CZŁOWIEK W ZESPOŁACH WIRTUALNYCH A BEZPIECZEŃSTWO W ZARZĄDZANIU INFORMACJĄ

<https://doi.org/10.33141/po.2019.07.08>

Paweł Kobis

Przegląd Organizacji, Nr 7 (954), 2019, ss. 57-64

www.przegladororganizacji.pl

©Towarzystwo Naukowe Organizacji i Kierownictwa (TNOiK)

Wprowadzenie

Niesłabnąca konkurencyjność przedsiębiorstw powoduje poszukiwanie coraz nowszych sposobów na osiągnięcie sukcesu gospodarczego, zwiększenie przychodów i zmniejszenie kosztów. Rozwój technik i technologii informatycznych multiplikuje narzędzia, których odpowiednie użycie może usprawnić procesy zarządzania informacją.

Zarządzanie informacją jest obecnie obszarem, który bezpośrednio wpływa na pozycję podmiotu gospodarczego na rynku (Jędrzejczyk, Kucęba, 2010, s. 286). Informacja, jako jeden z głównych czynników kreujących sukces organizacji gospodarczej, musi być aktualna, wartościowa, odpowiednio przetworzona i bezpiecznie magazynowana w zasobach systemu informatycznego, z którego korzysta podmiot gospodarczy.

Obecnie sposoby korzystania z zasobów informacji przedsiębiorstwa wymagają w przeważającej liczbie przypadków użycia komputera stacjonarnego lub urządzenia mobilnego. Informacje, przechowywane w postaci cyfrowej mogą być udostępniane, przesyłane praktycznie bez żadnych ograniczeń w zakresie ich liczby oraz ograniczeń przestrzennych. Jedynym warunkiem zdalnego przetwarzania informacji jest zapewnienie odpowiednich warunków bezpieczeństwa. Zasoby informacyjne są najłatwiejszym aktywem do przechwycenia i skopiowania przez potencjalną konkurencję (Olszak, 2018, s. 38), wymagają więc szczególnej ochrony.

Przetwarzanie informacji odbywa się na różnych szczeblach zarządzania organizacją oraz w różnych obszarach działalności podmiotu. Jednym z takich obszarów są tzw. zespoły wirtualne. Wspólna praca osób oddalonych od siebie o znaczne odległości geograficzne wymaga stosowania najnowocześniejszych rozwiązań z dziedziny telekomunikacji i informatyki. Jednocześnie wymaga stosowania szczególnych zasad dbania o bezpieczeństwo informacji, która przy tego typu działalności przesyłana jest wielokrotnie w krótkich odstępach czasu na duże odległości obejmujące niejednokrotnie poszczególne kontynenty.

Celem opracowania jest przedstawienie koncepcji zespołów wirtualnych, których funkcjonowanie jest możliwe i w pełni zależne od technik oraz technologii informatycznych i komunikacyjnych. Szczególny nacisk położono na bezpieczeństwo przetwarzania informacji z uwzględnieniem czynnika ludzkiego. W artykule za-

prezentowano współcześnie funkcjonujące modele informatyczne wspierające pracę zespołów. Opisano elementy funkcjonalne, dzięki którym możliwe są tzw. spotkania wirtualne. Szczególną uwagę zwrócono na najważniejsze zagadnienia dotyczące ich bezpieczeństwa. W części empirycznej opisano również aktualne badania dotyczące omawianych aspektów bezpieczeństwa przeprowadzone przez uznane wywiadownie gospodarcze na świecie.

Istota i cechy zespołów wirtualnych

Aby zdefiniować zespół wirtualny, należy przytoczyć pojęcie tradycyjnego zespołu roboczego. Zespoły tworzone są na podstawie grup roboczych składających się z indywidualnych osób. W przypadku przedsiębiorstwa jest to określona grupa pracowników. W zespole, w przeciwieństwie do grupy, istnieje dążenie do wspólnego celu, wzajemne uzupełnianie się ról, które wynikają ze zróżnicowania funkcjonalnego i podziału pracy (Sikorski, 2005, s. 4). Członkowie zespołu roboczego, poprzez wspólne działania, rozwiązują określone problemy zmierzając do osiągnięcia nakreślonych zamierzeń. Zespół w odróżnieniu od grupy jest tworem uformowanym z wypracowanymi relacjami opartymi na zaufaniu, wiedzy, doświadczeniu i współzależności (Pyszka, 2015, s. 36–54 za: Kopertyńska, Kmiołek, 2018, s. 52; Sukiennik i in., 2017, s. 48). Tradycyjny model zespołu funkcjonuje w obrębie danej organizacji gospodarczej lub w kilku nieznacznie oddalonych jej oddziałach. Domeną tego modelu są wzajemne, bezpośrednie, cykliczne spotkania. Obecnie, w czasach informacji w postaci cyfrowej, większość członków tradycyjnego zespołu roboczego używa nowych technik i technologii zarządzania informacją, może komunikować się za pomocą nowych form przekazu audio i wideo, ale w przypadku braku dostępu do rozwiązań teleinformatycznych (np. awarii) dalej może bez przeszkód realizować założone cele i pracować zespołowo.

