Zeszyty Naukowe UNIWERSYTETU PRZYRODNICZO-HUMANISTYCZNEGO w SIEDLCACH
Seria: Administracja i Zarządzanie
Nr 110 2016

dr inż. Tomasz Stefaniuk[1]
Uniwersytet Przyrodniczo-Humanistyczny w Siedlcach

Zagrożenia dla bezpieczeństwa informacji w zespołach wirtualnych

Threats to the security of information in virtual teams

Streszczenie: Zespoły wirtualne są coraz częściej zauważanym elementem współczesnych organizacji, który stale zyskuje na znaczeniu. Jednak poza wieloma zaletami tej formy organizacji pracy niosą one ze sobą nowe wyzwania, takie jak problemy z bezpieczeństwem informacji i systemów teleinformatycznych. Artykuł przedstawia zagadnienia bezpieczeństwa informacji i systemów informatycznych w zespołach wirtualnych. Dokonano w nim charakterystyki zespołów wirtualnych, przedstawiając pokrótce ich istotę oraz cechy odróżniające je od pozostałych form pracy zespołowej, jak również zdefiniowano bezpieczeństwo informacji i systemów teleinformatycznych, wskazując na główne atrybuty bezpieczeństwa oraz jego wpływ na skuteczną pracę zespołów wirtualnych. Zaprezentowano w nim również największe zagrożenia dla bezpieczeństwa informacji w zespołach wirtualnych, takie jak: cloud computing, stosowanie mobilnych urządzeń czy zagrożenia ze strony członków zespołu wirtualnego.
Słowa kluczowe: zespół wirtualny, bezpieczeństwo informacji, system zarządzania bezpieczeństwem informacji

Abstract: Virtual teams are an increasingly observed element of modern organizations, which is steadily gaining in importance. However, apart from the many advantages of this form of work organization they bring new challenges, such as problems with information and ICT systems security. This article outlines the problem of information and ICT systems security in virtual teams. In this article virtual teams are characterized by briefly presenting their nature and characteristics that distinguish them from other forms of teamwork, as well as defined security of information and ICT systems, indicating the main attributes of security and its impact on virtual teams effective work. It also presents the greatest threats to information security in virtual teams such as cloud computing, the use of mobile devices, or threats connected with virtual team members.
Keywords: virtual team, information security, information security management system

Wstęp

Wraz ze zmianami zachodzącymi współcześnie w otoczeniu przedsiębiorstw zmienia się forma i uwarunkowania pracy zespołowej. Z jednej strony coraz większym problemem staje się dostęp do wysoko wykwalifikowanych specjalistów. Z drugiej strony zespół pracowników danego przedsiębiorstwa nie zawsze jest w stanie podołać zadaniom, jakie zostały już wyznaczone. Konieczna jest współpraca międzyorganizacyjna, tworzenie zespołów złożonych ze specjalistów wielu współpracujących ze sobą organizacji. Inną przesłankę zmian w formie pracy

[1] Adres do korespondencji: Uniwersytet Przyrodniczo-Humanistyczny w Siedlcach, Wydział Nauk Ekonomicznych i Prawnych, ul. Żytnia 17/19 08-110 Siedlce, e-mail: tomasz.stefaniuk@uph.edu.pl

zespołowej stanowi rozwój technologii teleinformatycznych, który umożliwił nowe, wirtualne formy komunikacji. Z tego powodu liczne organizacje decydują się na zmianę tradycyjnych form pracy zespołowej na zespoły wirtualne. W przeprowadzonym w 2010 roku badaniu na reprezentantach firm z 77 krajów aż 80% respondentów potwierdziło swój udział w wirtualnych grupach specjalistów. Z kolei 64% badanych uznało zespół, w którym aktualnie pracowali, za wirtualny[2].

Zespoły wirtualne stwarzają dla organizacji zupełnie nowe możliwości. Przede wszystkim pozwalają na łatwiejsze tworzenie zespołów złożonych ze specjalistów wielu współpracujących ze sobą organizacji, umożliwiają znaczne obniżenie kosztów zarówno po stronie organizacji tworzącej zespoły wirtualne, jak również po stronie członków tych zespołów, ponadto powodują wzrost wydajności pracowników.

Oczywiście nie posiadają one samych zalet. Istnieją również negatywne konsekwencje stosowania tej formy pracy. Specyfika zespołów wirtualnych powoduje, iż problemy, które wiążą się z istnieniem każdego zespołu, w nich właśnie objawiają się najsilniej. Do takich problemów zaliczyć można m.in. budowanie zaufania, współpracę, kontrolę efektów pracy, komunikację czy wreszcie bezpieczeństwo informacji i systemów teleinformatycznych.

Przedstawienie znaczenia bezpieczeństwa informacji dla skutecznej pracy zespołu wirtualnego oraz analiza zagrożeń bezpieczeństwa informacji i systemów teleinformatycznych w tych zespołach jest celem niniejszego artykułu.

Istota zespołów wirtualnych

Zespoły wirtualne, określane przez P. Grajewskiego jako zespoły najnowszej generacji[3], rozwijają się bardzo dynamicznie, stwarzając nowe możliwości działania w warunkach globalizacji i informatyzacji. Według J. Goodbody bardzo szybko stają się one niezbędnym elementem globalnej gospodarki[4]. J. Lipnack i J. Stamps dowodzą, że zespoły wirtualne są kolejnym logicznym krokiem w ewolucji struktur organizacyjnych. Nie można bowiem rozwiązywać problemów dwudziestego pierwszego wieku, takich jak globalizacja czy digitalizacja, stosując dziewiętnastowieczne metody organizatorskie[5].

