

Marcin Gogolewski, Michał Ren

Wpływ standaryzacji i wzrostu bezpieczeństwa telekonferencji na efektywność komunikacji biznesowej

Ekonomiczne Problemy Usług nr 104, 319-327

2013

Artykuł został opracowany do udostępnienia w internecie przez Muzeum Historii Polski w ramach prac podejmowanych na rzecz zapewnienia otwartego, powszechnego i trwałego dostępu do polskiego dorobku naukowego i kulturalnego. Artykuł jest umieszczony w kolekcji cyfrowej bazhum.muzhp.pl, gromadzącej zawartość polskich czasopism humanistycznych i społecznych.

Tekst jest udostępniony do wykorzystania w ramach dozwolonego użytku.

MARCIN GOGOLEWSKI, MICHAŁ REN

Uniwersytet im. Adama Mickiewicza w Poznaniu

WPŁYW STANDARYZACJI I WZROSTU BEZPIECZEŃSTWA TELEKONFERENCJI NA EFEKTYWNOŚĆ KOMUNIKACJI BIZNESOWEJ

Wprowadzenie

Dynamiczny rozwój przemysłowy współczesnego świata wymusza konieczność ciągłego przemieszczania się, a co za tym idzie, koszty różnego rodzaju dojazdów stanowią istotną część wydatków praktycznie każdej działalności (pośrednio lub bezpośrednio): pozyskiwanie klientów, kontakty z innymi firmami, udział w szkoleniach i konferencjach, czy choćby dojazdy do odległych oddziałów własnej firmy. Łatwo można się zgodzić z tezą, że części tego typu kosztów nie da się uniknąć (np. dojazd serwisanta w celu naprawy urządzenia), bądź wyjazd jest celem samym w sobie. Jednak nie zawsze przejazd do innej lokalizacji wynika z rzeczywistej konieczności obecności danej osoby, a jest spowodowany jedynie brakiem dostępności odpowiednich środków technicznych (choćby możliwość zdalnego nauczania, wykorzystywana w niektórych krajach od dawna, np. na szerszą skalę już w latach pięćdziesiątych ubiegłego wieku w Australii¹, pokazuje, że to możliwe.

Co ciekawe, problemem nie jest zwykle brak możliwości technicznych *per se*, a jedynie brak odpowiedniej wiedzy, czy wspólnego dla wszystkich zainteresowanych narzędzia komunikacji. Obecne technologie dają w tej materii wiele możliwości, choć problem nie został do końca rozwiązany i wiele da się jeszcze osiągnąć.

¹ <http://australia.gov.au/about-australia/australian-story/school-of-the-air>.

1. Możliwości redukcji kosztów dojazdów

Warto się zastanowić, jakie kwoty wydawane mogą być na wyjazdy służbowe (z punktu widzenia finansów pojedynczej firmy). Analiza nasza nie ogranicza się oczywiście do tego typu podróży i jest częściowo prawdziwa także nawet dla zwykłych dojazdów do pracy, jednak dla pewnego uproszczenia skoncentrujemy się tutaj na tak zwanych wyjazdach służbowych, ponieważ to właśnie one generują bezpośrednie wydatki (dojazd do pracy nie jest zwykle opłacany przez pracodawcę, a dojazdy do klienta czasami pokrywane są przez klienta). Obecnie wyjazdy krajowe to wydatek około 200 złotych na podróż i co najmniej podobna kwota za każdą dobę pobytu (hotel, diety, dojazdy). Bierzymy pod uwagę koszty „pracowników niższego i średniego szczebla”, gdyż w większości przypadków to właśnie one stanowią największy składnik kosztów. W przypadku podróży międzynarodowych koszty (średnio na terenie Europy, zakładając odpowiednio wczesne planowanie wyjazdu) to suma około 1500 złotych dojazd i co najmniej 500 złotych za każdą dobę pobytu (stosujemy tu kolejne uproszczenie: zakładamy, że podróże odbywają się pomiędzy stosunkowo dobrze skomunikowanymi lokalizacjami, co jest o tyle uzasadnione, że zwykle właśnie tam znajdują się siedziby większości firm i organizacji). Biorąc pod uwagę nawet tylko kilka takich wyjazdów w roku, koszt wydaje się spory.

