Bezpieczeństwo fundamentem sukcesu czwartej rewolucji przemysłowej

Joanna Świątkowska

Streszczenie: Celem artykułu jest przybliżenie czytelnikom najważniejszych informacji dotyczących czwartej rewolucji przemysłowej oraz konsekwencji, jakie niesie ona dla bezpieczeństwa kluczowych systemów teleinformatycznych kraju. Tekst omawia potencjalne zagrożenia i wyzwania oraz inicjatywy, które powinny zostać podjęte, aby wzmacniać bezpieczeństwo współczesnych państw i społeczeństw.

Słowa kluczowe: Przemysł 4.0, czwarta rewolucja przemysłowa, IT, OT, polityka cyberbezpieczeństwa UE, automatyzacja

Abstract: *The main goal of the article is to provide the readers with key information on so called fourth industrial revolution and the impact that it brings on security of the vital national ICT systems. The text sheds light on potential threats and challenges but also on initiatives that are and should be undertaken to enhance security of modern countries and societies.*

Key words: Industry 4.0., fourth industrial revolution, IT, OT, cyber-threats, EU cybersecurity policy, automation

Niewiele było tak przełomowych wynalazków w historii rozwoju cywilizacji, które wpłynęłyby na rzeczywistość do tego stopnia, że zmieniły większość obszarów funkcjonowania życia ludzi. Maszyna parowa, silnik wysokoprężny oraz elektronika i oparte o nią komputery. To trzy najważniejsze wynalazki, kamienie milowe, które zmieniły przede wszystkim procesy wytwarzania dóbr. Nazywa się je wielkimi rewolucjami przemysłowymi. W chwili obecnej jesteśmy świadkami kolejnej rewolucji, w dodatku takiej, która dotyka nie tylko podstaw gospodarek, ale także innych obszarów funkcjonowania państw i społeczeństw, a w sposób szczególny bezpieczeństwa.

Celem niniejszego artykułu jest próba odpowiedzi na pytanie badawcze, czy sukces przemiany cywilizacyjnej, którą aktualnie obserwujemy, a która opiera się na wykorzystaniu informacji, może zostać zagrożony przez niewystarczające działania ochronne. Teza stawiana w niniejszej pracy mówi, że zapewnianie bezpieczeństwa jest niezbędnym warunkiem sukcesu tak zwanej IV rewolucji przemysłowej, a tym samym warunkuje stabilność funkcjonowania współczesnych państw. Aby udowodnić to twierdzenie, szczególnej analizie poddane zostały zagrożenia płynące z przestrzeni cyfrowej oraz uwarunkowania procesu związane z bezpieczeństwem. Narzędziami wykorzystywanymi w przygotowaniu niniejszego artykułu, które pozwoliły odnieść się do stawianej tezy, były: analiza strategicznych dokumentów źródłowych, krytyczny przegląd koncepcji i poglądów występujących w literaturze przedmiotu. Tekst zawiera także rekomendacje kierunkowe dotyczące zapewniania bezpieczeństwa w erze przemian cyfrowych. Z racji natury omawianych przemian cywilizacyjnych, opisanych poniżej, w niniejszym tekście termin bezpieczeństwa odnosił się będzie do bezpieczeństwa sieci i systemów informatycznych. Oznaczać będą one: „odporność sieci i systemów informatycznych, przy danym poziomie zaufania, na wszelkie działania naruszające dostępność, autentyczność, integralność lub poufność przechowywanych lub przekazywanych, lub przetwarzanych danych, lub związanych z nimi usług oferowanych, lub dostępnych poprzez te sieci i systemy informatyczne[1]".

