ZAGROŻENIA DLA BEZPIECZEŃSTWA WIEDZY W RAMACH ZARZĄDZANIA WIEDZĄ KLIENTA

https://doi.org/10.33141/po.2018.09.03

Przegląd Organizacji, Nr 9 (944), 2018, ss. 21-28
www.przegladorganizacji.pl

Bogusz Mikuła, Tomasz Stefaniuk

Wprowadzenie

Wiedza to główny strategiczny zasób dla każdego typu organizacji. W działalności gospodarczej jest on podstawą realizacji procesów biznesowych, decyduje o poziomie konkurencyjności, budując kluczowe i wyróżniające kompetencje przedsiębiorstwa, decyduje o przyjmowanych posunięciach w stosunku do przedsiębiorstw konkurencyjnych, partnerskich, jak też grup klientów. Szczególne znaczenie wiedzy wynika między innymi z faktu, że decyduje ona o stopniu i sposobach wykorzystania pozostałych zasobów będących w dyspozycji przedsiębiorstwa, zarówno rzeczowych (jak maszyny, urządzenia, surowce), jak i tych opartych na wiedzy (marki produktów, wizerunek, relacje z podmiotami otoczenia itp.). Dlatego też przedsiębiorstwa, które są świadome znaczenia wiedzy, dążą do maksymalnego wykorzystania posiadanych jej zasobów oraz dalszego ich rozwoju. Czynią to poprzez:

- racjonalizację swoich struktur organizacyjnych i wewnętrznych procesów w celu szerszego i lepszego wykorzystania zasobów wiedzy posiadanych w swojej dyspozycji,
- zakup lub tworzenie coraz bardziej wyrafinowanych rozwiązań technologicznych w zakresie przetwarzania informacji (wiedzy skodyfikowanej),
- maksymalizację procesów absorpcji wiedzy skodyfikowanej i doskonalenie metod jej zapisywania, przechowywania i przekazywania do potrzebujących jej pracowników,
- pozyskiwanie utalentowanych pracowników i pracowników wiedzy, którzy wnoszą do organizacji zdolności kreatywne i nowe zasoby wiedzy spersonalizowanej,
- rozbudowywanie relacji z otoczeniem pozwalających uzyskać dostęp do nowych zasobów wiedzy i pozyskiwać je lub też kreować wspólnie z innymi podmiotami, np. poprzez kooperację z partnerami zewnętrznymi,
- wprowadzanie nowych koncepcji i metod działania mających na celu pozyskanie wiedzy z otoczenia organizacji, czego przykładem jest zarządzanie wiedzą klienta (CKM – *customer knowledge management*).

Wszystkie te działania są czasochłonne, pracochłonne i kosztowne. Wartościową wiedzę jest trudno pozyskać i, jak się okazuje, łatwo stracić. Dlatego kluczową kwestią w obszarze zarządzania wiedzą jest zapewnienie jej bezpieczeństwa.

Bezpieczeństwo wiedzy znajduje się w obszarze zainteresowań dwóch dziedzin badań: zarządzania wiedzą i bezpieczeństwa informacji (Desouza, 2006 s. 4–6), przy czym ze względu na silne związki znaczeniowe wiedzy z informacją jest postrzegane jako naturalna ewolucja bezpieczeństwa informacji (Pereira, Santos, 2017, s. 236).

W związku z powyższym cel zapewnienie bezpieczeństwa wiedzy można definiować w oparciu o charakterystykę bezpieczeństwa informacji przyjętą w normie PN-ISO/IEC 27001:2014–12 jako zachowanie poufności, integralności i dostępności. Zgodnie z tym podejściem celem działań związanych z zapewnieniem bezpieczeństwa wiedzy jest jej utrzymanie w tajemnicy przed osobami nieuprawnionymi, które mogłyby z niej skorzystać (konkurenci, przestępcy itp.), a także zagwarantowanie dostępności i integralności tej wiedzy w organizacji. Z drugiej strony specyfika wiedzy – a w szczególności jej form występowania w organizacji – jako obiektu bezpieczeństwa wymaga odmiennego podejścia niż ma to miejsce w przypadku informacji.

