ZESZYTY NAUKOWE POLITECHNIKI ŚLĄSKIEJ 2015
Seria: ORGANIZACJA I ZARZĄDZANIE z. 80 Nr kol. 1933

Adrian KAPCZYŃSKI
Politechnika Śląska, Wydział Organizacji i Zarządzania
adrian.kapczynski@polsl.pl

INŻYNIEROWIE ZARZĄDZANIA W ŚWIECIE PEŁNYM CYFROWYCH MOŻLIWOŚCI

Streszczenie. W artykule przybliżono pojęcie rewolucji informacyjnej ze szczególnym uwzględnieniem jej skutków, które mogą wpłynąć na zmianę dotychczasowego podejścia do projektowania oraz realizacji procesów przez inżynierów zarządzania. W pracy przedstawiono zagadnienie bezpieczeństwa opartego na ocenie ryzyka będącego efektem zmiany w ramach rewolucji cyfrowej w obszarze paradygmatów informatyki jako dyscypliny naukowej.

Słowa kluczowe: rewolucja informacyjna, cyfrowy świat, inżynieria zarządzania, bezpieczeństwo informacji

MANAGEMENT ENGINEERS IN THE WORLD FULL OF DIGITAL POSSIBILITIES

Summary. The article brought closer to the concept of information revolution with particular emphasis on the effects that can alter the existing approaches and processes for management engineers. The paper presents an example of risk-based security as a chosen effect of changes in one of the paradigms of computer science as a scientific discipline.

Keywords: information revolution, digital world, engineering management, information security

1. Wprowadzenie

W dniu 13 czerwca 2005 roku w Centrum Edukacyjno-Kongresowym Politechniki Śląskiej odbył się mistrzowski wykład Profesora Ryszarda Tadeusiewicza, zatytułowany: „Internet jako źródło przemian cywilizacyjnych”. W trakcie tego wykładu zostały poruszone zagadnienia techniczne dotyczące Internetu, jednakże zasadnicza część wykładu była poświęcona interdyscyplinarnemu tematowi przemian cywilizacyjnych. Podniesiono korzyści

i koszty, jakie wyniknęły z wprowadzenia oraz upowszechnienia się ogólnoświatowej sieci komputerowej, w tym nawiązania do wschodzącego znaczenia cyberterroryzmu na świecie. Profesor Ryszard Tadeusiewicz w drugiej części wykładu – najciekawszej z punktu widzenia zainteresowań autora niniejszego artykułu – przedstawił spostrzeżenia dotyczące wpływu upowszechnienia dostępu do Internetu na życie w miasteczku akademickim Akademii Górniczo-Hutniczej w Krakowie. W szerokim spektrum poruszanych zagadnień dotyczących zmian w funkcjonowaniu społeczności akademickiej w miasteczku AGH wymieniane były liczne zagrożenia oraz zalecenia dotyczące niwelowania skutków materializacji tychże zagrożeń.

Od tamtego dnia minęło blisko 10 lat i oto w dniu 11 marca 2015 roku w Oku Miasta w Katowicach odbyło się spotkanie Śląskiej Kawiarni Naukowej, a gościem red. Rożka był prof. Ryszard Tadeusiewicz. Wśród podniesionych kwestii były skutki toczącej się wojny informacyjnej, aktywności bezzałogowych obiektów latających i ich znaczenie w zapewnieniu bezpieczeństwa oraz jako zagrożenia dla zdrowia i życia ludzkiego.

Oba przedstawione wykłady stały się inspiracją dla autora do wybrania problematyki, która jest interdyscyplinarna, z natury rzeczy stale aktualna i stanowi dobrą ilustrację zmiany wywołanej rewolucją cyfrową, której owoce (w postaci cyfrowych możliwości) istotnie wzbogaciły instrumentarium inżynierów zarządzania.

W niniejszym artykule podniesiono zagadnienia dotyczące rewolucji cyfrowej i jej implikacji. Bogaty zbiór zagadnień z przedmiotowej problematyki postanowiono zilustrować przykładem z obszaru bezpieczeństwa informacji opartego na ryzyku, który przedstawiono w końcowej części niniejszego opracowania.