Dla porównania do telekonferencji potrzeba sprzętu, oprogramowania i połączenia pomiędzy lokalizacjami. W przypadku „klasycznych” rozwiązań (dedykowane urządzenia, linie ISDN, pokoje do telekonferencji, komercyjne oprogramowanie) koszt pojedynczego „punktu” to, w zależności od wybranych rozwiązań, nawet kilkadziesiąt tysięcy złotych, ale nawet w tym przypadku od razu widać, że może być to dość atrakcyjna alternatywa w dłuższym okresie. Oczywiście zwykle technicznie możliwe jest wykorzystanie istniejącego sprzętu komputerowego (mało która firma czy organizacja nie posiada żadnego komputera), łączy internetowych (nawet gdy są to zwykle łącza szerokopasmowe o przeciętnych możliwościach) czy dostępnego za darmo oprogramowania. Choć rozwiązania takie mogą oferować istotnie niższy komfort użytkowania, to w praktyce będą często dostarczały podobnych możliwości, a jedynym kosztem będzie wstępna konfiguracja systemu i szkolenia pracowników. Niemniej jednak, w przeciwieństwie do wyjazdów, będzie to wydatek praktycznie jednorazowy (tj. nie uwzględniając konfiguracji nowych komputerów, aktualizacji oprogramowania czy szkolenia nowych pracowników, czyli normalnych kosztów działalności każdej organizacji).

2. Możliwe do uzyskania efekty

Głównym celem przeprowadzonej analizy jest ocena poziomu możliwych oszczędności finansowych, jednak warto się przez chwilę przyjrzeć rozwiązaniom,

które choć może nie najtańsze, są jednak obecne na rynku i mogą być stosowane głównie wtedy, gdy nie finanse, a na przykład czas (tracony na podróże) czy możliwość przebywania w wielu miejscach jednocześnie jest decydującym czynnikiem. W takim przypadku powinno zależeć na jak najlepszej „symulacji” obecności w danym miejscu, na swego rodzaju awatarze. Rozwiązania takie, jak choćby „robot” z projektu *Beam*, oferowane przez Suitable Technologies (<https://www.suitabletech.com/>) nie są może najtańsze (obecnie około 50 tys. złotych za „stanowisko”), a zastosowania ich ograniczone do ustalonych wcześniej lokalizacji, jednak jak widać z analizy kosztów podróży, mogą stanowić atrakcyjną alternatywę. Podobnie jak w przypadku zwykłych telekonferencji istnieją inne rozwiązania (np. tablety i tańszy sprzęt), które choć zdecydowanie skromniej wyposażone, oferują podobne funkcjonalności.

Warto zwrócić uwagę na fakt, że rozwiązania tego typu są już od jakiegoś czasu szeroko stosowane w wielu dziedzinach. Możliwe są np. operacje na odległość, zdalne sterowanie różnego rodzaju pojazdami lub, ostatnio coraz bardziej popularne, nauczanie na odległość².



Rys. 1. Beam Remote Presence Device (RPD)

Źródło: Suitable Technologies.

² M. Gogolewski, M. Ren: *Bezpieczne systemy zdalnego egzaminowania w e-learningu i gospodarce opartej na wiedzy.*

3. Problemy

Jak już zostało uzasadnione w poprzednich rozdziałach, istnieją możliwości zdecydowanego i racjonalnego ograniczenia niektórych kosztów, nie wspominając już o możliwej do zrealizowania w ten sposób strategii ochrony środowiska naturalnego. Dlaczego zatem wspomniane rozwiązania nie są powszechnie stosowane? Obecnie głównym problemem nie jest brak możliwości technicznych, ale brak ich standaryzacji. Wiele firm (np. Apple FaceTime, Microsoft NetMeeting, Skype) oferuje różne rozwiązania, jednak żadne z nich nie uzyskało decydującej przewagi, a co za tym idzie nie ma jednego wspólnego sposobu kontaktu pomiędzy wszystkimi zainteresowanymi. Jednak problemem nie jest tylko brak standaryzacji (krótko opisanej w następnym rozdziale), ale brak otwartości rozwiązań, który powoduje, że produkty, choć na poziomie standardu komunikacji nawet zgodne, nie współpracują i nie jest możliwe tworzenie połączeń pomiędzy nimi. Znaczenie szeroko rozumianej otwartości zostało przeanalizowane w artykule³. Innym problemem, podnoszonym przez niektórych potencjalnych użytkowników, jest bezpieczeństwo – głównie poufność prowadzonych rozmów. Jest to o tyle trudne do zrozumienia, że te same protokoły (RFC 3261), które służą do zabezpieczania komunikacji, wykorzystywane są przy połączeniach z bankami czy przesyłaniu innych wrażliwych danych, a w tych wypadkach większość użytkowników obdarza je pełnym zaufaniem.