I. Ilvonen (2013, s. 146), ze względu na fakt, iż to pracownicy – zarówno jako jednostki, jak i zbiorowo – posiadają i wykorzystują wiedzę, definiuje bezpieczeństwo wiedzy jako proces zabezpieczania wiedzy ludzi pracujących w organizacji. Należy zauważyć, że jest to podejście niepełne – nieuwzględniające między innymi wiedzy skodyfikowanej czy zautomatyzowanych procesów zarządzania wiedzą realizowanych bez udziału człowieka (np. w oparciu o sztuczną inteligencję).

Pełniejszą koncepcję przedstawił K.C. Desouza (2006, s. 4–5), stwierdzając, że zapewnienie bezpieczeństwa wiedzy musi nastąpić na trzech poziomach:

- produktu (obejmuje wiedzę w formie skodyfikowanej, przechowywaną np. w systemach informatycznych. W tym przypadku zapewnienie jej bezpieczeństwa jest tożsame z bezpieczeństwem informacji),
- ludzi (obejmuje człowieka jako twórcę i użytkownika wiedzy – zwłaszcza wiedzy utajonej. Ten poziom jest najmniej określony i stanowi przestrzeń badawczą w obszarze bezpieczeństwa wiedzy),
- procesu (obejmującego procesy zarządzania wiedzą: jej identyfikację, zachowanie, upowszechnienie i wykorzystanie).

Przyjmując perspektywę procesową, zapewnienie bezpieczeństwa wiedzy w organizacjach definiować można jako proces identyfikacji zagrożeń wewnętrznych i zewnętrznych dla bezpieczeństwa wiedzy oraz wyboru i zastosowania odpowiednich wariantów postępowania (stosownych zabezpieczeń) przeciwko tym zagrożeniom (Ilvonen i in., 2016, s. 4023).

Analizując koncepcję CKM, można postawić pytanie: czy jej wdrożenie nie pozostaje bez wpływu na zapewnienie bezpieczeństwa wiedzy w organizacji?

Stosowanie koncepcji CKM w organizacji pociąga za sobą zagrożenia dla bezpieczeństwa wiedzy, a celem niniejszego artykułu jest wskazanie tych zagrożeń oraz wyprowadzenie wniosków dotyczących kierunków działań podnoszących bezpieczeństwo zasobów wiedzy. Realizacja obranego celu wyznaczyła tok prowadzonych prac badawczych z wykorzystaniem metody analizy i krytycznej oceny literatury przedmiotu z zakresu CKM oraz zarządzania informacjami i wiedzą w obszarze bezpieczeństwa tych zasobów. W pierwszej kolejności scharakteryzowano służącą generowaniu wiedzy koncepcję CKM, skupiając główną uwagę na procesach przepływu wiedzy. Następnie dokonano identyfikacji i kategoryzacji zagrożeń dla bezpieczeństwa zasobów wiedzy, wynikających z realizacji poszczególnych procesów z udziałem wiedzy w ramach CKM (pozyskania wiedzy o kliencie, pozyskania wiedzy od klienta, kreowania wiedzy z klientem czy przekazania wiedzy klientowi), jak również ze stosowania w ramach CKM narzędzi teleinformatycznych. Przy zastosowaniu metody syntezy wyprowadzono zalecenia mające na celu zwiększenie poziomu bezpieczeństwa zasobów wiedzy wykorzystywanej i gromadzonej w ramach systemu zarządzania wiedzą klientów.

Istota zarządzania wiedzą klientów

Zarządzanie wiedzą klienta to pomysł na wykorzystanie zewnętrznego źródła wiedzy, jakim jest klient. Pomysł ten został mocno osadzony w koncepcji zarządzania relacjami z klientami (CRM – *customer relationship management*), ale CKM idzie dalej, starając się wykorzystać także potencjał twórczy klientów.