2. Rewolucja cyfrowa i jej implikacje

Czym jest rewolucja cyfrowa? Dla celów niniejszego artykułu odniesiemy się do definicji, która została sformułowana w pierwszej pracy habilitacyjnej poświęconej tematyce rewolucji cyfrowej [6]. Otóż Piotr Gawrysiak – autor rozprawy – definiuje ją w odniesieniu do wiedzy i jej dostępności. Wiedza to najcenniejsze dobro, którym dysponuje ludzkość, dobro, które jest dostępne dla wszystkich bez ograniczeń. O znaczeniu informacji w życiu społeczeństwa postindustrialnego pisał Alvin Toffler [13], który przybliżył skutki trzeciej fali przemian cywilizacyjnych, determinowanej rozwojem informatyki.

Integracja sieci telekomunikacyjnych, sieci transmitujących dane oraz infrastruktury dystrybucyjnej treści cyfrowe wykreowała nowe możliwości sprzyjające rozwojowi podmiotów, których działalność jest związana z wytwarzaniem oraz oferowaniem produktów

w postaci cyfrowej. Wykreowane produkty cyfrowe wymagają od odbiorcy treści cyfrowych, po pierwsze, dostępu do Internetu, a po drugie, urządzenia, do którego treści cyfrowe będą dostarczane.

Obecnie – poza rozwiązaniami stacjonarnymi – do dyspozycji użytkownika są rozwiązania mobilne, które nie wymagają utrzymania przewodowego połączenia z siecią. Urządzenia mobilne z bezprzewodowym dostępem do sieci w znakomitej większości przypadków zostały skonstruowane z myślą o interakcji człowiek-maszyna (ang. *Man-Machine Interaction*) [11]. W 2015 roku należy jednak uzupełnić wzmiankowaną grupę urządzeń o te rozwiązania sprzętowo-programowe [8], które wraz z wprowadzeniem nowej wersji protokołu komunikacyjnego (ang. *IP Next Generation*) zyskały atrybut autonomicznych urządzeń elektronicznych [3], przygotowanych do realizacji interakcji maszyna-maszyna (ang. *Machine-Machine Interaction*).

Oprócz istotnego postępu w przesyłaniu danych warto zwrócić uwagę na obszar związany z przechowywaniem danych, a w szczególności na trend przechowywania danych w sposób umożliwiający dostęp z dowolnego miejsca i w dowolnym czasie, przy wykorzystaniu dowolnego urządzenia. Przechowywanie danych w sieci w naturalny sposób wykreowało zapytanie o możliwość korzystania z funkcjonalności aplikacji jako usługi. Oznacza to nie tylko zmianę wynikającą z braku konieczności instalacji danej aplikacji na urządzeniu użytkownika (w infrastrukturze przedsiębiorstwa), lecz także zmianę modelu biznesowego (ang. *Pay as you go*, płać w miarę użytkowania).

Rewolucja cyfrowa stworzyła wiele cyfrowych możliwości, których wpływ (z punktu widzenia inżynierów zarządzania) może być postrzegany przez spadek znaczenia pośredników biznesowych, wzrost znaczenia kompetencji cyfrowych czy zmniejszenie barier towarzyszących inicjacji nowego podmiotu gospodarczego.

Na potrzeby niniejszego artykułu opracowano przykład ilustrujący wybrany aspekt (nowego) świata pełnego cyfrowych możliwości.

3. Bezpieczeństwo informacji oparte na ocenie ryzyka

Na wstępie omawiania opracowanego przykładu warto, aby Czytelnik poświęcił czas na przywołanie w pamięci wybranej organizacji ze świata praktyki gospodarczej, którą miał okazję bliżej poznać. Analizując (nawet powierzchownie) procesy główne oraz procesy pomocnicze wybranej organizacji, dostrzegamy przepływy materiałowe oraz przepływy informacyjne. Identyfikujemy zasoby materialne oraz niematerialne, jak również zmianę ich położenia w czasie zarówno w fizycznym układzie tras, jak i cyfrowym systemie nerwowym tejże organizacji. Bez pogłębionych rozważań docieramy do wypracowania spostrzeżeń o znaczeniu tych zasobów w realizacji procesów głównych oraz procesów pomocniczych