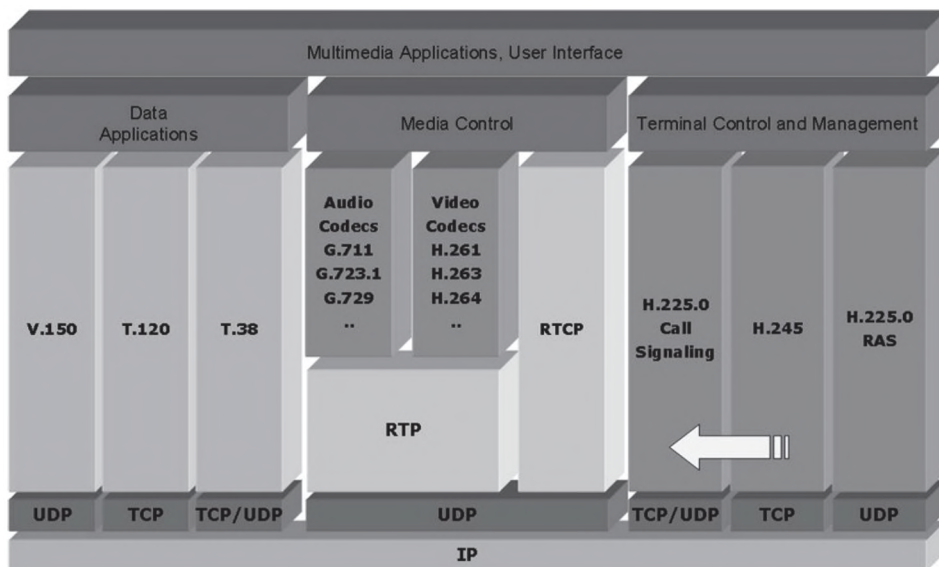
4. Protokoły

H.323

Jednym z pierwszych uniwersalnych standardów wykorzystywanych w telekonferencjach jest H.323. Został wprowadzony przez International Telecommunication Union w 1996 roku, jako sposób na przeprowadzanie telekonferencji w sieciach lokalnych. Ukazał się pod tytułem „Visual telephone systems and equipment for local area networks which provide a non-guaranteed quality of service”. Potrzeba realizowania telekonferencji poza sieciami lokalnymi była jednak tak duża, że H.323 szybko zaczęto stosować również do telekonferencji w sieciach rozległych. Już dwa lata później kolejna wersja standardu ukazała się jako „Packet-Based Multimedia Communications Systems” i pod tym tytułem funkcjonuje do dziś⁴.

³ M. Gogolewski, M. Ren: *Znaczenie wolnych i otwartych standardów dla bezpieczeństwa i rozwoju gospodarki elektronicznej*.

⁴ <http://www.itu.int/rec/T-REC-H.323/en/> H.323: Packet-based multimedia communications systems.



Rys. 2. Stos protokołu H.323

Źródło: M. Johnson: *Telecommunication Standardization Bureau*, ITU Standardization Sector.

Protokół H.323 jest w założeniu „parasolem”, pod którym funkcjonują inne protokoły będące rekomendacjami ITU, wraz z nim tworzące standard H.323. Najważniejsze z nich to:

1. H.225 „Call signalling protocols and media stream packetization for packet-based multimedia communication systems” – dotyczy wymagań technicznych w sytuacji, gdy transmisja przechodzi przez sieci pakietowe, bez gwarantowanej jakości przesyłania;
2. H.235 „Security and encryption for H-series (H.323 and other H.245-based) multimedia terminals” – cała rodzina rekomendacji, H.235.1-H.235.9, obejmująca bezpieczeństwo, prywatność i autentykację w multimedialnych strumieniach danych czasu rzeczywistego, przesyłanych w telekonferencjach;
3. H.245 „Control protocol for multimedia communication”, określa procedury i składnię komunikatów wymienianych przy negocjacji połączenia;
4. H.246 „Interworking of H-series multimedia terminals with H-series multimedia terminals and voice/voiceband terminals on GSTN and ISDN”, opisuje sposoby łączenia terminali używających różnych protokołów, jak również łączenia ich z globalną siecią telefoniczną;
5. H.281 „A far end camera control protocol for videoconferences using H.224”, jest protokołem używanym w wideokonferencjach do kontroli kamer;

6. H.341 „Multimedia management information base”, stanowi odpowiednik protokołu SNMP dla urządzeń i obiektów multimedialnych, umożliwiając uzyskanie informacji o nich i zachodzących zdarzeniach z nimi związanych;
7. H.450 „Generic functional protocol for the support of supplementary services in ITU-T H.323 systems”, to szereg rekomendacji (obecnie od H.450.1 do H.450.12) dotyczących usług takich jak przekierowanie połączenia, zawieszanie rozmowy, identyfikacja numeru, etc.;
8. H.460 „Guidelines for the use of the generic extensible framework” zawiera wskazówki, jak rozszerzać standard o moduły dodające funkcjonalność, tak by umożliwić negocjację wspieranych możliwości bez wprowadzania ich do standardu i wymuszania od wszystkich implementacji ich wspierania; obecnie obejmuje rekomendacje od H.460.1 do H.460.26.