Zespół wirtualny ma w zasadzie te same założenia funkcjonalne co tradycyjny zespół roboczy. Zasadniczą różnicą jest forma komunikacji pomiędzy członkami zespołu. Szczegółową definicję zespołu wirtualnego podał T. Oleksyn (2006, s. 175): „Zespoły wirtualne obejmują osoby, które rzadko spotykają się twarzą w twarz, niekiedy nie widzą się nigdy. Mogą je tworzyć ludzie pracujący

w różnych oddziałach, a nawet na różnych kontynentach, którzy wymieniają informację, tworzą wspólnie określone koncepcje i projekty, korzystając z komputerów i najnowszych systemów IT. Pozwala to przezwyciężyć ograniczenia czasowe i przestrzenne. Zespoły wirtualne nie są optymalną formą działania i współpracy – przede wszystkim z powodu ograniczeń w komunikacji. Ginią tu w dużym stopniu przekazy niewerbalne, słabo są ujawniane uczucia i emocje, współpracujący ludzie właściwie prawie się nie znają. Jednak zespoły te są często jedyną okazją do nawiązywania efektywnej współpracy ludzi, którzy w inny sposób – bez pośrednictwa komputerów, łączności satelitarnej – zupełnie nie byłoby w stanie współdziałać”.

Istnienie i funkcjonowanie zespołów wirtualnych jest więc w całości uzależnione od systemów IT (*Information Technology*). Brak systemu jest jednoznaczny z brakiem funkcjonowania zespołu. Jest to podstawowa i najważniejsza różnica między zespołem tradycyjnym a wirtualnym. Wśród zalet funkcjonowania zespołów wirtualnych można wymienić (DuFrene, Lehman, 2012, s. 5; Hunsaker, Hunsaker, 2008, s. 87–89; Stefaniuk, 2010, s. 154, 2014, s. 28–36 za Krawczyk-Bryłka, 2016, s. 100):

- możliwość pozyskiwania do zespołu i realizacji zadań osoby z dowolnej lokalizacji geograficznej – brak ograniczeń odległościowych;
- oszczędności wynikające z braku potrzeby dojazdu do fizycznego miejsca spotkania zespołu;
- nienormowany czas pracy – elastyczność w doborze godzin pracy;
- zmniejszenie liczby krótkotrwałych zwolnień lekarskich pracowników;
- skrócenie czasu realizacji zadań i zwiększenie wydajności pracy zespołu;
- innowacyjność w realizacji zadań wynikająca z różnorodności kulturowej członków zespołu;
- zmniejszenie barier w wykonywaniu pracy dla szczególnych grup pracowników, na przykład osób niepełnosprawnych;
- działanie proekologiczne wynikające z redukcji transportu pracowników;
- możliwość jednoczesnego uczestniczenia w kilku zespołach;
- możliwość szybkiej wymiany informacji.

Do wad funkcjonowania zespołów wirtualnych można zaliczyć:

- zależność jakości funkcjonowania zespołu od zaawansowania technologicznego narzędzi informatycznych;
- konieczność przerywania pracy w przypadku jakiegokolwiek awarii sieci komunikacyjnej;
- istniejące bariery stref czasowych (konieczność pracy w nocy lub w trybie off-line);
- bariery kulturowe pomiędzy członkami zespołu;
- możliwe bariery językowe;
- niezbędny wysoki poziom samokontroli i samodyscypliny wśród członków zespołu (brak formalnego nadzoru);
- konieczność zapewnienia wysokiej jakości zabezpieczeń dla przysyłanej informacji.

Wśród wymienionych zalet i wad funkcjonowania zespołów wirtualnych najważniejszy z punktu niniejszego artykułu jest aspekt zarządzania informacją, a w szczególności jej bezpieczeństwo w świetle używanych technik i technologii oraz tzw. czynnika ludzkiego (Kobis, Kisiołek, 2018, s. 45).

Praca w zespołach wirtualnych jest formą telepracy. Pozwala pracownikom samodzielnie (w określonych i narzuconych przez pracodawcę granicach) organizować własną pracę. Dla coraz większej liczby pracowników jest to duży atut przy wyborze pracodawcy. Według badań przeprowadzonych przez Instytut Gallupa (2017, s. 27) wynika, że ponad połowa (53%) badanych pracowników podczas podjęcia nowej pracy bierze pod uwagę pracę zdalną, dającą możliwość osiągnięcia większej równowagi między życiem zawodowym a prywatnym. W tym samym badaniu 51% pracowników którzy już pracują, deklaruje chęć zmiany na zajęcie, które oferowałoby im elastyczny czas pracy, a 37% zmieniłoby pracę na taką, którą mogliby wykonywać w dowolnym miejscu. Należy oczywiście zaznaczyć, że możliwość wyboru między pracą „stacjonarną” a zdalną jest ściśle zależna od branży oraz obszaru usług. Nie wszystkie bowiem dają się realizować w modelu telepracy.