Przed rozwinięciem tezy dotyczącej wpływu zachodzących przemian na bezpieczeństwo, konieczne staje się znalezienie odpowiedzi na pytanie, czym jest czwarta rewolucja przemysłowa i jaka jest jej natura. Sercem omawianych procesów jest ścisła integracja fizycznej rzeczywistości z tą związaną ze światem cyfrowym. Żyjemy w coraz bardziej zautomatyzowanym świecie, w dodatku w takim, w którym to komputery sterują wieloma procesami, także wytwórczymi. Przetwarzanie danych w chmurze, *big data* czy przede wszystkim Internet Rzeczy (IoT) – napędzają rewolucję. Koncepcję Internetu Rzeczy sformułował w 1999 roku Kevin Ashton w celu opisania systemu, w którym świat materialny komunikuje się z komputerami (wymienia dane) za pomocą wszechobecnych sensorów[2]. W otaczającej nas rzeczywistości pojawia się coraz więcej urządzeń, rozwiązań podłączonych do Internetu. Nie mamy już zatem do czynienia wyłącznie z połączeniem maszyny i komputera, ale z dalszą ich integracją opartą na dostępie do sieci, maszyny te i komputery są współprowadzone[3]. Sztandarowymi przykładami są oczywiście telefony, lodówki, inteligentne samochody czy domy – urządzenia znane z naszego codziennego funkcjonowania, które mogą komunikować się ze sobą. Jednak poza przedmiotami codziennego użytku warto zwrócić uwagę na automatyzację i cyfryzację procesów kluczowych z punktu widzenia funkcjonowania państw i gospodarek. Dziś mówimy o przemyśle nowej generacji, o przemyśle 4.0, gdzie większość zautomatyzowanych procesów, także realizowanych przez infrastruktury krytyczne, obsługiwanych jest zdalnie, za pomocą komputerów. Przynosi to wiele zalet i pożytku m.in.: większą efektywność, oszczędności, sprawniejsze niwelowanie usterek lub możliwość całkowitego unikania przestojów w produkcji itd.

Korzyści dla poszczególnych przedsiębiorstw oraz dla całych gospodarek zostały zauważone nie tylko przez konkretne podmioty gospodarcze, ale także przez decydentów najwyższego szczebla, którzy ideę czwartej rewolucji uczynili strategicznym celem swoich działań. Obranie kursu na przemysł 4.0 widoczne jest zarówno na poziomie międzynarodowym, jak i krajowym. Unia Europejska od kilku lat bardzo mocno realizuje przede wszystkim Jednolitą Agendę Cyfrową, czyli dalsze ucyfrowienie europejskiej gospodarki[4]. Sukces inicjatywy ma przełożyć się na znaczne korzyści finansowe, szacuje się bowiem, że postępująca cyfryzacja gospodarki, rozumiana jako jeszcze bardziej intensywne implementowanie produktów i usług teleinformatycznych, może przynieść około 110 miliardów euro przychodu rocznie dla europejskiej gospodarki w ciągu nadchodzących 5 lat[5]. Większa efektywność i znaczenie przemysłu dla gospodarki nie może dziwić, skoro stanowi on filar europejskiej ekonomii: odpowiada za 2 miliony przedsiębiorstw, 33 miliony miejsc pracy i 60% wzrostu wydajności[6]. Także na poziomie państw narodowych obserwujemy aktualnie bardzo wiele inicjatyw, wzmacniających proces czwartej rewolucji przemysłowej. Państwa takie, jak Francja, Niemcy, Włochy czy Wielka Brytania, bardzo mocno wspierają działania rozwijające Przemysł 4.0[7]. Dla przykładu Niemcy zainwestowały około 200 milionów euro w inicjatywę, która ma na celu szybszy i bardziej intensywny rozwój fabryk czwartej generacji[8]. Realizacja planu rozpoczęła się już 7 lat temu, a przewidywany okres implementacji zaplanowanych działań obejmuje okres 10–15 lat. Także polski rząd uczynił czwartą rewolucję, kierunkowskazem dla swoich rozwojowych planów. Flagowy projekt Ministerstwa Rozwoju, a także całego rządu, czyli *Strategia na rzecz odpowiedzialnego rozwoju*, jest oparta na pomyśle ucyfrowienia gospodarki.

Jednak, jak zostało wskazane na początku niniejszego tekstu, czwarta rewolucja przemysłowa ma nie tylko pozytywny wymiar. Nowoczesne technologie zrewolucjonizowały większość aspektów naszego życia – sposób komunikacji[10], kulturę, politykę i relacje międzynarodowe[11], strukturę społeczną[12] i wiele innych. Wpłynęły także fundamentalnie na kwestie związane z bezpieczeństwem, przynosząc wiele wyzwań i zagrożeń. Jeśli systemy oparte na nowoczesnych technologiach stanowią fundament kluczowych procesów państwowych, społecznych, a przede wszystkim gospodarczych, to ich potencjalne zakłócenie może mieć konsekwencje dla funkcjonowania całych państw. Pojawił się nowy wymiar podatności kluczowych systemów. Warto przyjrzeć się bliżej tym wyzwaniom.