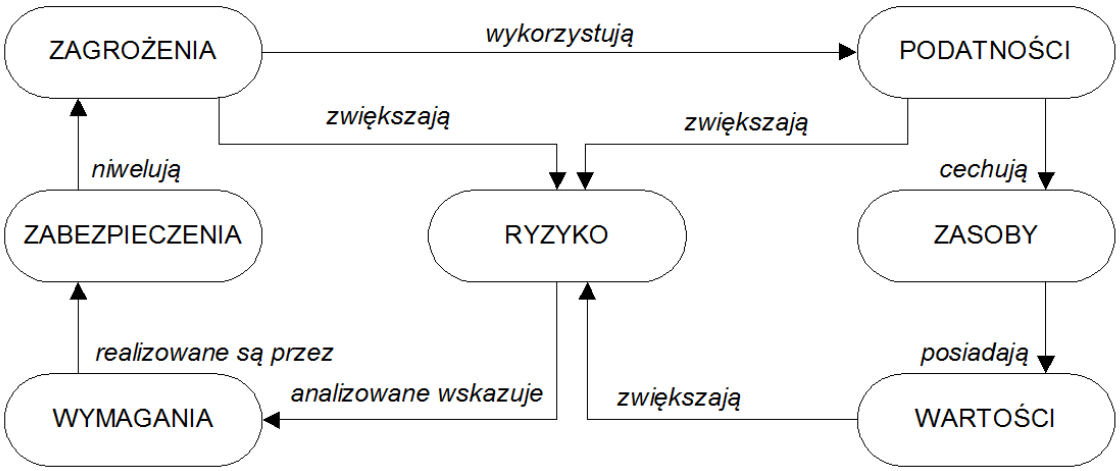
w ramach tej organizacji. Kolejnym i ostatnim krokiem będzie spojrzenie na tę organizację przez pryzmat „stanu równowagi", który jest zapewniany przez stosowanie środków o charakterze przeciwmiarowym dla zmaterializowanych zagrożeń skutkujących wyprowadzeniem rozważanego systemu z równowagi.

W niniejszym przykładzie przyjrzymy się wyłącznie zagadnieniu bezpieczeństwa informacji, co oznacza, że dalszy ciąg rozważań zostanie zawężony do tego obszaru i nie zostaną podjęte bardzo ważne problemy związane z bezpieczeństwem fizycznym i środowiskowym, a także bezpieczeństwem osobowym. Tematyka jest bardzo złożona, ale również dobrze opisana w literaturze przedmiotu, w tym w opracowaniach o charakterze normatywnym. Odwołując się wyłącznie do norm, które są przeznaczone do stosowania w Polsce (a których stosowanie jest dobrowolne), warto wskazać następujące:

- ISO/IEC/TR 13335-1 / PN-I-13335-1, podejmująca zagadnienia obejmujące:
  - wytyczne do zarządzania bezpieczeństwem systemów informatycznych,
  - terminologię, związki między pojęciami,
  - podstawowe modele bezpieczeństwa,
- ISO/IEC/TR 13335-2 / PN-I-13335-2, podejmująca zagadnienia dotyczące:
  - planowania i zarządzania bezpieczeństwem systemów IT,
  - podejść do prowadzenia analizy ryzyka,
  - planów zabezpieczeń,
  - znaczenia szkoleń i działań uświadamiających,
  - stanowisk pracy w instytucji związanych z bezpieczeństwem,
- ISO/IEC/TR 13335-3, poświęcona:
  - technikom zarządzania bezpieczeństwem systemów informatycznych,
  - formułowaniu trójpoziomowej polityki bezpieczeństwa,
  - rozwinięciu problematyki analizy ryzyka,
  - rozwinięciu problematyki implementacji planu zabezpieczeń,
  - reagowaniu na incydenty,
- ISO/IEC/TR 13335-4, traktująca o wyborze zabezpieczeń, uszczegóławiając:
  - klasyfikację i charakterystykę różnych form zabezpieczeń,
  - dobór zabezpieczeń ze względu na rodzaj zagrożenia i rodzaj systemu,
- ISO/IEC/WD 13335-5, omawiająca zagadnienia:
  - zabezpieczenia dla połączeń z sieciami zewnętrznymi,
  - doboru zabezpieczeń stosowanych do ochrony styku systemu z siecią zewnętrzną.