Modele informatyczne wspierające działalność zespołów wirtualnych

Obecnie można wyróżnić 3 modele informatyczne stanowiące środowisko dla funkcjonowania zespołów wirtualnych. Modele zawierają zarówno część struktury informatycznej odpowiedzialnej za przechowywanie i przetwarzanie informacji, jak i część komunikacyjną pomiędzy jej członkami. Są to:

- model tradycyjny IT;
- model cloud computing (CC);
- model mieszany zawierający struktury obu powyższych.

Tradycyjny model IT (rys. 1, prostokąt 1) opiera się na stworzeniu własnego zaplecza informatycznego pozwalającego na udostępnianie i przetwarzanie informacji z dowolnych lokalizacji na świecie. Nakłada na przedsiębiorstwo konieczność zapewnienia bezpieczeństwa informacji zarówno na płaszczyźnie zarządzania informacją z zewnątrz, jak i na płaszczyźnie przesyłania jej pomiędzy uczestnikami zespołu.

Model cloud computing (rys. 1, prostokąt 2) pozwala na stworzenie struktury informatycznej opartej na usługach świadczonych przez zewnętrzne firmy informatyczne (Kobis, Chmielarz, 2017). Przedsiębiorca tworząc zespoły wirtualne udostępnia środowisko pracy, które pod względem bezpieczeństwa i bezawaryjnej pracy monitorowane jest przez dostawcę (Kiełtyka, 2017, s. 36). Sam monitoruje tylko poziom wydajności, zmniejszając lub zwiększając określone zasoby w jednostkach czasu (połączenie d). W przypadku pracowników zdalnych jest to rozwiązanie wygodne i relatywnie bezpieczne, choć bezpieczeństwo chmury obliczeniowej jest od dawna tema-

tem wielu dyskusji naukowych nacechowanych wieloma przeciwieństwami. Kanały komunikacyjne w tym modelu są zabezpieczane zarówno ze strony usługodawcy chmury obliczeniowej, jak i poszczególnych odbiorców, czyli pracowników zespołu wirtualnego.

Na rysunku 1 przedstawiono w ogólnym zarysie wymianę informacji w poszczególnych modelach (model 1 i model 2). Pokazano relacje pomiędzy obszarami, oznaczając kierunki wymiany informacji (a, b, c, d).

Rys. 1. Modele informatyczne wspierające działalność zespołów wirtualnych funkcjonujące w organizacjach gospodarczych gdzie:

1 – model tradycyjny IT;

2 – model cloud computing;

U1, U2, U3, Un – uczestnicy zespołu wirtualnego;

a, b, c, d – kanały wymiany informacji pomiędzy elementami składowymi modeli;

Źródło: opracowanie własne

Bezpieczeństwo informacji w obszarach działania zespołów wirtualnych

Podejście do bezpieczeństwa zarządzania informacją jest ściśle związane z wykorzystywanym w przedsiębiorstwie modelem IT. Podmiotem w każdym z nich jest zespół wirtualny. Od postaw, zachowania, wyszkolenia pracowników należących do zespołu zależy w głównej mierze bezpieczeństwo zasobów cyfrowych organizacji. Informacja wymieniana pomiędzy członkami zespołu (rys. 1, połączenia a) jest bowiem przesyłana w sieci Internet, która jest siecią publiczną, powodującą ryzyko przechwycenia lub uszkodzenia transmisji cyfrowej. Ponadto, poza samym przesyłaniem, poszczególni członkowie zespołu przechowują, nadają i odbierają informacje za pomocą urządzeń komputerowych, nad którymi nie ma kontroli podmiot gospodarczy. Komputery te, często oprócz działań w obszarze zespołu wirtualnego używane są na wielu innych płaszczyznach, również do celów tzw.

„domowych”, co dodatkowo zwiększa ryzyko. Użytkownicy, wykorzystujący sprzęt komputerowy do zastosowań domowych, często nie zwracają uwagi na wiele istotnych aspektów:

- odpowiedniego zabezpieczania komputera przez dostępem osób niepowołanych (np. członków rodziny, znajomych);
- odpowiedniego zabezpieczenia antywirusowego, antymalware, antyspamowego;
- ustanawiania bezpiecznych haseł lub innych danych uwiarygadniających (np. biometrycznych);
- instalowania oprogramowania, które może mieć negatywne skutki w procesach komunikacji z serwerami przedsiębiorcy;
- zapewnienia bezpiecznego łącza komunikacyjnego, do którego nie mają dostępu osoby niepowołane (w skrajnych przypadkach używanie publicznych hot-spotów).