Przede wszystkim konieczne jest zwrócenie uwagi na fakt, że współczesne zastosowanie technologii teleinformatycznych nie sprowadza się wyłącznie do gromadzenia, przetwarzania i przesyłania danych w postaci cyfrowej. Należy dostrzec różnice w funkcjonowaniu tak zwanych systemów informatycznych (ang. *information technology* – IT) oraz systemów sterowania przemysłowego (ang. *operational technnology* – OT). W pierwszym przypadku systemy IT odpowiadają za szereg procesów biznesowych, w drugim przypadku często warunkują funkcjonowanie procesów produkcyjnych, działanie konkretnych urządzeń[13]. Atak na systemy biznesowe może przynieść wiele strat – utratę danych, wyciek informacji, straty finansowe czy wizerunkowe. Są to cyfrowe zagrożenia właściwe bardziej dla trzeciej rewolucji przemysłowej. W przypadku czwartej rewolucji przemysłowej wrogie ataki na ucyfrowione systemy sterowania przemysłowego mogą mieć znacznie bardziej dramatyczne konsekwencje – mogą doprowadzić do zniszczeń fizycznych, uszczerbku na zdrowiu, utraty życia czy paraliżu funkcjonowania danych systemów. Nie są to nierealne scenariusze, co pokazały choćby atak wirusa Stuxnet na irańskie instalacje nuklearne, zniszczenie niemieckiej huty stali w wyniku cyberataku czy zmasowany atak na system energetyczny Ukrainy. Nie ma już żadnych wątpliwości, że infrastruktura krytyczna współczesnych państw może zostać narażona na ataki płynące właśnie z cyberprzestrzeni.

Czwarta rewolucja przemysłowa będzie się pogłębiała i będzie obejmowała coraz to nowe aspekty naszej rzeczywistości. To proces nieodwracalny. Jej sukces jednak zależał będzie od tego, czy wraz z postępem i idącymi za nim udogodnieniami poszczególni interesariusze zadbają o zapewnienie fundamentów bezpieczeństwa. Niestety aktualna ocena podejmowanych działań jest w tym kontekście negatywna. Bardzo często producenci rozwiązań związanych z Internetem Rzeczy kładą większy nacisk na użyteczność produktów, systemów niż na ich zabezpieczenia[14]. Wiąże się to bardzo często z chęcią oszczędzania, z faktem, że sam rynek, konsumenci poprzez swoje decyzje nie wywołują wystarczającej presji. Oczekują oni bowiem tanich produktów, niekoniecznie w pierwszej kolejności stawiając na bezpieczeństwo rozwiązań. Dotychczas nie podjęto także wystarczających decyzji po stronie regulatorów, które narzucałyby stosowanie odpowiednich zabezpieczeń. Zagrożenia tymczasem nieustannie wzrastają, a złoczyńcy wiedzą, że miliony niezabezpieczonych urządzeń mogą stać się łatwym celem. W jednym ze swoich raportów na temat cyberbezpieczeństwa, zatytułowanym *What Every CEO Needs to Know About Cybersecurity*, firma AT&T wskazuje na wzrost aż o 458% prób skanowania systemów IoT w poszukiwaniu ich podatności[15]. Pokazuje to skalę problemu.

Mając na uwadze powyższe zagrożenia i wyzwania, konieczne staje się przyjęcie bardziej proaktywnego podejścia. Z punktu widzenia państw europejskich działania na poziomie Brukseli mają szansę przyczynić się do widocznych, pozytywnych działań. Zmiana w tym kierunku staje się coraz bardziej widoczna. W niedawno ogłoszonej propozycji tak zwanego pakietu cyberbezpieczeństwa Unii Europejskiej zaproponowano stworzenie systemu certyfikacji dla produktów i usług z punktu widzenia poziomu cyberbezpieczeństwa[16]. Ideą jest stworzenie dobrowolnego systemu certyfikacji, który ułatwiałby odbiorcom poszczególnych rozwiązań teleinformatycznych wybór tych produktów i usług, które kładą nacisk na cyberbezpieczeństwo. Niewątpliwie byłaby to także pozytywna mobilizacja dla samych wytwórców rozwiązań, którzy mogliby uczynić z bezpieczeństwa swych produktów i usług przewagę konkurencyjną. Innym działaniem podjętym na forum Unii Europejskiej, które ma szansę zwiększyć bezpieczeństwo całego przedsięwzięcia, jakim jest czwarta rewolucja przemysłowa, jest wdrożenie Dyrektywy