Tak jak każdy rodzaj zespołów, zespoły wirtualne są grupą składającą się z dwu lub więcej wzajemnie oddziaływujących na siebie i współzależnych osób, które łączą się, aby osiągnąć określone cele. Przy wyróżnianiu zespołów wirtualnych spośród innych form zespołowego działania zwraca się w literaturze przedmiotu uwagę na dwa główne kryteria[6]:

- rozdzielenie członków zespołu,
- komunikowanie się członków zespołu głównie za pomocą narzędzi teleinformatycznych.

[2] *The Challenges of Working in Virtual Teams*, Virtual Team Survey Report – 2010, RW[3] CultureWizard, New York, 2010, s. 2.
[3] P. Grajewski, *Organizacja procesowa. Projektowanie i struktura*, PWE, Warszawa 2007, s. 90-91.
[4] J. Goodbody, *Critical success factors for global virtual teams*, [dostęp 09.08.2011], http://www.allbusiness.com/human-resources/workforce-management/1045913-1.html [2009.02.15].
[5] J. Lipnack, J. Stamps, *Virtual Teams: Reaching Across Space, Time, and Organizations with Technology*, John Wiley & Sons, New York, USA, 2000, s. 37.
[6] Ibidem, s. 38.

Pierwsze kryterium oznacza, że członkowie zespołów wirtualnych nie mają ze sobą fizycznego kontaktu. Mogą być oddzieleni przestrzenią (odległością geograficzną) – wówczas pracują w różnych miejscach. Innym czynnikiem oddzielającym członków zespołu wirtualnego może być czas. W takim przypadku członkowie zespołu pracują w różnych okresach czasu. Mogą to być różne dni tygodnia, różne pory dnia/doby (w szczególnym przypadku – wynikające z różnych stref czasu). Niektórzy autorzy wyróżniają także możliwość oddzielenia członków zespołu przez bariery organizacyjno-strukturalne[7]. Bariery te nabierają szczególnego znaczenia w sytuacji, gdy członkowie zespoły wirtualnego pochodzą z różnych organizacji.

Drugie kryterium wyróżniające zespoły wirtualne – komunikowanie się członków zespołu głównie za pomocą narzędzi teleinformatycznych – jest następstwem oddzielenia od siebie członków zespołu. Odseparowanie nie jest równoznaczne z brakiem komunikacji. Bezpośredni przekaz komunikatów pomiędzy członkami tych zespołów stał się niemożliwy lub został znacznie ograniczony. Zastąpiony został więc komunikacją elektroniczną. Dlatego wykorzystanie narzędzi teleinformatycznych do komunikacji członków zespołu stało się główną cechą zespołu wirtualnego[8].

Wprawdzie w każdej formie pracy zespołowej stosowanie narzędzi teleinformatycznych do komunikowania się jest powszechne. Jednak tym, co wyróżnia zespół wirtualny spośród innych zespołów nie jest stopień wykorzystania samej technologii do komunikowania się, lecz stopień, w jakim komunikacja i współpraca w tych zespołach jest zdeterminowana przez technologię. Zespół tradycyjny w każdej chwili może zrezygnować z narzędzi teleinformatycznych, podczas gdy zespół wirtualny jest zupełnie uzależniony od tych technologii[9].

Jak zauważa H. Kopetz, systemy służące do komunikacji stanowią krytyczny zasób wszystkich systemów rozproszonych, a więc także zespołu wirtualnego, ponieważ jakakolwiek strata w procesie komunikacji powoduje straty wszystkich globalnych usług systemu[10]. Dlatego skuteczność zespołu wirtualnego jest silnie skorelowana ze skutecznością jego systemu komunikacji. Według J.R. Schermehorna skuteczna komunikacja zachodzi wówczas, gdy znaczenie komunikatu nadanego przez nadawcę i zinterpretowanego przez odbiorcę są identyczne[11]. Główna funkcja systemu komunikacji polega na zapewnieniu współpracy pomiędzy członkami zespołu. Warunkiem jego skuteczności jest zapewnienie wymiany informacji, tworzenie i utrzymanie relacji pomiędzy członkami zespołu oraz uzgadnianie znaczeń (troska o wzajemne zrozumienie).

Systemy teleinformatyczne dzięki zapewnieniu członkom zespołu dostępu do niezbędnych informacji i wiedzy, umożliwieniu przesyłania efektów pracy, konsultacji czy dyskusji w ramach zespołu umożliwiają realizację zadań składających się na cel istnienia zespołu. I właśnie ta zależność zespołów wirtualnych od systemów teleinformatycznych sprawia, że tak istotne dla ich funkcjonowania są kwestie bezpieczeństwa informacji i systemów teleinformatycznych.