W przypadku tradycyjnego modelu IT użytkownicy korzystają z zasobów informacyjnych przechowywanych w obrębie danej organizacji gospodarczej. Połączenie (rys. 1, połączenie b) z zasobami odbywa się poprzez łącza telekomunikacyjne, których poziom zabezpieczenia w każdym przypadku jest nieznan. Trudno bowiem dokładnie przeanalizować drogę poszczególnych pakietów danych. Mogą to być łącza szerokopasmowe, telefonii komórkowej, łącza kablowe, naziemne, satelitarne itd. Różnorodność połączeń wymusza stosowanie odpowiedniego szyfrowania transmisji, o które powinni zadbać zarówno sami członkowie zespołu wirtualnego, jak i dział IT udostępniający poszczególne zasoby. Dział IT odpowiedzialny jest ponadto, lub przede wszystkim, za bezpieczne udostępnianie zasobów przedsiębiorstwa. Na specjalistach IT ciąży odpowiedzialność stworzenia określonej hierarchii dostępu do informacji, stworzenia poziomów uwiarygodnienia użytkowników oraz nadzoru nad prawidłowym korzystaniem z zasobów i zabezpieczania ich w razie wystąpienia jakiegokolwiek awarii.

W modelu cloud computing aspekty bezpieczeństwa z przesyłaniem informacji pomiędzy członkami zespołu wirtualnego a chmurą obliczeniową (rys. 1, połączenie c) są praktycznie takie same jak w modelu tradycyjnym IT. Liczba nośników danych może być dowolna. W modelu tym zmienia się jednak odpowiedzialność po stronie udostępnianych informacji. Za zapewnienie bezpiecznego dostępu, ustalenie jego hierarchii, poziomów uwiarygodnienia odpowiada zarówno przedsiębiorca, jak i w dużym stopniu usługodawca cloud computingu. Ogólnie można stwierdzić, że usługodawca zapewnia bezpieczeństwo techniczne, natomiast przedsiębiorca, jako klient usługi, bezpieczeństwo organizacyjne związane z nadzorem IT (rys. 1, połączenie d).

Bezpieczeństwo informacji w każdym modelu informatycznym wymaga współdziałania ze sobą wszystkich elementów systemu bezpieczeństwa. Są to zabezpieczenia fizyczne (nieomawiane w niniejszym artykule), zabezpieczenia techniczne (programowe, sprzętowe), zasady zarządzania informacją w organizacji (polityka bezpieczeństwa, instrukcja zarządzania systemem informatycznym),

określone akty prawne (np. Rozporządzenie o Ochronie Danych Osobowych – RODO). Za organizacją, konfiguracją i należytych wdrożeniem wszystkich elementów bezpieczeństwa stoi człowiek, jego postawa, doświadczenie, przeszkolenie i profesjonalizm. Brak należytych postaw pracowniczych wynikających z wielu czynników socjologicznych, psychofizycznych oraz brak odpowiedniego, cyklicznego przeszkolenia oraz wiedzy może prowadzić do sytuacji, w której najnowocześniejsze zabezpieczenia techniczne zawodzą. Narastająca na rynku gospodarczym konkurencyjność wśród podmiotów gospodarczych wzmaga ponadto działania wywiadów gospodarczych, prób przekupstwa i podkupienia pracowników oraz wszelkich działań socjotechnicznych na pracownikach w celu kradzieży lub zniszczenia zasobów informacyjnych. W przypadku pracy stacjonarnej w przedsiębiorstwach istnieje pewnego rodzaju nadzór (w mniejszym lub większym stopniu) nad pracownikiem. W przypadku pracy zdalnej, występującej w zespołach wirtualnych, takiego nadzoru nie ma. Przykładowo, przy braku odpowiedniego przeszkolenia do przechwycenia informacji przez konkurencję mogą przyczynić się działania socjotechniczne, nieuwaga, lekkomyślność, natomiast przy niezadowoleniu z pracy do przechwycenia informacji może przyczynić się podkupienie pracownika, który następnie sam stanie się źródłem informacji dla osób trzecich. Bardzo często możliwości ku temu stwarza również fakt, że osoba pracująca zdalnie świadczy swoje usługi na rzecz różnych podmiotów gospodarczych. Według badania KPMG (2019, s. 5), czynnik ludzki w obszarze bezpieczeństwa jest największym wyzwaniem dla współczesnych przedsiębiorstw (63% wskazań wśród badanej populacji).