Lektura wymienionych dokumentów pozwala na systematyzację przedmiotowej problematyki, w której kluczowe są pojęcia: zasobów (aktywów mających określoną wartość dla organizacji), zagrożeń (przyczyn niepożądanego incydentu), podatności (słabości zasobów), zabezpieczeń (środków prewencyjnych, detekcyjnych oraz korygujących) oraz

ryzyka (prawdopodobieństwo tego, że określone zagrożenie wykorzysta słabość zasobu w celu spowodowania strat). Związki między tymi pojęciami ilustruje schemat relacji, który przedstawiono na rys. 1.



Rys. 1. Schemat relacji między pojęciami dotyczącymi bezpieczeństwa informacji
Fig. 1. Relations between terms in information security
Źródło: Opracowanie własne na podstawie ISO/IEC TR 13335.

Organizacja ma zasoby o określonej wartości oraz o określonych podatnościach, które są wykorzystywane przez zagrożenia, a które niwelują zabezpieczenia dobrane zgodnie ze zidentyfikowanymi wymaganiami. Centralnym elementem tego schematu związków terminologicznych jest ryzyko.

Klasyczne podejście w ramach zarządzania bezpieczeństwem informacji cechowało się analizą bieżącego stanu wynikającego z procesu prowadzącego do zapewnienia poufności, integralności oraz dostępności informacji. Skupiano uwagę na zagrożeniach polegających na możliwości ujawnienia, modyfikacji, a w szczególności zniszczenia informacji przez podmioty nieuprawnione.

Skutki rewolucji cyfrowej w analizowanym obszarze problemowym znalazły swój wyraz między innymi w ustanowieniu podejścia, w którym ryzyko stanowi podstawę rozważań dotyczących bezpieczeństwa informacji [4, 14]. Bezpieczeństwo oparte na ocenie ryzyka (ang. *risk based security)* podejmuje się zaadresowania potrzeby ochrony konkretnych zasobów przed konkretnymi zagrożeniami z zastosowaniem w zadanym horyzoncie czasowym środków ochrony adekwatnych do zagrożeń oraz do podatności [7]. Oznacza to konieczność określenia źródeł ryzyka (w ramach analizy ryzyka), określenia wielkości ryzyka (w ramach szacowania ryzyka), oceny ryzyka (wyznaczania wagi ryzyka) i wreszcie postępowania z ryzykiem (zastosowanie środków modyfikujących ryzyko) [10].

Autorski przykład przygotowano w obszarze związanym z atrybutem bezpieczeństwa informacji, jakim jest autentyczność, i odniesiono go do człowieka, który wchodzi w interakcję z systemem jako użytkownik tego systemu.

Klasyczne podejście oznaczałoby wybór jednokrotny, wybór jednej z metod uwierzytelniania, opartej na: wiedzy (znajomości hasła), posiadaniu (materialnego identyfikatora) czy też na cechach anatomii lub zachowania człowieka.

W podejściu właściwym dla wymagań współczesnych organizacji, w którym stosuje się **uwierzytelnianie oparte na ocenie ryzyka**, dokonano by doboru relewantnie silnej metody uwierzytelniania w stosunku do wymagań w tym zakresie, właściwym dla danego użytkownika, realizującego uwierzytelnianie w zadanej lokalizacji, w zadanym punkcie w czasie, uzyskującego dostęp do określonych zasobów organizacji. U podstaw przygotowania tych wymagań leżą wyniki przeprowadzonej analizy ryzyka w tym obszarze.

Przy uwzględnieniu dostępnych rozwiązań organizacyjnych oraz technicznych implementacja bezpieczeństwa opartego na ocenie ryzyka w organizacji jest w pełnej rozciągłości możliwa. Uwierzytelnianie oparte na ocenie ryzyka stanowi interesujące zagadnienie, które zostanie podjęte w ramach dalszych prac badawczych.