Niewątpliwą zaletą protokołu H.323 i zapewne wiodącą przyczyną jego szerokiego rozpowszechnienia było wczesne opublikowanie szczegółowej dokumentacji standaryzacyjnej przez powszechnie uznaną, międzynarodową organizację standaryzacyjną ITU, działającą z ramienia Organizacji Narodów Zjednoczonych i zawiadującą m.in. ustalaniem standardów przewodowej globalnej sieci telefonicznej, jak i koordynacją przydzielania zakresów pasma radiowego. Dokumentacja była również od samego początku powszechnie dostępna na bezpłatnej licencji, a prace nad rozszerzeniami i uaktualnieniami standardu wciąż trwają, dzięki czemu pozostaje on aktualny.

SIP

SIP – Session Initiation Protocol jest protokołem zdefiniowanym przez IETF – Internet Engineering Task Force. Działa w najwyższej – siódmej – warstwie modelu ISO/OSI. Powstał w roku 1996. Jest protokołem tekstowym, podobnym do protokołów HTTP czy SMTP. Ostatnia jego wersja została opublikowana w 2002 roku jako RFC 3261.⁵

Wprawdzie celem SIP jest udostępnienie przez sieć funkcji telefonu (i więcej), to sam protokół ich nie definiuje. Podobnie jak H.323 podstawowy protokół skupia się na inicjalizacji sesji i sygnalizacji pomiędzy końcówkami. Reszta funkcjonalności jest realizowana poprzez rozszerzenia. IETF opublikowało ponad 180 dokumentów RFC związanych z protokołem SIP, z czego do najważniejszych należą:

1. RFC 3265 „Session Initiation Protocol (SIP) – Specific Event Notification” pozwala węzłom SIP prosić inne węzły o zawiadomienia o zdarzeniach ich dotyczących;
2. RFC 3261 „S/MIME Advanced Encryption Standard (AES) Requirement for the Session Initiation Protocol (SIP)” określa wymagania dotyczące algorytmów kryptograficznych, takich jak funkcje skrótu, podpis cyfrowy czy szyfro-

⁵ <http://tools.ietf.org/html/rfc3261> SIP: Session Initiation Protocol.

wanie (warto w tym miejscu wspomnieć, że SIP może wspierać również TLS – Transport Layer Security);

3. RFC 4916 „Connected Identity in the Session Initiation Protocol (SIP)” zapewnia możliwość poproszenia węzła SIP o podanie swojej tożsamości i ewentualne jej potwierdzenie przez serwis autentykacji;
4. RFC 5621 „Message Body Handling in the Session Initiation Protocol (SIP)” opisuje przetwarzanie wiadomości w protokole SIP, rozszerzając i uściślając RFC 3261;
5. RFC 5630 „The Use of the SIPS URI Scheme in the Session Initiation Protocol (SIP)”, wbrew nazwie, nie dotyczy głównie samego użycia URI (Uniform Resource Identifier), ale rozpatruje różne scenariusze, w których węzły SIP chcą się porozumieć w sposób bezpieczny, w różnych wariantach użycia TLS;
6. RFC 5922 „Domain Certificates in the Session Initiation Protocol (SIP)” określa sposoby użycia certyfikatów X.509 istniejącej infrastruktury klucza publicznego w bezpiecznym połączeniu SIP poprzez TLS do autentykacji domen SIP.

Protokół SIP, choć początkowo rozwijał się wolniej od H.323, obecnie bardziej zyskuje na znaczeniu. Coraz więcej infrastruktury obsługującej telekonferencje jest z nim zgodne, urządzenia go implementujące są powszechnie dostępne w sprzedaży i tanie, a programy obsługujące SIP są dostępne na większości platform. Wiele firm, również na rynku polskim, oferuje konta SIP z możliwością połączenia do sieci telefonicznej. Wiele komunikatorów internetowych, np. popularny Skype, oferuje możliwość połączenia SIP ze swoją siecią.