Bezpieczeństwo informacji dotyczące obszarów funkcjonowania zespołów wirtualnych – wyniki badań

W badaniach dotyczących bezpieczeństwa informacji w procesach funkcjonowania zespołów wirtualnych należy stosować podejście cechujące się analizą

badan poszczególnych obszarów, wyszczególnionych na rysunku 1, takich jak:

1. Bezpieczeństwo przekazywania informacji przez sieć Internet.
2. Bezpieczeństwo korzystania z informacji przechowywanej w sieci lokalnej przedsiębiorstwa.
3. Bezpieczeństwo związane z użyciem urządzeń mobilnych.
4. Bezpieczeństwo korzystania z informacji przechowywanej w chmurze obliczeniowej.

W niniejszym podrozdziale przedstawiono badania dotyczące bezpieczeństwa informacji w wymienionych wyżej obszarach przez uznane wywiadownie gospodarcze na świecie.

Przekazywanie informacji poprzez sieć globalną związane jest bezpośrednio z narzędziami, które są do tego celu wykorzystywane. Kluczowym zagadnieniem jest odpowiednie szyfrowanie wysyłanych i odbieranych informacji. Przekazywanie informacji w sieci można ogólnie podzielić na 2 kategorie: informacje związane z komunikacją pomiędzy członkami zespołu (komunikatory internetowe) oraz informacje związane z przesyłanymi plikami oprogramowania roboczego (tworzenie bezpiecznych kanałów VPN). W przypadku komunikacji z użyciem komunikatorów za bezpieczne można uznać oprogramowanie, które zapewnia szyfrowanie typu E2E (End to End), czyli na całej drodze komunikacji pomiędzy osobami. Na rysunku 2 przedstawiono najczęściej wykorzystywane na świecie oprogramowanie komunikacyjne według badania firmy Statista (2019) (stan na kwiecień 2019 roku). Przedstawione dane dotyczą wprowadznie wszystkich użytkowników (prywatnych i instytucjonalnych), pozwalają jednak nakreślić ogólne spojrzenie na rodzaj używanego na świecie oprogramowania i jego bezpieczeństwo w chwili publikacji niniejszego artykułu.

Spośród wymienionego na rysunku oprogramowania pełne szyfrowanie w chwili pisania artykułu zapewniały takie aplikacje, jak: WhatsApp, Facebook Messenger, Snapchat oraz Viber. Szyfrowanie/desyfrowanie odbywa się na urządzeniu odbiorcy i nadawcy, stąd podsłuchiwanie rozmowy staje się praktycznie niemożliwe. Poszczególne

Rys. 2. Użycie komunikatorów internetowych na świecie liczona w milionach użytkowników na miesiąc
Źródło: opracowanie własne na podstawie: Statista, 2019

funkcje dotyczące bezpieczeństwa komunikatorów zmieniają się bardzo dynamicznie, stąd dogłębna analiza oprogramowania w niniejszym artykule nie wydaje się być celowa. Używanie oprogramowania do komunikacji bez szyfrowania generuje ryzyko podsłuchania rozmów, a tym samym kradzież informacji.

Bezpieczne przesyłanie informacji w postaci elektronicznej w sieci globalnej zapewnia tworzenie tzw. kanałów VPN (*Virtual Private Network*). Dostępne są różne standardy tworzenia takich sieci, różniące się przede wszystkim poziomem bezpieczeństwa w zakresie komunikacji sieciowej. Na rysunku 3 przedstawiono globalne użycie wirtualnych sieci prywatnych (VPN) z podziałem na poszczególne regiony w pierwszym kwartale 2018 roku.

Największy udział procentowy zaobserwować można w Azji i Pacyfiku. Wśród użytkowników krajów europejskich tylko co 6 użytkowników zabezpieczał transmisję przed możliwą utratą lub przejęciem informacji. Jest to stosunkowo niski wskaźnik, uwzględniając obecny poziom cyberprzestępczości w Internecie. Tworzenie bezpiecznych

kanałów VPN powoduje odseparowanie przesyłanych informacji od pozostałych sygnałów w sieci, a uzupełnienie kanału o szyfrowanie uniemożliwia odczytanie treści przez osoby niepowołane.

Kolejne badanie, przeprowadzone przez KPMG (rys. 4), opublikowane w kwietniu 2019 roku, pokazuje największe cyberzagrożenia w opinii przedsiębiorców powodujące utratę lub kradzież informacji. Badanie to ilustruje zarówno bezpieczeństwo informacji w sieci lokalnej, jak i bezpieczeństwo informacji związane z używaniem urządzeń mobilnych.