---

[7] Np. D.L. Duarte, N.T. Snyder: *Mastering Virtual Teams: Strategies, Tools, and Techniques That Succeed*, Jossey Bass, 2001, s. 4-5; J. Lipnack, J. Stamps, op. cit., s. 38.
[8] T. Stefaniuk, *Komunikacja w zespole wirtualnym*, Difin, Warszawa 2014, s. 22.
[9] D.L. Duarte, N.T. Snyder, op. cit., s. 4-5.
[10] H. Kopetz, *Real-time systems: design principles for distributed embedded applications*, Kluwer Academic Publisher, Massachussets 1998, s. 33.
[11] J.R. Schermehorn, *Zarządzanie. Kluczowe koncepcje*, PWE, Warszawa 2008, s. 305.

Bezpieczeństwo informacji i systemów teleinformatycznych oraz jego znaczenie dla skutecznej pracy zespołu wirtualnego

Bezpieczeństwo informacji jest interpretowane na wiele sposobów, przy czym powszechną praktyką jest tutaj utożsamianie go ze spełnianiem szeregu atrybutów. W potocznym znaczeniu informacje są bezpieczne, gdy osoby nieuprawnione nie mają do nich dostępu (atrybut poufności). Według R. Borowieckiego i M. Kwiecińskiego bezpieczeństwo informacji jest to obrona polegająca na uniemożliwieniu i utrudnieniu zdobywania danych o fizycznej naturze aktualnego i planowanego stanu rzeczy i zjawisk we własnej przestrzeni funkcjonowania oraz utrudnianiu wnoszenia entropii informacyjnej do komunikatów i destrukcji fizycznej do nośników danych (atrybut poufności i integralności)[12].

Z kolei M. Plecka i A. Rychły-Lipińska z bezpieczeństwem informacji utożsamiają zapewnienie tajności, spójności i niezawodności działań związanych z gromadzeniem, przetwarzaniem i udostępnianiem danych wyłącznie uprawnionym osobom, co wynika z zajmowanego przez nie stanowiska lub wykonywania powierzonych im zadań[13].

Najszerszą listę atrybutów bezpieczeństwa informacji prezentuje norma PN-ISO/IEC 27001:2007, według której bezpieczeństwo informacji to zachowanie poufności, integralności i dostępności informacji; dodatkowo mogą być brane pod uwagę inne właściwości, takie jak autentyczność, rozliczalność, niezaprzeczalność i niezawodność[14]. Interpretację powyższych atrybutów bezpieczeństwa informacji przedstawiono w tabeli 1.

Wielu autorów zawęża pojęcie bezpieczeństwa informacji do ochrony danych cyfrowych, jak czyni to P. Tyrała, pisząc, że bezpieczeństwo informacji to działania zmierzające do zabezpieczenia zasobów informacyjnych w pamięciach komputerów oraz w sieciach teleinformatycznych[15]. Jednak powszechniejsze jest stosowanie pojęcia bezpieczeństwa teleinformatycznego (Information Technology – IT security lub Information and Communication Technology – ICT security), które jest rozumiane jako zespół procesów zmierzających do zdefiniowania, osiągnięcia i utrzymywania założonego poziomu poufności, integralności, dostępności, rozliczalności, autentyczności i niezawodności, czyli atrybutów bezpieczeństwa w systemach teleinformatycznych[16].

Ze względu na coraz większe uzależnienie się od technologii teleinformatycznych oraz od szybkiego dostępu do informacji bezpieczeństwo informacji oraz systemów teleinformatycznych staje się w organizacjach istotnym elementem strategicznej analizy ryzyka. Przyczyną takiego stanu rzeczy są coraz większe straty ponoszone przez organizacje na skutek występowania incydentów bezpieczeństwa.

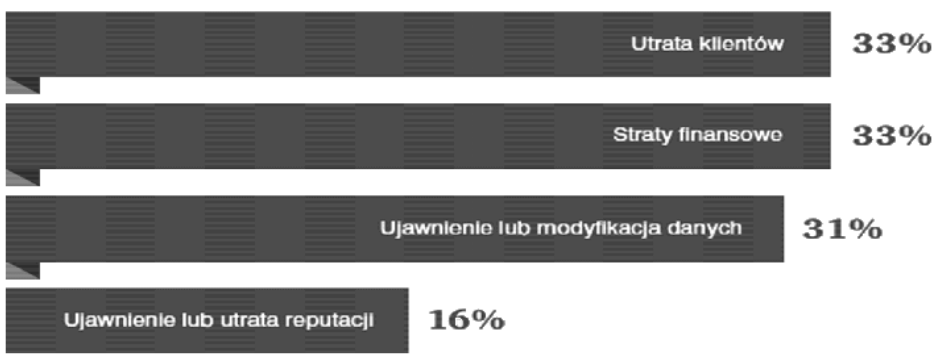
[12] R. Borowiecki, M. Kwieciński, *Monitorowanie otoczenia. Przepływ i bezpieczeństwo informacji. W stronę integralności przedsiębiorstwa*, Zakamycze 2003.
[13] M. Plecka, A. Rychły-Lipińska, *Bezpieczeństwo informacyjne*, [w:] *Wybrane problemy bezpieczeństwa. Dziedziny bezpieczeństwa,* A. Urbanek (red.), Wydawnictwo Społeczno-Prawne, Słupsk 2013, s. 165.
[14] PN-ISO/IEC 27001:2007, s. 12.
[15] P. Tyrała, *Zarządzanie kryzysowe. Ryzyko – bezpieczeństwo – obronność,* Wydawnictwo Adam Marszałek, Toruń 2001,s. 64.
[16] A. Białas, *Bezpieczeństwo informacji i usług w nowoczesnej instytucji i firmie*, WNT, Warszawa 2006, s. 33-34.

