Tomasz Klasa

Zachodniopomorska Szkoła Biznesu

Monitorowanie bezpieczeństwa systemu informacyjnego organizacji wirtualnej – przegląd stanu prac badawczych

Streszczenie:
Organizacje wirtualne, ze względu na swoje specyficzne cechy, bardzo mocno opierają się na rozwiązaniach teleinformatycznych. W wielu przypadkach systemy informatyczne stanowią wręcz fundament działania tego typu organizacji. Jednocześnie, organizacje te cechuje bardzo duża zwinność i elastyczność – cechy zwykle stojące w sprzeczności z zachowaniem stałego poziomu bezpieczeństwa. Ponieważ tradycyjna forma zarządzania bezpieczeństwem opiera się o długotrwałe, powtarzalne procedury, w organizacji wirtualnej może być konieczna zmiana podejścia. Istotnym elementem procesu zarządzania bezpieczeństwem informacji jest monitorowanie uzyskanych efektów. Także w tym wypadku cechy typowe dla organizacji wirtualnych mogą utrudniać skuteczne i efektywne śledzenie działania wdrożonego systemu zarządzania bezpieczeństwem. W poszukiwaniu uniwersalnego rozwiązania do monitorowania bezpieczeństwa informacji w systemie informacyjnym organizacji wirtualnej przeanalizowano prace z zakresu zarządzania bezpieczeństwem informacji w organizacjach wirtualnych.

Słowa kluczowe: organizacje wirtualne, monitorowanie bezpieczeństwa informacji, zarządzanie bezpieczeństwem

Wprowadzenie

Monitorowanie bezpieczeństwa informacji w tradycyjnej organizacji nie jest zadaniem łatwym i zawsze wymaga solidnego przygotowania. W przypadku organizacji wirtualnych, ze względu na jej unikalne cechy i właściwości, zadanie to staje się jeszcze trudniejsze. Prowadzone są liczne prace nad sposobami zarządzania bezpieczeństwem informacji, ale wiele z nich opiera się o założenia, które znacząco utrudniają lub wręcz uniemożliwiają ich zastosowanie w dynamicznym środowisku organizacji wirtualnej. Ponadto, wiele z istniejących rozwiązań koncentruje się na ocenie i analizie ryzyka, pozostawiając etap monitorowania bezpieczeństwa bez szczegółowego rozpoznania. Dość powszechną praktyką jest też opracowywanie rozwiązań dedykowanych wybranym obszarom funkcjonalnym, np. sieciom komputerowym, co wymusza integrację wielu różnych rozwiązań. Aby ustalić, czy istnieją rozwiązania dostosowane do specyfiki organizacji wirtualnych, cechujące się odpowiednią elastycznością i obejmujące swoim działaniem wszelkie aspekty działalności organizacji wirtualnych, w tym monitorowanie bezpieczeństwa, przeprowadzono analizę aktualnych prac badawczych.

Organizacja wirtualna

Próby zdefiniowania organizacji wirtualnej w zarządzaniu trwają od lat 80-tych XX w. W tym czasie szereg osób wprowadziło własną definicję tego pojęcia, przy czym poszczególne propozycje różnią się diametralnie i odzwierciedlają odmienne obszary badawcze. Jak dotąd, nie udało się uzgodnić jednej, uniwersalnej definicji.

Saabeel, Verduijn, Hagdorn i Kumar[1] dokonali podziału znanych definicji organizacji wirtualnej na dwa podejścia: procesowe i strukturalne.

Do podejścia procesowego zaliczono m.in. [2],[3]:

- organizacja w ciągłej ewolucji, dostosowująca, adaptująca się i odtwarzająca by odpowiadać nowym celom biznesowym[4],
- obszar aktywności biznesowej, w którym główna część zadań jest wykonywana zdalni[5] ,
- nowoczesny model organizacji skupiający się na zasobach niematerialnych; przekształca wiedzę w procesy wytwarzające wartość dodaną[6],
- efekt łączenia i zastosowania różnych koncepcji zarządzania, od just-in-time, przez lean management po zarządzanie zaufaniem [7],
- organizacja, której produkty spełniają potrzeby wirtualne[8],
- przedsiębiorstwo działające w Internecie lub które, oprócz działania na rynku tradycyjnym, działa także na rynku wirtualnym[9],
- organizacja o skrajnym[10].