Respondenci za zagrożenia niosące najwyższe ryzyko dla przedsiębiorstwa uznali utratę informacji za pośrednictwem złośliwego oprogramowania (malware), kradzież informacji przez pracowników oraz możliwość wyłudzenia opłat z użyciem kampanii ransomware, czyli szyfrowania informacji na komputerach użytkowników. Wszystkie trzy typy zagrożeń związane są bezpośrednio z działaniem czynnika ludzkiego. Oprócz ewidentnego czynnika ludzkiego, jakim jest kradzież, zagrożenia typu

Rys. 3. Wykorzystanie VPN i serwerów proxy wśród użytkowników Internetu na całym świecie oraz w poszczególnych regionach w pierwszym kwartale 2018 roku

Źródło: opracowanie własne na podstawie: Statista, 2018

Rys. 4. Klasyfikacja największych zagrożeń dla organizacji w 5-stopniowej skali ryzyka

Źródło: opracowanie własne na podstawie: KPMG, 2019, s. 9

malware oraz ransomware najczęściej związane są z niską świadomością użytkowników w zakresie bezpieczeństwa przetwarzanych informacji. Wynika ona z braku odpowiedniego przeszkolenia kadry pracowniczej oraz z działań socjotechnicznych agresora. Nieświadomi użytkownicy, poprzez działania typu: otwieranie wiadomości email niewiadomego pochodzenia, instalowanie oprogramowania z nieznanych źródeł itp., stają się ogniwem w procesie zarażania stanowisk komputerowych złośliwym oprogramowaniem.

Zagrożenia związane z używaniem urządzeń mobilnych według respondentów obarczone są najniższym ryzykiem utraty informacji. Aż 19% respondentów w ogóle nie dostrzega ryzyka w zakresie włamań do urządzeń mobilnych, a aż 35% to ryzyko uważa za minimalne. Łącznie jest to ponad połowa ankietowanych. Należy jednak przy tego typu odpowiedziach uwzględnić fakt, że wiele podmiotów gospodarczych nie toleruje praktyki korzystania z tego typu rozwiązań przy zarządzaniu informacją przedsiębiorstwa, a praca zdalna poza obszarem organizacji nie występuje w praktyce w każdym z podmiotów.

W literaturze przedmiotu wciąż można spotkać duże rozbieżności w ocenie bezpieczeństwa chmury oblicze-

niowej. Zwolennicy nowego modelu IT, w tym oczywiście usługodawcy, starają się przekonać przedsiębiorców do bezpiecznego lokowania swoich informacji na serwerach zdalnych. Argumenty przemawiające za bezpieczeństwem informacji w chmurze obliczeniowej są wysoce logiczne. Największe firmy IT, inwestując bowiem w infrastrukturę cloud computingu, muszą przekonać potencjalnych użytkowników o jej bezpieczeństwie. Czynnikiem bezpieczeństwa informacji jest najbardziej istotny w przypadku decyzji o przenoszeniu zasobów na serwery zdalne. Usługodawcy inwestują więc w najnowocześniejsze zabezpieczenia w zakresie ochrony informacji: zabezpieczenia, których przeciętne przedsiębiorstwo nie implementuje w swoich działach IT. Można więc zaryzykować stwierdzenie, że cloud computing powinien być bezpieczniejszy od lokalnego serwera stacjonarnego. Dodatkowo, na usługodawcach CC ciąży presja, że jakakolwiek nagłośniona utrata informacji przez ich klienta może decydować o ich „być albo nie być” na rynku gospodarczym.

Chmura obliczeniowa, jako model stosunkowo nowy, budzi jednak wśród przedsiębiorców pewne obawy. Podmiotom przyzwyczajonym do lokalnego przechowywania informacji według dotychczasowego tradycyjnego

Rys. 5. Poziom zaniepokojenia bezpieczeństwem chmury obliczeniowej zdaniem specjalistów ds. bezpieczeństwa cybernetycznego

Źródło: opracowanie własne na podstawie: Crowd Research Partners, Cybersecurity Insiders, 2018, s. 6

Rys. 6. Jakie jest ryzyko naruszenia bezpieczeństwa informacji w środowisku chmury obliczeniowej w porównaniu z tradycyjnym modelem IT?

Źródło: opracowanie własne na podstawie: Crowd Research Partners, Cybersecurity Insiders, 2018, s. 11

Rys. 7. Czy aplikacje udostępniane w chmurze obliczeniowej są mniej czy bardziej bezpieczne od ich stacjonarnych odpowiedników?

Źródło: opracowanie własne na podstawie: Crowd Research Partners, Cybersecurity Insiders, 2018, s. 12

modelu IT, trudno uwierzyć w bezpieczeństwo informacji w przypadku, kiedy nie wiadzą, gdzie fizycznie informacja ta się znajduje. Obawy potwierdzają również specjaliści ds. bezpieczeństwa cybernetycznego. Organizacje Cybersecurity Insiders oraz Crowd Research Partners (2018) przeprowadziły badanie, w którym specjalistów zapytano o zdanie na temat bezpieczeństwa związanego z wdrażaniem chmury obliczeniowej w przedsiębiorstwach. Pytanie sformułowano w taki sposób, aby respondenci określili swój poziom zaniepokojenia związany z samym bezpieczeństwem cloud computing. Wyniki przedstawia rysunek 5.