Tab. 1. Atrybuty bezpieczeństwa informacji

Nazwa	Znaczenie
poufność	właściwość, że informacja nie jest udostępniana lub wyjawiana nieupoważnionym osobom, podmiotom lub procesom
integralność	właściwość zapewnienia dokładności i kompletności aktywów
dostępność	właściwość bycia dostępnym i użytecznym na żądanie upoważnionego podmiotu
rozliczalność	właściwość systemu pozwalającą przypisać określone działanie w systemie do osoby fizycznej lub procesu oraz umiejscowić je w czasie
niezaprzeczalność	brak możliwości zanegowania swego uczestnictwa w całości lub w części wymiany danych przez jeden z podmiotów uczestniczących w tej wymianie
niezawodność	właściwość oznaczająca spójne, zamierzone zachowanie i skutki

Źródło: M. Ratajczyk-Mrozek, A.I. Adamik, M. Najda-Janoszka, P. Wróbel, T. Stefaniuk, R. Niedbał, *Koncepcje zarządzania zorientowane na współdziałanie i wspomagające je narzędzia informatyczne*, TNOiK, Dom Organizatora, Toruń 2016, s. 119.

Najczęstszym – bezpośrednim skutkiem potencjalnych incydentów bezpieczeństwa jest utrata lub kradzież danych. W Polsce niemal połowa wszystkich ataków kończy się wyciekiem lub niedostępnością pewnych informacji. Z raportu firmy MediaRecovery i kancelarii Ślęzak, Zapiór i Wspólnicy wynika, że aż dwie trzecie polskich firm poniosło szkodę finansową z powodu wycieku danych. Według PwC w 13% przypadków firmy z tytułu cyberprzestępczości straciły od 150 tys. zł do nawet 15 mln zł[17]. Najczęstsze skutki incydentów bezpieczeństwa w Polsce w roku 2015 zaprezentowano na rysunku 1.



Rys.1. Skutki incydentów bezpieczeństwa w Polsce

Źródło: *W obronie cyfrowych granic – czyli 5 rad, aby realnie wzmocnić ochronę firmy przed cyberryzykiem*, Raport PwC, 2016, s. 4.

[17] M. Duszczyk, *Polskie firmy na celowniku szpiegów*, „Rzeczpospolita" [dostęp 09.08.2015], http://www4.rp.pl/artykul/1149414-Polskie-firmy-na-celowniku-szpiegow.html.

Wszystkie przedstawione powyżej konsekwencje incydentów bezpieczeństwa dotyczą także zespołów wirtualnych. Jednak ze względu na swą zależność od technologii teleinformatycznych zespoły te są szczególnie wrażliwe na zakłócenia dostępności informacji oraz problemy związane z ich integralnością. Współpraca będąca podstawą każdej pracy zespołowej wymaga wzajemnych kontaktów członków zespołu – wymiany myśli, spostrzeżeń, ale przede wszystkim efektów ich pracy. Rozdzielenie członków zespołu wirtualnego sprawia, iż jakakolwiek forma porozumiewania się pomiędzy nimi jest możliwa tylko dzięki narzędziom teleinformatycznym. Dlatego wystąpienie incydentu bezpieczeństwa informacji powoduje w zespołach wirtualnych zakłócenia jego procedur i procesów, a w efekcie zmniejszenie skuteczności tego zespołu.

Podczas prowadzonych nad zespołami wirtualnymi badań dokonałem powiązania oceny poszczególnych elementów skuteczności pracy badanych zespołów wirtualnych z czynnikami skuteczności procesu komunikacji oraz wybranymi atrybutami bezpieczeństwa informacji. Korelację z największą ilością czynników skuteczności zespołu wirtualnego posiadają następujące elementy:

- dostęp do informacji wtedy, gdy jest ona niezbędna;
- poprawność zrozumienia wysłanych wiadomości;
- czas oczekiwania na odpowiedź kierownika/członków zespołu.

Czynniki te skorelowane są ze:

- średnią dokładnością i rzetelnością wykonania zakończonych zadań;
- jakością produktu finalnego;
- terminowością realizowanych zadań;
- sposobem planowania i zorganizowania pracy w zespole;
- sposobem definiowania i rozwiązywania problemów w zespole.

Konkludując, dostęp do informacji oraz ich integralność są istotnymi elementami warunkującymi skuteczną pracę zespołu wirtualnego, a każdy incydent naruszający powyższe atrybuty bezpieczeństwa informacji będzie prowadził do zmniejszenia skuteczności pracy zespołu wirtualnego.

Najważniejsze zagrożenia dla bezpieczeństwa informacji w zespole wirtualnym

Ostatnie lata obfitują w medialne doniesienia związane z udanymi włamaniami i kradzieżą tysięcy danych w takich firmach jak Sony, Oracle, Adobe, Microsoft czy Google. Kradzieże te przyjmują często formę skoordynowanych przez konkretne państwo działań, co ujawniły dane z raportu Mandianta[18] dotyczącego włamań przedstawicieli Chińskiej Republiki Ludowej do baz danych organizacji działających głównie w USA, Kanadzie i Wielkiej Brytanii.