Wśród definicji o podejściu strukturalnym zaklasyfikowano m.in. [11], [12] :

- tymczasowa sieć niezależnych podmiotów połączonych infrastrukturą IT w celu współdzielenia zasobów, możliwości, kosztów I dostępu do własnych I nowych rynków; kompleksowy system łączący klientów z ich dostawcami[13],
- zestaw wymiennych modułów zbudowany wokół sieci teleinformatycznych, wykorzystujących elastyczne zasoby ludzkie, outsourcing i sieci partnerstwa strategicznego[14].

Innym podejściem do klasyfikacji jest wyróżnienie poziomów organizacji wirtualnych. Pierwotnie wyodrębniono dwa poziomy organizacji wirtualnych [15], [16], zgodnie z którym organizacja na Poziomie 1:

- posiada zdecentralizowaną organizację złożoną z wielu rozproszonych komórek współpracujących za pomocą narzędzi IT,
- nie istnieje jako całość w jednej lokalizacji,
- wszystkie komórki mają fizyczne lokalizacje, ale wszystkie połączenia są wirtualne,
- posiada płaską strukturę zarządzania, z bardziej niezależnymi komórkami i częściowo niezależnymi zespołami.

Poziom 2 organizacji wirtualnej cechuje:

- brak fizycznej lokalizacji – istnieje ona tylko formalnie, łącząc przedsiębiorstwa, jednostki organizacyjne lub osoby w celu osiągnięcia określonych celów biznesowych,
- struktura istnieje tylko do osiągnięcia określonego celu, a nie by utrzymać i rozwijać organizację,
- osiągnięcie celu może oznaczać zamknięcie organizacji.