Jak widać aż 91% specjalistów, w mniejszym lub większym stopniu, jest zaniepokojonych bezpieczeństwem modelu cloud computing.

Niewiele bardziej optymistyczne są same organizacje gospodarcze. Przeprowadzone badania wskazują, że przedsiębiorstwa uważają, że chmury publiczne są bardziej narażone na naruszenia bezpieczeństwa niż tradycyjne, lokalne środowiska IT (49%). Respondenci, którzy uważają, że chmury publiczne są mniej ryzykowne w przypadku naruszeń bezpieczeństwa, stanowią jedynie 17% grupę badanych, co pokazano na rysunku 6 (Crowd Research Partners, Cybersecurity Insiders, 2018, s. 11).

Bardziej optymistycznie wyrażają się ci sami respondenci w przypadku aplikacji uruchamianych w modelu SaaS (Software as a Service). Tylko 25% z nich (rys. 7) uważa, że aplikacje te oferują niższy poziom bezpieczeństwa w stosunku do ich tradycyjnych odpowiedników. Zaś aż 57% uważa aplikacje w modelu SaaS tak samo lub bardziej bezpieczne.

W przypadku wyboru modelu aplikacji komputerowych przez użytkowników problem jest nieco większy i może się pogłębiać. Niektórzy producenci oprogramowania rezygnują bowiem ze sprzedaży tradycyjnych „pułkowskich” wersji swoich produktów, oferując klientom jedynie model abonamentowy (np. firma Adobe). Tym samym wybór sposobu korzystania z aplikacji na rynku oprogramowania będzie stawał się coraz bardziej trudny dla przeciwników cloud computing.

Podsumowanie

Tworzenie zespołów wirtualnych pozwoliło przedsiębiorstwom na realizację zadań, które w tradycyjnych zespołach roboczych były trudne lub niemożliwe do wykonania. Współczesne rozwiązania informatyczne umożliwiły bowiem rekrutację pracowników bez uwzględniania lokalizacji, a z uwzględnieniem ich wiedzy i kompetencji. Procesy te wymagają jednak zaakceptowania i zminimalizowania pewnych zagrożeń wynikających zarówno z aspektów ludzkich, kulturowych, jak i technicznych.

Przytoczone w niniejszym artykule badania dotyczące bezpieczeństwa obszarów, w których funkcjonują zespoły wirtualne, stanowią ogólny zarys potencjalnego ryzyka zarządzania informacją. Każdy z opisywanych elementów infrastruktury IT wymaga w aspekcie bezpieczeństwa informacji dogłębnych badań uwzględniających zarówno

aspekty techniczne, jak i tzw. czynnik ludzki. Nowe techniki i technologie, ułatwiając z jednej strony procesy komunikacyjne, oferując rozwiązania pozwalające na przetwarzanie, magazynowanie informacji na odległość, utrudniają z drugiej strony nadzór nad prawidłowym dysponowaniem zasobów informacyjnych. Praca zdalna wymaga od pracownika szczególnej ostrożności w aspekcie zarządzania informacją, wymuszając na przedsiębiorcach szczególne podejście w procesie rekrutacji i tworzenia zespołów wirtualnych.

Analizując obecnie funkcjonujące modele IT (tradycyjny, cloud computing) oraz obserwując ich rozwój na przestrzeni ostatnich kilku lat, można zaryzykować stwierdzenie, że model chmury obliczeniowej w obszarze pracy zdalnej jest bardziej efektywny i najlepiej rokujący na przyszłość. Dynamiczny rozwój centrów obliczeniowych oraz oprogramowania w modelu SaaS pozwala na stosunkowo łatwe zarządzanie informacją na odległość. Dla podmiotów gospodarczych jest to również możliwość oddelegowania określonych aspektów zarządzania bezpieczeństwem informacji do przedsiębiorstw świadczących usługi cloud computingu, szczególnie biorąc pod uwagę wysoce dynamiczne zmiany technik i technologii zarówno od strony przetwarzania informacji, jak i od strony jej zabezpieczania. Kontrowersje budzi oczywiście sam fakt umieszczania zasobów informacyjnych na obcych serwerach. Wydaje się jednak, że trend ten będzie podlegał pewnej normalizacji.

dr inż. Paweł Kobis
Politechnika Częstochowska
Wydział Zarządzania
ORCID: 0000-0003-0714-1888
e-mail: pawel.kobis@wz.pcz.pl