W roku 2014 liczba cyberataków notowanych na świecie wzrosła o 48%, do ponad 117 tys. dziennie – wynika z raportu PwC pt. „Zarządzanie ryzykiem w cy-

[18] W lutym 2013 r. firma Mandiant, zajmująca się analizą ruchu internetowego i cyberbezpieczeństwem, w swoim raporcie opisała włamania przedstawicieli Chińskiej Republiki Ludowej do baz danych organizacji działających głównie w USA, Kanadzie i Wielkiej Brytanii i wykradzenie z nich setek terabajtów danych. W raporcie opisano systematyczne kradzieże danych z co najmniej 141 firm skupionych w branżach uważanych przez Chińczyków jako strategiczne: zbrojeniowej, energetycznej i medialnej Za: *Największe zagrożenia dla bezpieczeństwa w Internecie w roku 2013* – Raport, Fundacja Bezpieczna Cyberprzestrzeń, s. 6-7.

berprzestrzeni". W sumie uczestnicy światowego badania odnotowali ok. 42,8 mln naruszeń cyberbezpieczeństwa. W Polsce w tym samym okresie mamy do czynienia ze wzrostem cyberataków na poziomie 41%[19]. W roku 2015 w naszym kraju odsetek ten był jeszcze wyższy i wyniósł aż 46%[20].

Rośnie równocześnie skala oszustw internetowych. Jak wynika z danych Komendy Głównej Policji przekazanych „Rzeczpospolitej", w pierwszym półroczu roku 2015 było ich ponad 1,2 tys., czyli o niemal połowę więcej niż w tym samym okresie roku ubiegłego, kiedy doszło do 837 takich przestępstw. Należy przy tym zaznaczyć, że sieciowi oszuści doskonalą swoje metody i wykazują się niemałą inwencją[21].

Chociaż polskie firmy się do tego nie przyznają, to są szpiegowane nie tylko przez krajowych konkurentów, ale również przez Rosjan czy nawet Chińczyków, przy czym najbardziej na ataki narażone są spółki chemiczne, IT oraz energetyczne[22]. Gazeta „Rzeczpospolita", powołując się na firmę audytorską PwC, która przeprowadziła symulację ataków na kilkadziesiąt polskich firm, obnażyła fakt, iż spółki nie mają odpowiednich zabezpieczeń, a ochrona strategicznych danych praktycznie nie istnieje. W trakcie zorganizowanego symulowanego ataku na systemy bezpieczeństwa polskich firm w ciągu kilku godzin udało się wykraść informacje ze 100% kontrolowanych firm[23]. Ponadto zaledwie jedno na sto poddanych testom przedsiębiorstw zauważyło, że jest obiektem ataku.

Przedstawione powyżej dane o incydentach bezpieczeństwa informacji dotyczyły różnorodnych podmiotów bez względu na ich formę organizacyjną. Ale to wirtualne formy organizacji pracy są na te incydenty szczególnie narażone. Geograficzne rozdzielenie członów zespołu wirtualnego stwarza nowe wymagania co do dostępności informacji i wiedzy poza siedzibą organizacji, co z kolei rodzi zagrożenia dla jej bezpieczeństwa. Dane w organizacjach stosujących zespoły wirtualne są coraz częściej rozproszone i współdzielone pomiędzy wielu partnerów, dostawców, zleceniobiorców oraz klientów. Wymaga to ich przechowywania w chmurze (cloud computing). Według międzynarodowego badania, w którym wzięło udział 676 praktyków bezpieczeństwa informacji, to właśnie zwiększająca się ilość usług cloud computing została uznana za jedno z największych obecnie zagrożeń dla organizacji w dziedzinie bezpieczeństwa informacji, przy czym odsetek re-

[19] Zarządzanie ryzykiem w cyberprzestrzeni. Kluczowe obserwacje z wyników ankiety „Globalny stan bezpieczeństwa informacji 2015", s. 15, [dostęp 20.08.2015], http://www.pwc.pl/pl/publikacje/assets/gsiss_2015_polska.pdf.

[20] *W obronie cyfrowych granic – czyli 5 rad, aby realnie wzmocnić ochronę firmy przed cyberryzykiem*, Raport PwC, 2016, s. 4.

[21] Dla przykładu – hakerzy włamali się do systemu komputerowego Urzędu Miejskiego w Jaworznie i ukradli z konta niemal milion złotych w trakcie dokonywania przez urząd przelewu dla jednej z firm. Innym głośnym incydentem było włamanie się do serwerów Plus Banku i kradzież danych, m.in. o transakcjach i płatnościach kartami dużej liczby klientów. Haker miał zażądać od banku pieniędzy, a gdy ich nie otrzymał, opublikował w sieci skradzione poufne informacje, np. dane pół tysiąca klientów biznesowych, podając nazwiska właścicieli firm i numery kart płatniczych. Za: http://www.biztok.pl/biznes/polskie-firmy-wydaja-na-bezpieczenstwo-it-miliony-dolarow-rynek-nieustannie-rosnie_a22098.

[22] A. Braumberger, *Nowy wymiar wojny międzynarodowej. Polskie koncerny na celowniku mocarstw*, [dostęp 20.08.2015], http://www.biztok.pl.

[23] Rosja i Chiny okradają polskie spółki, 2014, [dostęp 27.08.2015], www.wmeritum.pl.

spondentów, którzy zidentyfikowali wykorzystanie zasobów cloud computing jako główny problem, wzrósł w przeciągu roku z 28 do 44 procent[24].