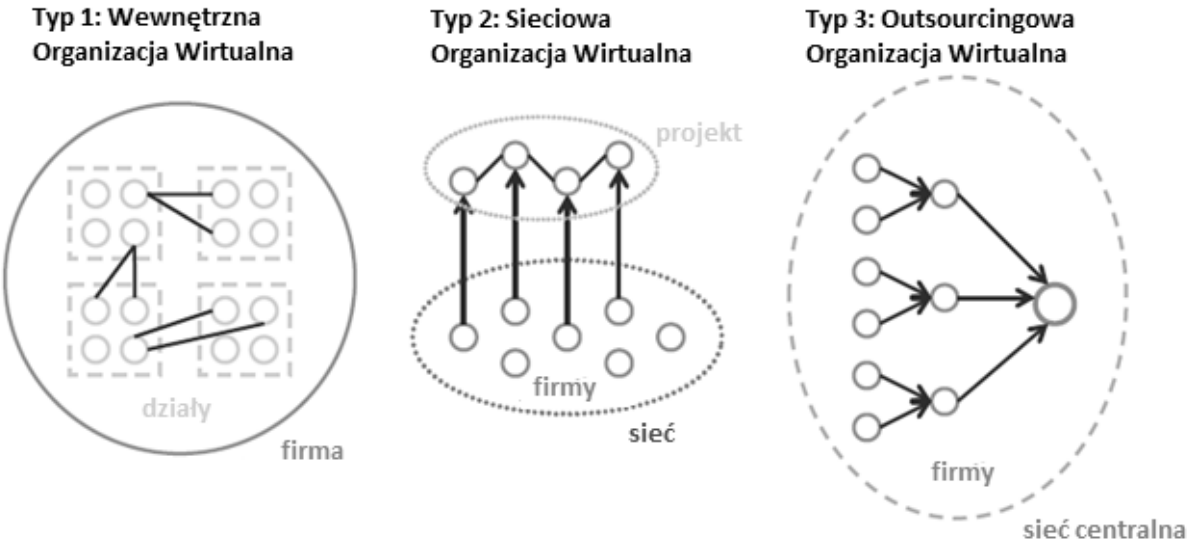
---

[1] W. Saabeel i inni, A model of virtual organization – a structure and process perspective. *Electronic Journal of Organizational Virtualness*. 2002, No1, s. 1-16.
[2] Ibidem
[3] M. Brzozowski, Ewolucja pojmowania wirtualności i definiowanie organizacji wirtualnej. [w:] P. Płoszajski, G. Bełza. Wybory strategiczne firm – nowe instrumenty analizy i wdrażania. Oficyna Wydawnicza Szkoły Głównej Handlowej, Warszawa 2006, s. 121-132.
[4] R. Hale, P. Whitlam, Towards the virtual organization.The McGraw-Hill Companies, Londyn 1997, s. 3.
[5] S. Cohen, On becoming virtual. Training and Development. 1997, 51:5, s. 30-37.
[6] K. Perechuda, Organizacja wirtualna.Ossolineum, Wrocław 1997, s. 7.
[7] Davidow, W. and Malone, M. 1992. The virtual corporation.Harper Business, New York 1992, s. 1-49.
[8] J. Niemczyk, Metody organizacji i zarządzania.Wyd.Terra, Poznań-Wrocław 2000, s. 181.
[9] K. Olejczyk, Organizacja wirtualna. Wykorzystanie Internetu. Nowoczesne zarządzanie przedsiębiorstwem. Politechnika Zielonogórska, Zielona Góra 2000, s. 36.
[10] W. Werther, Structure-driven strategy and virtual organization design. Business Horizons. 1999, issue 42:2, s. 13-18.
[11] W. Werther, Structure-driven strategy and virtual organization design. Business Horizons. 1999, issue 42:2, s. 13-18.
[12] M. Brzozowski, Ewolucja pojmowania… op. cit.
[13] J. Byrne, The virtual corporation, "Business Week" z dnia 8.2.1993, s. 98-103.
[14] W. Anthony i inni, Human resource management. A strategic approach. Dryden Press, Forth Worth 1999, s. 693.
[15] W. Appel, R. Behr, Towards the theory of Virtual Organizations: A description of their formation and figure. Newsletter 1998. 1998, nr 2, s. 23.
[16] M. Brzozowski, Ewolucja pojmowania… op. cit.

Podczas gdy organizacja wirtualna poziomu 1. jest niezależnym tworem, jej odpowiednik poziomu 2. jest sztucznym bytem istniejącym formalnie, zwykle w celu ułatwienia osiągnięcia określonych celów.

Dziesięć lat później, w oparciu o analizę kilkudziesięciu publikacji definiujących pojęcie organizacji wirtualnej wraz z przykładami ich działania pod kątem ponad dwudziestu kryteriów, przeprowadzono ponowną klasyfikację definicji, dzieląc je na trzy poziomy[17]:

- poziom 1: zwirtualizowana korporacja (m.in. międzynarodowe korporacje, wewnętrzna wirtualizacja w sektorze konsultingu),
- poziom 2: wirtualna organizacja sieciowa, (m.in. sieci małych, niezależnych firm współpracujących: z sektora wysokich technologii, grupy freelancerów, grupy wytwarzających oprogramowanie open-source),
- poziom 3: sieć łańcuchów wartości wirtualnych (m.in. organizacje koncentrujące się na podstawowej działalności, a resztę prac zlecające na zewnątrz – ekstremalny outsourcing).



Rysunek 1. Wizualizacja cech strukturalnych trzech poziomów organizacji wirtualnej
Źródło: opracowanie własne na podstawie Riemer, N. Vehring, Should 'virtual' mean 'vague'? … op. cit.

Wskutek braku jednej, ogólnie przyjętej definicji organizacji wirtualnej nie opracowano kompleksowej taksonomii dla organizacji wirtualnych. Putnik i Cruz-Cunha zaproponowali więc rozwiązanie opisujące organizację wirtualną w pięciu wymiarach (wejście, kontrola, wyjście, mechanizm, proces), a także rozszerzony cykl życia organizacji. Rozwiązanie to nie jest kompletne, celowo zostało opracowane z pominięciem zagadnień opisanych wcześniej w literaturze, jednak pozwalając na rozszerzanie go o inne fragmenty[18].

Cechy organizacji wirtualnej a bezpieczeństwo informacji

Organizacje wirtualne zwykle mają ograniczoną infrastrukturę: nieliczne biura i budynki rozproszone na dużym obszarze, często formują sieć biur. Wymagają technologii komunikacyjnych. Typowa dla organizacji wirtualnej jest wysoka elastyczność i błyskawiczne podążanie za nowymi wymaganiami rynku. Towarzyszy temu luźniejsza struktura organizacyjna, często sieciowa lub macierzowa, oparta o zespoły o dynamicznym składzie. Wszystko to wpływa na ryzyko. W tabeli 1 wyróżniono źródła ryzyka typowe dla organizacji wirtualnych[19] (patrz tabela 1).

[17] K. Riemer, N. Vehring, Should 'virtual' mean 'vague'? A plea for more conceptual clarity in researching virtual organisations. Electron Markets. 2012, nr 22, s. 267–282.
[18] G.D. Putnik, M.M. Cruz-Cunha, A Taxonomy for Virtual Enterprises. Journal of Universal Computer Science. 2014, Vol. 20, 6, s. 859-884.
[19] M. Alawamleh, K. Popplewell, Risk Sources … op. cit.