XMPP

Extensible Messaging and Presence Protocol pierwotnie nazywał się Jabber. Powstał w 1999 roku jako owoc prac społeczności open source Jabber. Później standard ten został skodyfikowany przez XMPP working group, założoną przez IETF (Internet Engineering Task Force) i opublikowany jako dokumenty RFC.⁶ Obecnie nad jego uaktualnianiem i rozszerzaniem sprawuje pieczę XMPP Standards Foundation.

W odróżnieniu od protokołów opisanych wyżej powstał w założeniu jako protokół komunikatora internetowego. Od samego początku obsługiwał więc funkcje właściwych takim protokołom, takich jak listy kontaktów czy śledzenie obecności. Początkowo nie zawierał wsparcia dla multimedialnych telekonferencji, jednak jest z założenia rozszerzalny, podobnie do protokołów opisanych wyżej. Jego podstawowe funkcje, opisane w najwcześniejszych wydanych dokumentach RFC, to zaledwie:

⁶ <http://tools.ietf.org/html/rfc6120> Extensible Messaging and Presence Protocol (XMPP): Core.

1. RFC 3920 „Extensible Messaging and Presence Protocol (XMPP): Core” opisujący podstawową strukturę protokołu;
2. RFC 3921 „Extensible Messaging and Presence Protocol (XMPP): Instant Messaging and Presence” dotyczący wymiany wiadomości tekstowych i statusów użytkowników;
3. RFC 3922 „Mapping the Extensible Messaging and Presence Protocol (XMPP) to Common Presence and Instant Messaging (CPIM)” pozwalający komunikatorom implementującym XMPP porozumiewanie się z komunikatorami implementującymi CPIM;
4. RFC 3923 „End-to-End Signing and Object Encryption for the Extensible Messaging and Presence Protocol (XMPP)” określający mechanizmy kryptograficzne zapewniające bezpieczeństwo i autentykację, takie jak szyfrowanie czy podpis cyfrowy.

Protokół XMPP rozwija się bardzo dynamicznie, czego dowodem jest choćby coraz częstsze wykorzystywanie go do tele- i wideokonferencji. Jednak oprogramowanie oparte o XMPP, obsługujące multimedialne konferencje, nie jest jeszcze tak rozpowszechnione jak oparte o SIP czy H.323, a rozwiązań sprzętowych w praktyce się nie spotyka.

Podsumowanie

W dobie kryzysu, z jakim boryka się spora część światowej gospodarki, telekonferencje stanowią bardzo atrakcyjną alternatywę dla tradycyjnych spotkań biznesowych, konsultacji medycznych i innych, które do tej pory wymagały osobistego kontaktu zainteresowanych stron. Jak widać, zastosowanie otwartych, bezpiecznych standardów daje możliwość realnych oszczędności zarówno finansowych, jak i czasowych, a do jego realizacji potrzeba tylko zmiany mentalności, rezygnacji ze „starych, wypróbowanych narzędzi” i otwarcia się na nowe, innowacyjne rozwiązania.

Literatura

1. Gogolewski M., Ren M., Nitschke Ł., Tyksiński T.: *Bezpieczne systemy zdalnego egzaminowania w e-learningu i gospodarce opartej na wiedzy*, Zeszyty Naukowe Uniwersytetu Szczecińskiego nr 651, Ekonomiczne Problemy Usług nr 68, 2011.
2. Gogolewski M., Ren M.: *Znaczenie wolnych i otwartych standardów dla bezpieczeństwa i rozwoju gospodarki elektronicznej*, Zeszyty Naukowe Uniwersytetu Szczecińskiego nr 702, Ekonomiczne Problemy Usług nr 87, 2012.

3. <http://www.itu.int/rec/T-REC-H.323/en/>, *H.323: Packet-based multimedia communications systems*.
4. <http://tools.ietf.org/html/rfc3261>, *SIP: Session Initiation Protocol*.
5. <http://tools.ietf.org/html/rfc6120>, *Extensible Messaging and Presence Protocol (XMPP): Core*.

**EFFECTS OF STANDARIZATION
AND INCREASING SECURITY OF TELECONFERENCES
ON EFFICIENCY OF BUSINESS COMMUNICATION**

Summary

The dynamic economic growth of today necessitates frequent travel, the cost of which forms a significant part of almost every business. While a part of those costs is unavoidable, some travel expenses are incurred only because of failure to employ suitable technical means, and can be drastically cut, as has been amply demonstrated by initiatives such as long-distance learning conducted on a big scale in Australia over half a century ago. Currently, the problem is usually not the lack of technical solutions, but lack of knowledge of how to employ them, or lack of common communication tool, standard for all stakeholders. Currently, technologies and standards exist that make this possible, however the problem has not been wholly solved.

Translated by Michal Ren