Znamienny jest fakt, że wśrod polskich badanych ponad połowa zadeklarowała, że ich firmy nie planują wprowadzenia oddzielnej strategii bezpieczeństwa dla chmury obliczeniowej, dla *Big Data* czy strategii poświęconej bezpieczeństwu informacji w kontekście funkcjonowania mediów społecznościowych.

Drugą konsekwencją rozdzielenia członków zespołu wirtualnego jest coraz większy stopień korzystania z urządzeń i systemów informatycznych, w tym oczywiście poza siedzibą organizacji. Nowinki technologiczne umożliwiają realizację różnorakich zadań biznesowych poza siedzibą firmy z niespotykaną dotychczas efektywnością. Równocześnie jednak zagrożenia związane z naruszeniem bezpieczeństwa informacji potrafią wstrzymać pracę całego zespołu. W zespole wirtualnym zdecydowanie łatwiej o materializację takowych zagrożeń, ponieważ wraz z przemieszczeniem się członków zespołu poza siedzibę firmy (zazwyczaj do domu) przemieszczają się także informacje i systemy informatyczne niezbędne do wykonywania pracy.

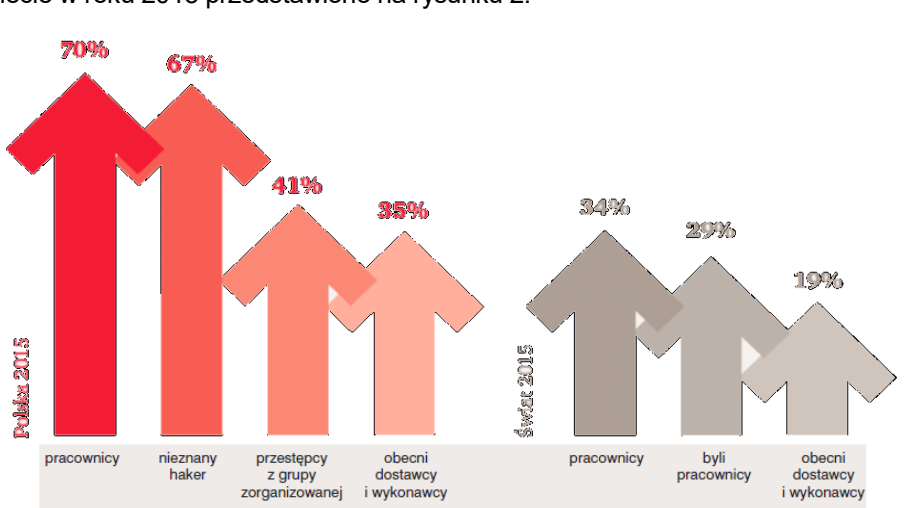
Znamienne jest to, że członkowie zespołów wirtualnych w swojej pracy stosują urządzenia mobilne. Wpisuje się to w ogólnoświatowy trend stałego wzrostu wykorzystania tych urządzeń (w roku 2014 na całym świecie sprzedano prawie miliard smartfonów tylko z systemem Android). Fakt powyższy z jednej strony rodzi zagrożenia uzależnień od Internetu, ale stwarza równocześnie wiele nowych zagrożeń związanych z bezpieczeństwem. Każde urządzenie, które jest wyposażone w jakiekolwiek oprogramowanie, jest potencjalnie narażone na ataki. Jeżeli dodatkowo posiada funkcję komunikacji, np. wysyłania/odbierania danych, to zawsze istnieje możliwość przejęcia nad nim zdalnej kontroli lub chociażby „podsłuchania" informacji, jakie przesyła. Jak łatwo się domyśleć, crackerzy chętnie wykorzystują fakt, że coraz więcej urządzeń łączy się z globalną siecią. Dla samego systemu Android zidentyfikowano już ponad 1,2 milionów mobilnych wirusów[25]. Pomimo że smartfony i tablety są wszechobecnym narzędziem pracy członków zespołów wirtualnych a informacje o zagrożeniach z nimi związanych są obecne w czołówkach serwisów informacyjnych, to organizacje nie spieszą się z wprowadzaniem zabezpieczeń mających przeciwdziałać zagrożeniom ze strony urządzeń przenośnych[26].

Warto również pamiętać o tym, że większość domów – podstawowych miejsc pracy członków zespołu wirtualnego – nie posiada gaśnic, wykrywaczy dymu czy planów ewakuacyjnych. Zdecydowanie gorsze są również zabezpieczenia antywłamaniowe w porównaniu z tymi stosowanymi w siedzibie firmy.

Poza tym nikt nie jest w stanie skontrolować, jakie osoby członek wirtualnego zespołu będzie zapraszać do domu, z kim będzie rozmawiać i komu będzie pokazywać poufne dane ze swojego komputera. Jak wynika z przeprowadzonych badań, około 50% wszystkich pracowników deklaruje, że z ich firmowego laptopa korzysta rodzina[27]. Być może dlatego już od wielu lat wszystkie badania poświę-

[24] *2014 State of Endpoint Risk Report*, Ponemon Institute LLC, Traverse City, 2014, s. 4.
[25] Kurs na funta, [dostęp 20.08.2015], http://kurs-na-funta.pl/security/wzrost-liczby-zagrozen-dla-systemu-android/?lang=pl.
[26] Jedynie nieco ponad połowa organizacji na świecie (54%) wdrożyło strategię bezpieczeństwa dla urządzeń przenośnych The Global State of Information Security® Survey 2015, s. 25.
[27] http://www.InfoWatch.com.

cone bezpieczeństwu informacji wskazują na człowieka jako głównego sprawcę incydentów zagrażających bezpieczeństwu informacji. Należy zauważyć, że aż 70% wszystkich nadużyć zostało w ubiegłym roku popełnionych przez pracowników organizacji[28]. Zestawienie źródeł incydentów bezpieczeństwa w Polsce i na świecie w roku 2015 przedstawiono na rysunku 2.