W tradycyjnych organizacjach zagrożenia te są zwykle łatwe do obsłużenia standardowym procesem zarządzania bezpieczeństwem, ale w organizacjach wirtualnych istotnie utrudniają zarządzanie bezpieczeństwem, a w szczególności jego monitorowanie. Działania związane z przeciwdziałaniem zagrożeniom w organizacjach wirtualnych można podzielić na[20]:

- zapewnienie bezpieczeństwa fizycznego, technicznego i informacyjnego,
- zapewnienie technicznej i fizycznej ochrony przekazów informacji.

Ze względu na fakt, że komunikacja w ramach organizacji wirtualnej zazwyczaj odbywa się za pomocą infrastruktury teleinformatycznej, jakiekolwiek problemy techniczne na poziomie sieci skutkują zakłóceniem ciągłości działania organizacji. Jednocześnie, każda z licznych zmian może wpłynąć na uznany wcześniej za bezpieczny stan systemu informacyjnego. Koegzystencja tych dwóch problemów jest zauważalnie trudniejsza do opanowania niż każdy z nich z osobna: np. problem z komunikacją między dwoma zespołami może być skutkiem awarii sieci, albo wynikać ze zmiany składu zespołów i błędnego użycia zasad komunikacji z poprzedniej grupy w nowym zespole. Częste zmiany w organizacji oznaczają też konieczność wdrożenia nieustannego procesu uczenia się wszystkich członków organizacji. Proces ten musi być sprawny, niezakłócony, a jednocześnie w pełni kontrolowany. Każdy podmiot w organizacji wirtualnej musi błyskawicznie otrzymać i przyswoić wiedzę niezbędną do kontynuowania pracy.

W rezultacie dokonując dynamicznego doboru członków zespołu (np. zgodnie z metodą A. Dziurzańskiej[21]) w warunkach ograniczonych zasobów ludzkich trzeba pamiętać o adekwatnym zarządzaniu prawami dostępu do informacji, w tym instrukcji szkoleniowych czy bazy wiedzy.

Źródło ryzyka	Waga
1. Brak zaufania	91%
2. Utrata komunikacji	89%
3. Niewłaściwa umowa o współpracy	87%
4. Współdzielenie informacji	82%
5. Zaangażowanie zarządu	82%
6. Niewłaściwy dobór partnerów	78%
7. Różnice w ontologii	73%
8. Struktura i budowa organizacji	73%
9. Kultura	71%
10. Heterogeniczność partnerów	69%
11. Lokalizacja geograficzna	67%
12. Wiedza o ryzyku	67%
13. Jednoczesna przynależność do wielu organizacji wirtualnych	64%

Tabela 1. Źródła ryzyka wraz z wagami

Źródło: tłumaczenie własne na podstawie M. Alawamleh, K. Popplewell, Risk Sources Identification… op.cit.

W organizacji o tradycyjnym modelu zarządzania na rozwiązanie takich problemów jest zwykle znacznie więcej czasu, co pozwala na metodyczne postępowanie w obliczu każdej zmiany. W przypadku organizacji wirtualnej jakiekolwiek metodyczne podejście do tego problemu, bez wsparcia w postaci znaczącej automatyzacji, spowoduje zablokowanie zmian w organizacji lub procesu uczenia się, a w rezultacie do utraty konkurencyjności. Ponieważ pracownicy powodują 70-80% incydentów bezpieczeństwa[22], [23] (licząc wraz z dostawcami usług i podwykonawcami ponad 90%[24]), a zasoby organizacji wirtualnej stanowią głównie wartości niematerialne i prawne[25], takie jak know-how i wiedza, stwarza to znacznie poważniejsze ryzyko nieuczciwego zachowania pracowników [26].

[20] M. Alawamleh, K. Popplewell, Risk Sources … op. cit.

[21] A. Dziurzańska, Metoda komponowania zespołu. [w:] W. Olejniczak. Zespół – Kultura – Projekt.Wydawnictwo Zachodniopomorskiej Szkoły Biznesu w Szczecinie, Szczecin 2009, s.120-140.

[22] B. Contos, Enemy at the Water Cooler: Real-Life Stories of Insider Threats and Enterprise Security Management Countermeasures. s.l. : Syngress, 2006, s. 3-68.

[23] Trendmicro. 2012. Most data security threats are internal, Forrester says. Trendmicro. http://blog.trendmicro.com/most-data-security-threats-are-internal-forrester-says/.

[24] PWC. 2015. Global State of Information Security Survey 2015. Global State of Information Security Survey.