Parlamentu i Rady UE w sprawie środków na rzecz wysokiego wspólnego poziomu bezpieczeństwa sieci i systemów informatycznych na terytorium Unii – tak zwanej Dyrektywy NIS[17]. Wskazuje ona sektory w których identyfikowani będą tak zwani dostawcy usług kluczowych, którzy zobligowani będą do wdrażania szeregu działań nakierowanych na bezpieczeństwo. Do sektorów tych zalicza się między innymi: sektor energetyki, transportu, bankowości, służby zdrowia. Ważnym elementem jest to, że państwa członkowskie powinny wdrożyć instrumenty, które pozwolą weryfikować to, czy poszczególni operatorzy rzeczywiście realizują odpowiednie działania na rzecz zwiększania cyberbezpieczeństwa.

Podsumowując, sukces czwartej rewolucji przemysłowej ma szansę powodzenia wyłącznie wtedy, gdy zagwarantowany zostanie jej fundament – bezpieczeństwo. Nie sposób bowiem wyobrazić sobie oparcia kluczowych procesów, systemów na rozwiązaniach niewystarczająco stabilnych i pewnych. Do niedawna aspekt związany z bezpieczeństwem znajdował się na drugim miejscu. Najwyższy czas to zmienić. Będzie to wspólna odpowiedzialność zarówno producentów i dostarczycieli rozwiązań, odbiorców, jak i decydentów, którzy swoimi instrumentami, także regulacyjnymi, mogą przyczynić się do pozytywnych przemian.

Przypisy

1 *Dyrektywa Parlamentu Europejskiego i Rady (UE) 2016/1148 z dnia 6 lipca 2016 r. w sprawie środków na rzecz wysokiego wspólnego poziomu bezpieczeństwa sieci i systemów informatycznych na terytorium Unii*, http://eur-lex.europa.eu/legal-content/PL/TXT/?uri=CELEX%3A32016L1148, dostęp: 08.11.2017.

2 Chylińska K.: *Nowe technologie – Internet Rzeczy*, http://blog.e-odo.pl/2015/10/17/nowe-technologie-internet-rzeczy/, 17.10.2015, [za:] http://iab.org.pl/wp-content/uploads/2015/09/Raport-Internet--Rzeczy-w-Polsce.pdf, dostęp: 23.10.2017.

3 *What is the difference between Internet of Things (IoTs) and cyber-physical systems (CPS)?*, https://www.quora.com/What-is-the-difference-between-Internet-of-Things-IoTs-and-cyber-physical-systems-CPS, dostęp: 23.10.2017.

4 *Digitising European Industry*, https://ec.europa.eu/digital-single-market/en/policies/digitising-european-industry, dostęp: 23.10.2017.

5 Ibidem.

6 Ibidem.

7 *Industry 4.0 Digitalisation for productivity and growth*, http://www.europarl.europa.eu/RegData/etudes/BRIE/2015/568337/EPRS_BRI(2015)568337_EN.pdf, dostęp: 23.10.2017.

8 Ibidem.

9 Ministerstwo Rozwoju, *Plan na rzecz odpowiedzialnego rozwoju*, https://www.mr.gov.pl/media/14840/Plan_na_rzecz_Odpowiedzialnego_Rozwoju_prezentacja.pdf, dostęp: 08.07.2017.

10 *Cyberkultura*, http://cyberkultura.com.pl/cyberkultura, dostęp: 23.10.2017.