4. Podsumowanie

W niniejszym artykule przedstawiono skutki rewolucji cyfrowej oraz wskazano jej wybrane implikacje. W szczególności zwrócono uwagę na skutki tej rewolucji w obszarze bezpieczeństwa informacji. Zidentyfikowano tradycyjne (statyczne) podejście, które opiera się na definiowaniu w odniesieniu do systemu oraz danych atrybutów bezpieczeństwa: poufności, integralności i dostępności. Wymagania podmiotów współczesnej praktyki gospodarczej w świetle obecnych zagrożeń oraz dostępnych środków ochrony wskazują na zasadność sięgania do nowego podejścia, które ustanawia ryzyko jako punkt wyjścia do formułowania wymagań dotyczących założeń systemu zarządzania bezpieczeństwem informacji.

Współczesny świat jest pełen cyfrowych możliwości, wśród których dominujące w 2015 roku stają się te, które realizują niewidzialną analitykę danych w organizacji [9, 12]; inteligentne maszyny wspomagające procesy decyzyjne oraz produkcyjne [2, 5], wszechobecna informatyka [1] to tylko wybrane obszary, których innowacyjność kreuje konieczność rozważenia aktualnych paradygmatów stosowanych przez inżynierów zarządzania, kierujących organizacjami w XXI wieku.

Bibliografia

1. Abowd G.D., Mynatt E.D.: Charting past, present, and future research in ubiquitous computing. ACM Transactions on Computer-Human Interaction (TOCHI), Vol. 7, No. 1, 2000.
2. Chaudhuri S., Dayal U., Narasayya V.R.: An overview of business intelligence technology. Commun. ACM, 54(8):88-98, 2011.
3. Chen K., Lien S.: Machine-to-machine communications: Technologies and challenges. Ad Hoc Networks, Vol. 18, 2014.
4. Dissanayaka A., Annakkage U.D., Jayasekara B., Bagen B.: Risk-Based Dynamic Security Assessment. Power Systems, IEEE Transactions on, Vol. 26, Issue 3, 2011.
5. Franceschini N.H.: Small Brains, Smart Machines: From Fly Vision to Robot Vision and Back Again. Proceedings of the IEEE 102(5), 2014.
6. Gawrysiak P.: Cyfrowa rewolucja. Rozwój cywilizacji informacyjnej. Wydawnictwo Naukowe PWN, Warszawa 2008.
7. Grunske L., Joyce D.: Quantitative risk-based security prediction for component-based systems with explicitly modeled attack profiles. Journal of Systems and Software, Vol. 81, Issue 8, August 2008.
8. Gubbi J., Buyya R., Marusic S., Palaniswami M.: Internet of Things (IoT): A vision, architectural elements, and future directions, Future Generation Computer Systems, Vol. 29, Issue 7, 2013.
9. Markarian J., Brobst S., Bedell J.: Critical success factor deploying pervasive bi. Microstrategy 2007.
10. McCalley J., Vittal V., Abi-Samra N.: Overview of risk based security assessment. Proc. 1999 IEEE Power Eng. Soc. Summer Meeting, 1999.
11. Shaer O., Hornecker E.: Tangible User Interfaces: Past, Present, and Future Directions. Foundations and Trends in Human-Computer Interaction, Vol. 3, No. 1–2, 2010.
12. Thompson S.G., Azvine B.: No pervasive computing without intelligent systems, BT Technology Journal, 22, No. 3, 2004.
13. Toffler A.: Trzecia fala. PIW, Warszawa 1997.
14. Viduto V.: Huang W., Maple C.: Toward optimal multi-objective models of network security: Survey. Automation and Computing (ICAC), 17th International Conference, 2011.

Abstract

In the article the author brought closer the issues related with information revolution and its key impacts in our everyday life and illustrates it with example related with information security based on risk.

In the introduction the two references were presented which were the inspiration for selection of information security as basis for further research. The digital opportunities that

may alter the existing approaches and processes from managing engineers point of view have been described in next part of this article. Finally, the author presents the classic and modern approaches to information security. The modern approach is risk-oriented while the traditional one focuses on static definition of security attributes: confidentiality, integrity and availability. The main part of this paper ends with brief example of risk-based authentication which is the area of interest of further research and development.