Rozproszona struktura organizacji wirtualnej utrudnia także ustalenie właściwej jurysdykcji prawnej (związane z pkt. 11 listy zagrożeń, patrz tab. nr 1), ponieważ poszczególne komponenty składowe organizacji wirtualnej mogą podlegać:

- prawu właściwemu dla miejsca rejestracji organizacji wirtualnej (dot. 1. stopnia),
- prawu właściwemu dla miejsca rejestracji zleceniodawcy usługi/zadania, do wykonania której(-go) powołana została organizacja wirtualna (dot. 2. stopnia),
- prawu właściwemu dla lokalizacji infrastruktury IT (serwery, bazy danych),
- prawu właściwemu dla lokalizacji pracowników organizacji wirtualnej.

Ponadto, dane przetwarzane przez organizację wirtualną podlegają standardowym regulacjom m.in. w zakresie ochrony danych osobowych (w Polsce Ustawa o Ochronie Danych Osobowych), ochrony informacji niejawnych (w Polsce Ustawa o Ochronie Informacji Niejawnych). Ponieważ prawne wymagania wobec bezpieczeństwa informacji są zależne od kraju, do ważnych składowych zarządzania bezpieczeństwem informacji w organizacji wirtualnej należy zaliczyć ustalenie, dla każdego elementu systemu informacyjnego, jurysdykcji prawnej właściwej w zadanym czasie. Dopiero na tej podstawie można dobrać właściwy profil zabezpieczeń.

Nie oznacza to jednak, że cechy organizacji wirtualnej tworzą unikalny, nieporównywalny z żadnym innym środowiskiem zbiór. Biorąc pod uwagę rozproszoną strukturę i dynamikę działania zachodzi pewne podobieństwo między zarządzaniem organizacją wirtualną, a zarządzaniem siecią łańcucha dostaw, gdzie zabezpieczenia techniczne nie zwiększą bezpieczeństwa, jeśli[27]:

- organizacja nie jest w stanie ich wykorzystać,
- nie można na nich polegać,
- nie odpowiadają wymaganiom łańcucha dostaw.

Rozwiązanie techniczne nie zapewni wyższego poziomu bezpieczeństwa w organizacji wirtualnej, jeśli jego użycie będzie okresowo niemożliwe (np. ze względu na ograniczony dostęp do sieci). Ponadto, rozwiązanie techniczne, które nie pozwoli na sprawne podążanie za ciągłymi zmianami w strukturze organizacji, nie pozwoli na skuteczne wykrycie ani zinterpretowanie incydentów bezpieczeństwa.

Z kolei posiłkując się porównaniem cech typowej infrastruktury ITC w organizacji typu „biurowego" z systemami automatyki przemysłowej[28], można zauważyć, że organizacje wirtualne zawierają część cech typowych dla każdego z tych dwóch środowisk. Charakterystyka systemu oraz sposób jego utrzymania w organizacji wirtualnej jest zwykle zbliżony do organizacji biurowej, podobnie jak skutki zrealizowania się ryzyka. Jednocześnie praktyki w zakresie zarządzania bezpieczeństwem są zbliżone raczej do stosowanych w systemach automatyki przemysłowej, niż w typowych biurach. Przyczyn takiego stanu rzeczy można szukać w rozproszeniu geograficznym organizacji wirtualnej (utrudnia stosowanie zabezpieczeń fizycznych) oraz mobilności jej zasobów (wpływa na zabezpieczenie łączności). Ponadto, dynamiczny charakter organizacji wirtualnej implikuje niski poziom audytu bezpieczeństwa, a nawet tzw. kultury bezpieczeństwa. Choć przyczyny są inne niż w systemach automatyki przemysłowej, to skutek jest analogiczny.

Analiza istniejących rozwiązań

Przeanalizowano szereg prac, dedykowanych (zgodnie z deklaracją ich autorów) organizacji wirtualnej, reprezentujących różne koncepcje i podejścia do procesu zarządzania bezpieczeństwem. Brano pod uwagę następujące cechy:

- Pokrycie procesu zarządzania bezpieczeństwem – czy rozwiązanie obejmuje wszystkie jego etapy w porównywalnym stopniu?

http://www.pwc.com/gx/en/consulting-services/information-security-survey/key-findings.jhtml.

[25] K. Perechuda, Organizacja wirtualna. Ossolineum, Wrocław 1997, s.7.