11 Chourci N.: *Cyberpolitics in International Relations*, Massachusetts 2012.

12 Castells M.: *Społeczeństwo Sieci*. Wydawnictwo Naukowe PWN, Warszawa 2008.

13 Świątkowska J.: *Cicha wojna*. „Chemia Przemysłowa" 4–5/2015, [za:] Ryba M.: *Rola elementów teleinformatycznych w funkcjonowaniu infrastruktury krytycznej*, [w:] Świątkowska J. (red.) *Bezpieczeństwo infrastruktury krytycznej – wymiar teleinformatyczny*, Instytut Kościuszki, 2014, s. 59.

14 Integrated Solutions, *Jak zapewnić bezpieczne funkcjonowanie Internetu Rzeczy*, http://blog.integratedsolutions.pl/komunikacja-m2m-i-iot/jak-zapewnic-bezpieczne-funkcjonowanie-internetu-rzeczy/, dostęp: 04.07.2017.

15 Ibidem.

16 *Cybersecurity package*, https://ec.europa.eu/info/law/better-regulation/initiatives/com-2017-477_en, dostęp: 23.10.2017.

17 Dyrektywa…, op. cit.

Literatura

[1] Chourci N.: *Cyberpolitics in International Relations*. Massachusetts 2012.

[2] Chylińska K.: *Nowe technologie – Internet Rzeczy*, http://blog.e-odo.pl/2015/10/17/nowe-technologie-internet-rzeczy/, 17.10.2015, [za:] http://iab.org.pl/wp-content/uploads/2015/09/Raport-Internet-Rzeczy-w-Polsce.pdf, dostęp: 23.10.2017.

[3] *Cyberkultura*, http://cyberkultura.com.pl/cyberkultura, dostęp: 23.10.2017.

[4] *Cybersecurity package*, https://ec.europa.eu/info/law/better-regulation/initiatives/com-2017-477_en, dostęp: 23.10.2017.

[5] *Digitising European Industry*, https://ec.europa.eu/digital-single-market/en/policies/digitising-european-industry, dostęp: 23.10.2017.

[6] *Dyrektywa Parlamentu Europejskiego i Rady (UE) 2016/1148 z dnia 6 lipca 2016 r. w sprawie środków na rzecz wysokiego wspólnego poziomu bezpieczeństwa sieci i systemów informatycznych na terytorium Unii*, http://eur-lex.europa.eu/legal-content/PL/TXT/?uri=CELEX%3A32016L1148, dostęp: 08.11.2017.

[7] *Industry 4.0 Digitalisation for productivity and growth*, http://www.europarl.europa.eu/RegData/etudes/BRIE/2015/568337/EPRS_BRI(2015)568337_EN.pdf, dostęp: 23.10.2017.

[8] Integrated Solutions, *Jak zapewnić bezpieczne funkcjonowanie Internetu Rzeczy*, http://blog.integratedsolutions.pl/komunikacja-m2m-i-iot/jak-zapewnic-bezpieczne-funkcjonowanie-internetu-rzeczy/, dostęp: 04.07.2017.

[9] Castells M.: *Społeczeństwo Sieci*. Wydawnictwo Naukowe PWN, Warszawa 2008.

[10] Ministerstwo Rozwoju, *Plan na rzecz odpowiedzialnego rozwoju*, https://www.mr.gov.pl/media/14840/Plan_na_rzecz_Odpowiedzialnego_Rozwoju_prezentacja.pdf, dostęp: 08.07.2017.

[11] Świątkowska J.: *Cicha wojna*. „Chemia przemysłowa" 4–5/2015, [za:] Ryba M.: *Rola elementów teleinformatycznych w funkcjonowaniu infrastruktury krytycznej*, [w:] Świątkowska J. (red.) *Bezpieczeństwo infrastruktury krytycznej – wymiar teleinformatyczny*, Instytut Kościuszki, 2014.

[12] *What is the difference between Internet of Things (IoTs) and cyber-physical systems (CPS)?*, https://www.quora.com/What-is-the-difference-between-Internet-of-Things-IoTs-and-cyber-physical-systems-CPS, dostęp: 23.10.2017.

dr Joanna Świątkowska – Adiunkt, Uniwersytet Pedagogiczny im. KEN w Krakowie, Dyrektor Programowy Europejskiego Forum Cyberbezpieczeństwa, Redaktor Naczelna „European Cybersecurity Journal"

artykuł recenzowany