństwa, środków i sposobów kształtowania pewności stanu posiadania (w tym tożsamości) poszczególnych podmiotów i ich szans (swobód) rozwojowych;
- funkcjonalne (procesualne) – pozwala obserwować zmienność w czasie, a więc dynamikę i ewolucję subiektywnych i obiektywnych aspektów bezpieczeństwa podmiotów, tj. pewności ich istnienia (przetrwania), ich stanu posiadania i szans (swobód) rozwojowych.

Pojęcia bezpieczeństwa informacyjnego nie należy zawężać do zagadnień związanych z bezpieczeństwem informatycznym. Bezpieczeństwo informatyczne polega na podejmowaniu działań zmierzających do zabezpieczenia zasobów informacyjnych w pamięciach komputerów oraz w sieciach teleinformatycznych. Bezpieczeństwo informacyjne, nazywane również zamiennie bezpieczeństwem informacji, nie odnosi się tylko do reguł i procedur związanych z cyfrową obróbką i przechowywaniem danych i informacji. Obejmuje ono ogół procesów, w trakcie których dochodzi do generowania i przetwarzania danych i informacji. Inaczej rzecz ujmując, bezpieczeństwo informacyjne stanowi zbiór działań, metod, procedur, podejmowanych przez uprawnione podmioty, zmierzających do zapewnienia integralności gromadzonych, przechowywanych i przetwarzanych zasobów informacyjnych, poprzez zabezpieczenie ich przed niepożądanym, nieuprawnionym ujawnieniem, modyfikacją, zniszczeniem [4].. Zgodnie ze zbliżonym podejściem bezpieczeństwo informacyjne dotyczy zagwarantowania sobie przez dany podmiot integralności, kompletności oraz wiarygodności posiadanych zasobów informacyjnych w każdej formie, nie tylko elektronicznej. Zawiera w sobie

wszelkie wysiłki służące ochronie posiadanych informacji, istotnych w kontekście bezpieczeństwa funkcjonowania danego podmiotu (a więc mających wpływ na jego sprawne funkcjonowanie i spełnianie swoich funkcji), jak i zapewnianiu przewagi informacyjnej przez zdobywanie nowych lub bardziej aktualnych danych i informacji, a także podejmowanie akcji dezinformacyjnych wobec swoich rywali (konkurentów, przeciwników) [5].

Niezwykle ważne jest posiadanie strategii zapewniającej utrzymanie niezbędnego poziomu bezpieczeństwa oraz przygotowanie planów funkcjonowania w sytuacjach szczególnych zagrożeń. Bezpieczeństwo informacji jest tym sektorem, który decyduje o działaniu wielu innych sektorów, ujawnienie informacji gospodarczych lub biznesowych może niekorzystnie wpływać na rozwój wielu dziedzin naukowych. Dla większości podmiotów znajdujących się na rynku niezwykle ważną kwestią jest dostęp do usług zabezpieczenia wiadomości wiedzy i źródeł ich pozyskiwania. Uzależnienie społeczeństwa od prawidłowego funkcjonowania informacji, czego przykładem w sieci jest Internet sprawia, że priorytetem staje się zabezpieczenie sieci i usług telekomunikacyjnych na odporność przed wszelkiego rodzaju zagrożeniami struktur komunikacyjnych. Bezpieczeństwo informacji (nie mówimy o informacjach z klauzulami tajności czy dostępności) ma trzy różne aspekty, do których należą:

- dostępność, co oznacza, że system jest odpowiednio zabezpieczony przed przerwami w jego funkcjonowaniu oraz ma dostęp do niezbędnych danych, które w różny sposób mogą być wykorzystane;
- wyłączność, inaczej integralność, co oznacza, że niemożliwe jest manipulowanie funkcjami i danymi dostępnymi w systemie;
- poufność, prywatność, sekretność, oznacza, że nie jest możliwe dotarcie do funkcji danych w systemie, ani ich odczytanie.

Zdarzające się z różnych przyczyn usterki systemów telekomunikacyjnych oraz informatycznych, a także celowe ataki mogą w różnym stopniu wpłynąć na wyżej wymienione aspekty bezpieczeństwa. Ataki osób, organizacji, instytucji, w sposób przemyślany lub nie, na sieci telekomunikacyjne można podzielić następująco:

- ataki fizyczne na infrastrukturę telekomunikacyjną;
- ataki elektromagnetyczne na strukturę telekomunikacyjną;
- ataki przy użyciu środków logicznych, skierowane przeciw systemom informacyjnym w systemach sieci telekomunikacyjnych;
- zagrożenia społeczne wobec decydentów w systemach zarządzania i sterowania sieciami telekomunikacyjnymi;
- przeciążenie ruchem sieci telekomunikacyjnej;
- uzależnienie od innych sektorów społeczeństwa.

Do Polskiej Infrastruktury Krytycznej mającej wpływ na Europejską Infrastrukturę można zaliczyć zasoby fizyczne, usługi, sprzęt informatyczny, sieci i inne elementy infrastruktury, których zakłócenie lub zniszczenie miałoby poważny wpływ na zdrowie, bezpieczeństwo, dobrobyt gospodarczy, bądź społeczny trzech lub większej liczby państw członkowskich. Opracowaną przez operatorów planów ochrony obiektów zaliczonych do infrastruktury krytycznej koncepcję analizuje i zatwierdza organ koordynujący ochronę infrastruktury krytycznej w danym kraju.

1. A. Bąkiewicz, U. Żuławska (red.): Rozwój w dobie globalizacji. PWE, Warszawa 2010, s. 36-37.

2. B. Gregor, M. Stawiszyński: e-Commerce. Oficyna Wydawnicza Branta, Bydgoszcz – Łódź 2002, s. 17.

3. R. Zięba (red.): Bezpieczeństwo międzynarodowe po zimnej wojnie. Wydawnictwa Akademickie i Profesjonalne, Warszawa 2008, s. 16-22.

4. K. A. Wojtaszczyk, A. Materska-Sosnowska (red.): Bezpieczeństwo państwa. Wybrane problemy. Oficyna Wydawnicza ASPRA-JR, Warszawa 2009, s. 193-194.

5. M. Madej, M. Terlikowski (red.): Bezpieczeństwo teleinformatyczne państwa. Polski Instytut Spraw Międzynarodowych, Warszawa 2009, s. 18.