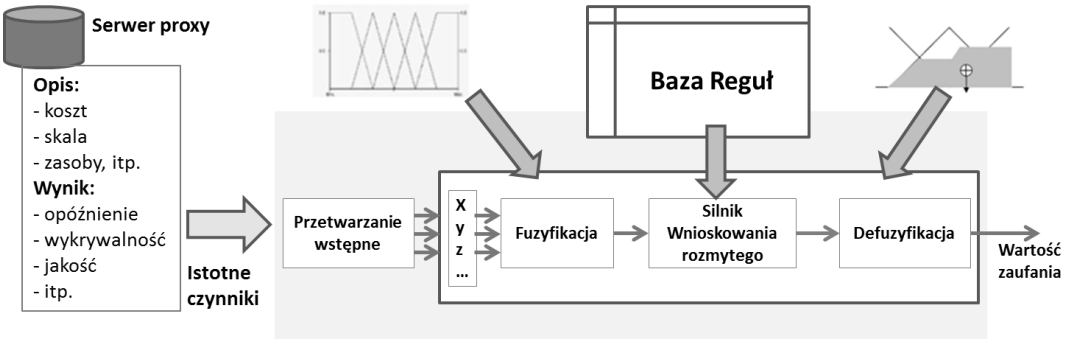
[26] M. Blim, Organizacja wirtualna… op. cit.

[27] H. Salmela i inni, Enhancing supply chain security with vulnerability management and new technology. IET Intell. Transp. Syst. 4, 2010, Vol. 4, s. 307–317.

[28] M. Cheminod i inni, Review of Security Issues in Industrial Networks. IEEE TRANSACTIONS ON INDUSTRIAL INFORMATICS. 2013, Vol. 9, 1, s.277-293.

- Kompleksowość rozwiązania – czy za jego pomocą można obsłużyć wszelkie zasoby organizacji wirtualnej, czy tylko ich część (np. sieć komunikacyjną)?
- Elastyczność rozwiązania – czy pozwala ono na szybką adaptację zgodnie ze zmieniającą się strukturą lub wymaganiami organizacji wirtualnej, czy proces ten nie jest pracochłonny oraz czy jest łatwe to do przeprowadzenia?

Kluczowym warunkiem zapewnienia funkcjonowania organizacji wirtualnej jest zaufanie[29]. Jedną z prób zapewnienia zaufania było wykorzystanie modelu TrustCoM [30] w środowisku dynamicznej organizacji wirtualnej[31]. Wyznaczenie listy parametrów podlegających monitorowaniu oparto o model zapewniający zaufanie w organizacji – integrujący zasoby, usługi oraz użytkowników biorących udział w realizowanych procesach. Inne podejście do zapewnienia zaufania w organizacji wirtualnej stało się podstawą dla próby rozwiązania problemu doboru partnerów tworzących organizację[32]. W tym celu zastosowano model rozmyty oceny zaufania do kandydata (patrz rys. nr 2).



Rysunek 2. Rozmyty model wywodzenia zaufania do kandydata
Źródło: J. Mun i inni… op.cit.

Następnie, sumując tak otrzymane wartości zaufania μRj na poziomie celów, wynikające z powiązanych z tymi celami informacji IEi posiadanych przez kandydata, wyznaczono wartość zaufania do poszczególnych kandydatów. Całość przyjmuje postać wzoru (1):

$$T_S(E_i) = \sum_{j=1}^{N} \delta_j \mu_{Rj}(I_{Ei}). \quad (1)$$

Następnie wyznaczane jest zaufanie do całej organizacji wirtualnej, jako suma zaufania do członków organizacji T_S (E_i) oraz do samej organizacji T_S (〖VO〗 _i):

$$T_{VO}(VO_i) = \alpha \sum_{k=1}^{M} \xi_k T_S(E_k) + (1-\alpha) T_S(VO_i). \quad (2)$$

Porównując otrzymaną wartość zaufania do organizacji, w zależności od dobranych kandydatów, można wskazać skład organizacji wirtualnej o najwyższym dostępnym poziomie zaufania. Model ten nie nadaje się wprost do doboru zakresu monitorowania – wymagał by istotnej adaptacji.

Poszukiwano także sposobu zapewnienia sprawnego funkcjonowania tak zmiennej organizacji, poprzez usprawnienie koordynacji działań i współpracy członków organizacji[33]. Podejmowano także próby klasyfikacji metod i mierników oceny ryzyka w organizacjach wirtualnych, by na tej podstawie wyprowadzić model kontroli ryzyka minimalizujący możliwe straty[34].

[29] M. Alawamleh, K. Popplewell, Risk Sources… op. cit.
[30] T. Dimitrakos i inni, TrustCoM - A Trust and Contract Management Framework enabling Secure Collaborations in Dynamic Virtual Organisations. ERCIM News. 2004, 59 (October 2004) , s. 59.
[31] P. Kearney, Trust and security in virtual organizations. BT Technology Journal. 2006, Vol. 24, 2, s. 209-213.
[32] J. Mun i inni, A goal-oriented trust model for virtual organization creation. Journal of Intelligent Manufacturing. 2011, Vol. 22, s. 345-354.
[33] B.M. Costache i inni, Quality and Risk Management Activities in Virtual Organization. Annals of DAAAM for 2008 & Proceedings of the 19th International DAAAM Symposium. 2008, s.313-314.
[34] N. Wang, Research on Virtual Enterprise Risk Control Based on Optimization. Advanced Materials Research. 2010, Vols. 129-131, s. 1267-1272.