Bibliografia

- [1] Crowd Research Partners, Cybersecurity Insiders (2018), *Cloud Security Report*, <https://pages.cloudpassage.com/rs/857-FXQ-213/images/2018-Cloud-Security-Report%20%281%29.pdf>, access date: 17.05.2019.
- [2] DuFrene D., Lehman C.M. (2012), *Communication Strategies for Virtual Teams*, Business Expert Press, New York.
- [3] Gallup (2017), *State of the American Workplace*, <https://news.gallup.com/reports/199961/7.aspx>, access date: 13.05.2019.
- [4] Hunsaker P.L., Hunsaker J.S. (2008), *Virtual Teams: A Leader's Guide*, „Team Performance Management: An International Journal”, No. 14, pp. 86–101.
- [5] Jędrzejczyk W., Kucęba R. (2010), *Postrzeganie informacji i wiedzy w organizacjach gospodarczych*, [w:] L. Kiełtyka (red.), *Rozwój i doskonalenie funkcjonowania przedsiębiorstw*, Difin, Warszawa, s. 285–301.
- [6] Kiełtyka L. (2017), *Narzędzia i technologie multimedialne wspomagające pracę menedżerów we współczesnych organizacjach*, „Przegląd Organizacji”, Nr 8, s. 33–42.
- [7] Kobis P., Chmielarz G. (2017), *The Barriers and Benefits of Implementing Cloud Computing in Economic Organizations*, „Informatyka Ekonomiczna”, Nr 3, s. 66–79.

- [8] Kobis P., Kisiółek A. (2018), *Zarządzanie bezpieczeństwem danych w przedsiębiorstwach MSP z uwzględnieniem czynnika ludzkiego – wyniki badań*, „Przegląd Organizacji”, Nr 8, s. 44–52.
- [9] Kopertyńska M.W., Kmiotek K. (2018), *Czynniki motywujące członków zespołów kreatywnych w sektorze IT – wyniki badań pilotażowych*, „Przegląd Organizacji”, Nr 3, s. 51–57.
- [10] KPMG (2019), *Barometr cyberbezpieczeństwa. W obronie przed cyberatakami*, <https://assets.kpmg/content/dam/kpmg/pl/pdf/2019/04/pl-Raport-KPMG-Barometr-Cyberbezpieczenstwa-W-obronie-przed-cyberatakami.pdf>, data dostępu: 18.05.2019 r.
- [11] Krawczyk-Bryłka B. (2016), *Budowanie zespołu wirtualnego – zasady i wyzwania*, „Studia Informatica Pomerania”, Nr 2, s. 99–111.
- [12] Oleksyn T. (2006), *Zarządzanie kompetencjami. Teoria i praktyka*, Oficyna Ekonomiczna, Kraków.
- [13] Olszak C.M. (2018), *Tworzenie wartości biznesowej w oparciu o zasoby Big Data*, „Przegląd Organizacji”, Nr 7, s. 35–45.
- [14] Pyszka A. (2015), *Modele i determinanty efektywności zespołu*, „Studia Ekonomiczne”, Tom 230, s. 36–54.
- [15] Sikorski C. (2005), *Język konfliktu: kultura komunikacji społecznej w organizacji*, C.H. Beck, Warszawa.
- [16] Statista (2018), *Share of Internet Users Worldwide Who Have Used a VPN in the Past Month as of 1st Quarter 2018, by Region*, <https://www.statista.com/statistics/306955/vpn-proxy-server-use-worldwide-by-region/>, access date: 14.05.2019.
- [17] Statista (2019), *Most Popular Global Mobile Messenger Apps as of April 2019, Based on Number of Monthly Active Users (in Millions)*, <https://www.statista.com/statistics/258749/most-popular-global-mobile-messenger-apps/>, access date: 10.05.2019.
- [18] Stefaniuk T. (2010), *Specyfika zespołów wirtualnych*, Zeszyty Naukowe Akademii Podlaskiej. Administracja i Zarządzanie, Nr 84, s. 153–165.
- [19] Stefaniuk T. (2014), *Komunikacja w zespole wirtualnym*, Difin, Warszawa.
- [20] Sukiennik M., Brzychczy E., Napieraj A. (2017), *Analiza pracy zespołów w organizacji z wykorzystaniem technik eksploracji procesów*, „Przegląd Organizacji”, Nr 11, s. 46–52.

Human in Virtual Teams and Information Security Management

Summary

Development of the IT market to a large extent is shaping the manner in which contemporary economic organisations are functioning. Information stored, processed digitally, provides a possibility to create new forms of operating structures of economic entities. One of such forms are work/research teams, which ever frequently operate within the structure of so-called virtual teams. They pose a great chance for enterprise development, simultaneously generating for them new organisational challenges. The objective of the present paper is to present the concept of virtual teams, whose functioning is fully dependent on possible thanks to the development of ICT technologies, which in the aspect of information security consider the human factor. The author has presented IT models functioning in contemporary enterprises, which support teamwork. Functional elements have been presented as well, which enable to organise so-called virtual meetings and discussed the most vital issues regarding their security. Additionally, the author has presented current research related to the discussed security areas that was conducted by renowned credit information agencies in the world.

Keywords

virtual teams, security, information, human factor