Przepływy wiedzy występujące w ramach CRM należą do trzech kategorii (Gebert i in. 2003, s. 109):

- wiedza dla klienta – jest niezbędna dla uzyskania przez klienta satysfakcji poprzez zaspokojenie jego potrzeb w zakresie posiadania wiedzy, przykładowo dotyczącej produktu, rynku i dostawców,
- wiedza o klientach – jest gromadzona w celu zrozumienia motywacji klientów i zastosowania personalizacji. Dotyczy ich historii, powiązań, wymagań, oczekiwań i decyzji zakupowych,
- wiedza od klienta – obejmuje wiedzę o produktach, dostawcach i rynku. Gromadzona jest poprzez interakcje z klientami dla podtrzymania procesu ciągłego doskonalenia, np. doskonalenia usług serwisowych lub rozwoju produktu.

Klient jednak zatrzymuje część swojej wiedzy dla własnych celów. Dodatkowo część z tej zatrzymanej wiedzy ma postać ukrytą (Rowley, 2006, s. 10) i nie może być w prosty sposób pozyskana od klienta. Taka wiedza okazać się może szczególnie cenna. Dlatego też CKM w porównaniu do klasycznego CRM koncentruje się na wiedzy będącej w posiadaniu klienta i jego potencjale do jej wykorzystania w procesie kreowania nowej wiedzy. Aktywizacja klienta polega na pobudzeniu go do ujawnienia i wykorzystania w procesie konwersji wiedzy wszystkich posiadanych zasobów wiedzy, łącznie z wiedzą przez niego zatrzymywaną dla własnych celów (Mikuła, 2016, s. 42). Tak więc przedmiotem zainteresowania CKM stają się następujące zasoby wiedzy:

- wiedza o kliencie,
- wiedza od klienta,
- wiedza dla klienta,
- wiedza wspólnie kreowana przez przedsiębiorstwo wraz z klientem.

Ze wskazanymi rodzajami wiedzy związane są cztery główne grupy procesów, na których koncentruje się CKM (rys. 1):

- pozyskiwanie wiedzy o kliencie,
- pozyskiwanie wiedzy od klienta,
- transfer wiedzy do klienta (udostępnianie wiedzy, rozpowszechnianie wiedzy lub/i dzielenie się wiedzą z klientem),
- wspólne z klientem kreowanie wiedzy.

CKM polega zatem na planowaniu, organizowaniu i kontroli przedsięwzięć w odniesieniu do wiedzy i potencjału innowacyjnego klienta mających na celu pozyskanie wiedzy o kliencie i wiedzy klienta oraz jej rozwój poprzez łączenie z wiedzą przedsiębiorstwa, a także dostarczanie wiedzy klientowi w celu zaspokojenia jego potrzeb i wspólne kreowanie z klientem nowej wiedzy dla udoskonalenia działalności przedsiębiorstwa i tworzenia innowacyjnych rozwiązań.

Dla usprawnienia procesów z udziałem wiedzy zastosowanie znajduje technika komputerowa, która z powodzeniem może wspomóc również realizację CKM. Wykorzystane mogą być te narzędzia, które znalazły zastosowanie w ramach CRM, a to (Porębska-Miąc, 2005, s. 356–357):

- narzędzia wspomagające komunikację, pracę grupową i wspólnoty praktyków – narzędzia realizujące koncepcję sieci pracowniczych, groupware i workflow oraz różne kanały komunikacji, takie jak: e-mail, fora dyskusyjne, czaty, zdalne konferencje itp.,
- narzędzia obsługujące zasoby informacyjne (pamięć organizacyjna) – są to wszelkie repozytoria, jak np.: foldery publiczne, DSM, CMS, bazy najlepszych praktyk, bazy przypadków,
- narzędzia sztucznej inteligencji, obejmujące algorytmy zaawansowanych technologii, tj. statystyczne, sztucznej inteligencji, data mining, których celem jest między innymi indeksowanie, wyszukiwanie, kategoryzowanie, strukturalizowanie, wnioskowanie, przewidywanie, kontekstualizacja, personalizacja, raportowanie itd. informacji zawartych w repozytoriach.