Ponieważ organizacje wirtualne często przyjmują postać struktur macierzowych, szczególnie w zakresie alokacji zadań i uprawnień, istotnym faktem jest, że stwierdzono brak systemów zapewniających weryfikowalność struktur macierzowych [35]. Jako rozwiązanie tego problemu zaproponowano politykę weryfikowalności opartą o kodowany w XML język. Umożliwiło to monitorowanie zadań, a także wykrywanie ataków i anomalii. Pomimo założonej decentralizacji wnioskowania, uznano, że monitorowanie wszystkich elementów systemu w czasie zbliżonym do rzeczywistego jest niemożliwe w tego typu organizacji. Monitorowanie zrealizowano więc jako proces cykliczny, powtarzany z wyznaczoną częstotliwością, określoną mianem okna czasowego TW. Jego wartość wyznaczono jako stosunek rozmiaru kolejki J_max do różnicy średniej liczby zadań J_in w kolejce oraz czasu T wykonania porcji zadań j_out (por. wzór 3).

$$TW = \frac{J_{max}}{\left(\frac{J_{in}}{t}\right) - \frac{c}{\left(\frac{T}{J_{out}}\right)}}. \tag{3}$$

Optymalny rozmiar okna TW, wspólny dla wszystkich węzłów, eksperymentalnie ustalono na 110-210s[36].

Z kolei prace nad gromadzeniem danych prowadzone są przede wszystkim pod kątem doskonalenia modeli danych oraz modeli komunikacyjnych (zwykle jako struktury wieloagentowe[37],[38]). Coraz większą uwagę zaczęto przywiązywać zapewnieniu bezpieczeństwa komunikacji – podstawowym rozwiązaniem stały się modele uwierzytelniania oparte o role, ściśle powiązane z istniejącą polityką bezpieczeństwa oraz własnymi zasadami kontroli [39], [40]. Za rozwinięcie tego podejścia można uznać zapobieganie atakom poprzez wymuszenie dynamicznej autoryzacji, której celem jest zapobieganie atakom równoległym (powtórzenia, podszywanie się pod strony komunikacji[41]) poprzez identyfikację nieuczciwych (wrogich) uczestników komunikacji . Jest to także typowy przykład wykrywania anomalii w oparciu o zasady zawarte we frameworku.

Kolejnym podejściem do wnioskowania o stanie bezpieczeństwa systemu, jest identyfikacja anomalii na podstawie symulacji przepływów za pomocą sieci Petri, a nie w oparciu o statyczny framework. Identyfikacja na podstawie modelu, a nie na podstawie uprzednio zgromadzonych danych, pozwala na wykrycie problemów zanim te faktycznie wystąpią [42]. Niewątpliwą zaletą tego rozwiązania jest ograniczenie nieprawidłowości już na etapie koncepcyjnym. Niestety, ze względu na konieczność aktualizacji modelu wraz wprowadzeniem zmian strukturalnych w organizacji, jest ono trudne w implementacji.

Zupełnie innym kierunkiem doskonalenia wykrywania anomalii jest analiza behawioralna organizacji – możliwe jest wczesne wykrycie prawdopodobnego intruza na podstawie analizy rozbieżności między deklaracjami (słowami) a faktycznymi czynami, z zastosowaniem praw psychologii społecznej. Prowadzone są także prace nad udoskonaleniem rozwiązań opartych o metody wielokryterialne. Przykładem może być metoda oceny ryzyka dla zbioru dostawców usług na podstawie ich współpracy oraz kluczowych mierników procesów dla infrastruktury tworzącej organizację wirtualną: najpierw przeprowadzana jest ocena lokalnego ryzyka za pomocą drzew zdarzeń (ETA), a następnie ocena zagregowanego ryzyka za pomocą metody AHP .