Rys. 2. Źródła incydentów bezpieczeństwa w Polsce i na świecie w roku 2015

Źródło: *W obronie cyfrowych granic – czyli 5 rad, aby realnie wzmocnić ochronę firmy przed cyberryzykiem*, Raport PwC, 2016, s. 10.

Zagrożenia wewnętrzne uznawane są za groźniejsze niż zewnętrzne, gdyż ich konsekwencje prowadzą do znacznie większych strat i komplikacji[29]. Część zdesperowanych i niezadowolonych pracowników próbowało celowo zdyskredytować lub wykorzystać firmy, w których aktualnie lub w przeszłości pracowali. Jednak w większości przypadków pracownicy są wykorzystywani jedynie jako środek do przenoszenia złośliwego oprogramowania czy jako obiekt ataku phishingowego i wykorzystującego socjotechnikę, stając się w ten sposób narzędziem w ręku rzeczywistych sprawców. Zdecydowanie łatwiej bowiem cyberprzestępcom wykorzystać naiwność człowieka niż złamać coraz to doskonalsze zabezpieczenia sprzętowo-programowe. Takich pracowników można podzielić na trzy kategorie: beztroskich i niedoświadczonych, wprowadzonych w błąd oraz padających ofiarą ataków typu inżynierii społecznej.

Bardzo często pracownicy wykonują lwią część pracy cyberprzestępców, stosując np. te same loginy i hasła w różnych serwisach, które nie są równie dobrze zabezpieczone. Wystarczy więc, że włamywacz wydobędzie informacje z bazy danych z tego teoretycznie nieistotnego portalu, aby chwilę później, wyko-

[28] The Global State of Information Security® Survey 2015, PwC, s. 16

[29] M. Jabłoński, M. Mielus, *Zagrożenia bezpieczeństwa informacji w organizacji gospodarczej* [w:] *Bezpieczeństwo informacji i biznesu. Zagadnienia wybrane*, M. Kwieciński (red.), Krakowskie Towarzystwo Edukacyjne, Kraków 2010, s. 31

rzystując zdobyte dane, zalogować się do naszej skrzynki pocztowej lub wykraść dane znajdujące się na przykład na firmowym dysku wirtualnym.

Jest to szczególnie istotne w zespołach wirtualnych, których członkowie nie mogą liczyć na szybkie wsparcie ze strony administratora czy serwisanta w miejscu swojej pracy. Rzadkością są również szkolenia dla członków zespołu wirtualnego dotyczące zagrożeń bezpieczeństwa informacji. Jest to szczególnie istotne, gdyż do większości naruszeń bezpieczeństwa informacji dochodzi w środowisku pracy oraz w związku z mediami społecznościowymi, na co wskazało aż 64% respondentów[30].

Zespoły wirtualne to często współpracujący nad projektem członkowie innych organizacji lub zewnętrzni partnerzy biznesowi, którzy poznali się dopiero w trakcie aktualnej współpracy. Wprawdzie w ramach prowadzonych przeze mnie badań okazało się, że prawie dwie trzecie (61,5%) ankietowanych deklarowało, że zna wszystkich pozostałych członków swojego zespołu, to 33,3% znało jedynie niektórych członków zespołu, natomiast 7,7% badanych nie znało nikogo spośród członków swojego zespołu. Jest to szczególnie istotne, gdyż jak wynika z badań PwC, wśród osób wchodzących w skład sieci powiązań firmy, na drugim miejscu pod względem generowania incydentów bezpieczeństwa w Polsce znaleźli się partnerzy biznesowi, wskazywani przez 22% respondentów, dostawcy usług i konsultanci – 17% oraz klienci, wskazani przez 9% badanych. Jest to zagrożenie bardzo często niezauważane przez organizacje, gdyż tylko 50% respondentów przeprowadza ocenę ryzyka swoich dostawców[31].

Podsumowanie

Oddzielenie od siebie członków zespołu wirtualnego sprawia, że jego praca jest uzależniona od wykorzystania systemów teleinformatycznych. Umożliwiają one dostęp do niezbędnych informacji i wiedzy, przesyłanie efektów pracy, konsultacje czy dyskusje w ramach zespołu. Jednym słowem zapewniają współpracę pomiędzy członkami zespołu i pozwalają na realizację zadań składających się na cel istnienia zespołu wirtualnego. W związku z powyższym wystąpienie incydentu bezpieczeństwa informacji powoduje w zespołach wirtualnych zakłócenia jego procedur i procesów, a w efekcie zmniejszenie skuteczności tego zespołu. Z drugiej strony, zespoły wirtualne są narażone na wiele zagrożeń. Dane w organizacjach stosujących zespoły wirtualne są coraz częściej rozproszone i współdzielone przez członków zespołów wirtualnych, którzy najczęściej w pracy korzystają z urządzeń mobilnych. Pozbawieni wsparcia ze strony administratora czy serwisanta w miejscu swojej pracy stają się często łatwą ofiarą dla hakerów.

W konsekwencji zasadne wydaje się wdrożenie w zespołach wirtualnych systemu zarządzania bezpieczeństwem informacji. W przypadku wielu zespołów wirtualnych tworzonych na krótki okres czasu zawiłe procedury i działania SZBI mogą wydawać się zbyt zbiurokratyzowane, czy wręcz zbędne. Jednak z perspektywy organizacji powołującej okresowo zespoły wirtualne złożone z członków tej organizacji, bądź z osób z zewnątrz, posiadanie systemu zarządzania bezpieczeństwem informacji wydaje się być koniecznością.

[30] *W obronie cyfrowych granic*…, s. 11.
[31] *Cyberbezpieczeństwo w Polsce i na świecie,* materiały ze spotkania prasowego PwC.

Bibliografia

2014 State of Endpoint Risk Report, Ponemon Institute LLC, Traverse City, 2014.

Białas A., *Bezpieczeństwo informacji i usług w nowoczesnej instytucji i firmie*, WNT, Warszawa 2006.

Borowiecki R., Kwieciński M., *Monitorowanie otoczenia. Przepływ i bezpieczeństwo informacji. W stronę integralności przedsiębiorstwa*, Zakamycze 2003.

Braumberger A., *Nowy wymiar wojny międzynarodowej. Polskie koncerny na celowniku mocarstw*, [dostęp 20.08.2015], http://www.biztok.pl.

Cyberbezpieczeństwo w Polsce i na świecie, materiały ze spotkania prasowego PwC.

Duarte D.L., Snyder N.T., *Mastering Virtual Teams: Strategies, Tools, and Techniques That Succeed*, Jossey Bass, 2001.

Duszczyk M., *Polskie firmy na celowniku szpiegów*, „Rzeczpospolita", [dostęp 09.08.2015], http://www4.rp.pl/artykul/1149414-Polskie-firmy-na-celowniku-szpiegow.html.

Goodbody J., *Critical success factors for global virtual teams.* [dostęp 09.08.2011], http://www.allbusiness.com/human-resources/workforce-management/1045913-1.html [2009.02.15].

Grajewski P., *Organizacja procesowa. Projektowanie i struktura*, PWE, Warszawa 2007.

http://www.biztok.pl/biznes/polskie-firmy-wydaja-na-bezpieczenstwo-it-miliony-dolarow-rynek-nieustannie-rosnie_a22098.

http://www.InfoWatch.com.

Jabłoński M., Mielus M., *Zagrożenia bezpieczeństwa informacji w organizacji gospodarczej*, [w:] *Bezpieczeństwo informacji i biznesu. Zagadnienia wybrane,* M. Kwieciński (red.), Krakowskie Towarzystwo Edukacyjne, Kraków 2010.

Kopetz H., *Real-time systems: design principles for distributed embedded applications*, Kluwer Academic Publisher, Massachussets 1998.

Kurs na funta, [dostęp 20.08.2015], http://kurs-na-funta.pl/security/wzrost-liczby-zagrozen-dla-systemu-android/?lang=pl.

Lipnack J., Stamps J., *Virtual Teams: Reaching Across Space, Time, and Organizations with Technology*, John Wiley & Sons, New York, USA, 2000.

Największe zagrożenia dla bezpieczeństwa Internecie w roku 2013 – Raport, Fundacja Bezpieczna Cyberprzestrzeń.

Plecka M., Rychły-Lipińska A., *Bezpieczeństwo informacyjne*, [w:] *Wybrane problemy bezpieczeństwa. Dziedziny bezpieczeństwa*, A. Urbanek (red.), Wydawnictwo Społeczno-Prawne, Słupsk 2013.

PN-ISO/IEC 27001:2007.

Ratajczyk-Mrozek M., Adamik A.I., Najda-Janoszka M., Wróbel P., Stefaniuk T., Niedbał R., *Koncepcje zarządzania zorientowane na współdziałanie i wspomagające je narzędzia informatyczne*, TNOiK, Dom Organizatora, Toruń 2016.

Rosja i Chiny okradają polskie spółki, 2014, [dostęp 27.08.2015], www.wmeritum.pl.

Schermehorn J.R., *Zarządzanie. Kluczowe koncepcje*, PWE, Warszawa 2008.

Stefaniuk T., *Komunikacja w zespole wirtualnym*, Difin, Warszawa 2014.

The Challenges of Working in Virtual Teams, Virtual Team Survey Report – 2010, RW3 CultureWizard, New York, 2010.
The Global State of Information Security® Survey 2015, PwC.
Tyrała P., *Zarządzanie kryzysowe, Ryzyko – bezpieczeństwo – obronność,* Toruń 2001.
W obronie cyfrowych granic – czyli 5 rad, aby realnie wzmocnić ochronę firmy przed cyberryzykiem, Raport PwC, 2016.
Zarządzanie ryzykiem w cyberprzestrzeni. Kluczowe obserwacje z wyników ankiety „Globalny stan bezpieczeństwa informacji 2015", [dostęp 20.08.2015], http://www.pwc.pl/pl/publikacje/assets/gsiss_2015_polska.pdf.