[35] W. Lee i inni, Agent-based accountable grid computing systems. The Journal of Supercomputing. 2013, Vol. 65, 2, s. 903-929.
[36] Ibidem
[37] E. Rigaud, F. Guarnieri, Towards an agent oriented virtual organization dedicated to risk prevention in small and medium size companies. 13th International Workshop on Database and Expert Systems Applications, Proceedings. 2002, s. 280-285.
[38] J. Li i inni, A secure collaboration service for dynamic virtual organizations. Information Sciences. 2010, 180, s. 3086–3107.
[39] Ibidem
[40] N. Wang i inni, Toward SVOPME, a Scalable Virtual Organization Privileges Management Environment. Journal of Physics: Conference Series, International Conference on Computing in High Energy and Nuclear Physics (CHEP 2010). 2011, vol. 331, s. 1-6.
[41] Z. Zhao, An Efficient Anonymous Authentication Scheme for Wireless Body Area Networks Using Elliptic Curve Cryptosystem. Journal of Medical Systems. 2014, 38:13, Feb.2014, s. 1-7.
[42] A. Badr-El-Din, Virtual Organizations, the Organic Structure and Petri Nets. Vision 2020: Sustainable Growth Economic Development and Global Competitiveness. 2014, Vols. 1-5, s. 551-559.

Wnioski

W świetle cech organizacji wirtualnych oraz typowych problemów z nimi związanych, można zauważyć, że zarządzanie bezpieczeństwem informacji zgodnie z modelem PDCA (np. wg (ISO/IEC27001:2013)) jest znacząco utrudnione. Podstawowym problemem jest zbyt długotrwały proces analizy i oceny bezpieczeństwa informacji, poprzedzający wdrożenie odpowiednich środków zaradczych. Trwa on na tyle długo, że w wielu przypadkach niemożliwe będzie dokończenie go zanim badany system informacyjny ulegnie kolejnej zmianie. Tradycyjne organizacje zmieniają się stosunkowo powoli – na potrzeby audytu możliwe jest zapewnienie na przykład dwumiesięcznego okresu bez wprowadzania jakichkolwiek zmian w organizacji. W przypadku organizacji wirtualnej takie założenie jest praktycznie niemożliwe do wdrożenia. Ponadto, zmienność właściwej jurysdykcji prawnej może wręcz uniemożliwić zarządzanie bezpieczeństwem informacji zgodnie z PDCA.

Bezpieczeństwo informacji w organizacjach wirtualnych jest przedmiotem wielu prac badawczych – szereg opracowań w tym zakresie powstało w ciągu kilku ostatnich lat, co potwierdza aktualność zagadnienia. Część prac bazuje na pojęciu zaufania (ang. trust), a więc dąży do utrzymania stanu systemu uznawanego jako zaufany, a nie zapewnienia stanu uznanego jako bezpieczny. Choć pojęcia te są zbliżone, nie są tożsame, co sprawia, że rozwiązania oparte o zaufanie wymagają odpowiedniej adaptacji, by mogły być zastosowane w procesie zarządzania bezpieczeństwem. Powstają także rozwiązania ograniczone do wybranych aspektów bezpieczeństwa systemu organizacji wirtualnej, np. służące kontroli dostępu, czy zabezpieczeniu komunikacji. Prowadzone są także prace nad wykrywaniem anomalii w organizacjach wirtualnych, skoncentrowane na specyficznych cechach ich funkcjonowania. Podobnie jak w przypadku tradycyjnych organizacji, prace badawcze są prowadzone punktowo, w wybranych obszarach. Zwykle celem jest osiągnięcie wyższej skuteczności wykrywania anomalii albo skuteczniejsze zabezpieczenie informacji czy komunikacji. M.in. ze względu na mnogość definicji organizacji wirtualnej i wynikające z tego faktu zróżnicowanie podejścia do tego zagadnienia, poszczególne prace nie tworzą spójnej całości. Nie stwierdzono także prowadzenia badań, których celem jest integracja wielu aspektów bezpieczeństwa organizacji wirtualnej. Uzasadnione jest więc podjęcie próby wyznaczenia modelu referencyjnego zintegrowanego systemu monitorowania bezpieczeństwa organizacji wirtualnej.

Information security monitoring in a virtual organizations' information system – state of the art review

Summary:
Virtual organizations, due to their specific character, rely strongly on ICT. In many cases, IT systems form a real foundation of such an organization. At the same time, such organizations are very flexible and agile, which is in contrary to sustaining steady level of security. Because of that, implementation of information security management system in a virtual organization may require significant change of approach, as traditional form relies on long-lasting, cyclic procedures. A significant element of the information security management proces is monitoring of obtained results. Also in this case, the character of a virtual organization may prevent from successful and effective following activity of implemented security management system. When searching for a universal solution of security monitoring for virtual organizations, current state of the art focusing on security management in virtual organizations was analyzed.

Keywords: virtual organizations, information security management, security management