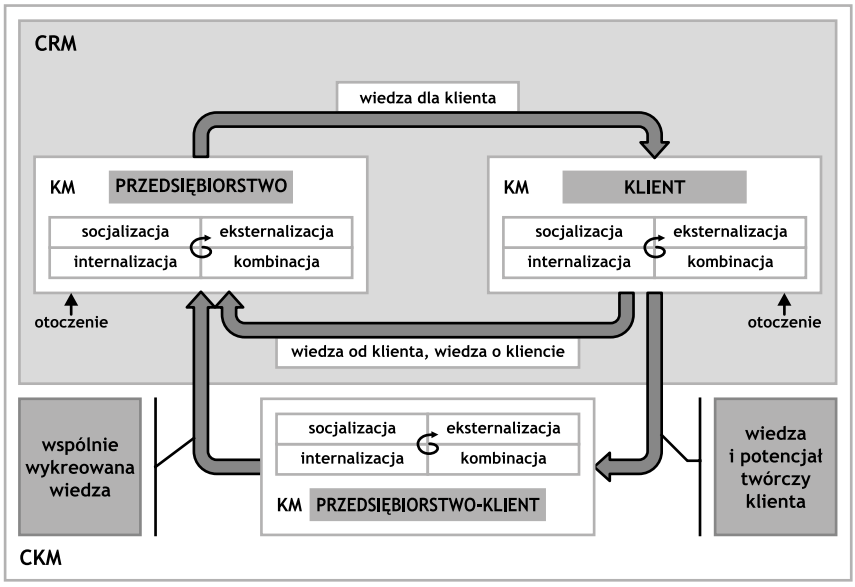
Zagrożenia dla bezpieczeństwa zasobów wiedzy w ramach CKM

Praca z zasobami wiedzy w ramach CKM i wykorzystanie techniki komputerowej w procesach objętych CKM niesie wiele zagrożeń dla przedsiębiorstwa i jego klientów, które związane są z nieuprawnionym pozyskaniem wiedzy przez któryś z podmiotów współdziałających lub stronę trzecią (rys. 2). Sytuacja ta jest tym bardziej skomplikowana, że CKM wymaga wejścia w środowisko sieciowe, a to nic innego – zgodnie z koncepcją „rury" J. Owen-Smitha i W.W. Powella (2004, s. 5–21) – jak „wyssanie" wiedzy z podmiotów uczestniczących poprzez relacje będące kanałami przepływu wiedzy. Ochrona wiedzy w środowisku sieciowym jest więc zadaniem niezwykle skomplikowanym.

Zagrożenia dla bezpieczeństwa zasobów wiedzy wynikają już z samego faktu realizacji poszczególnych procesów w ramach CKM: pozyskania wiedzy o kliencie, pozyskania wiedzy od klienta, kreowania wiedzy z klientem czy przekazania wiedzy klientowi. Fakt zaangażowania klienta we wspólne kreowanie wiedzy (poprzez włączenie go np. do zespołu tworzenia innowacji, wspólnoty twórczej) lub powierzenia mu roli prosumenta powoduje konieczność przekazania mu konkretnych zasobów wiedzy. Taka sytuacja tworzy możliwość rozpowszechnienia tych zasobów (np. w Internecie) lub ich udostepnienia (np. podmiotom konkurencyjnym) przez klienta.

Także stosowane w ramach CKM narzędzia teleinformatyczne niosą ze sobą większe lub mniejsze możliwości zaistnienia incydentów zagrażających bezpieczeństwu zasobów wiedzy (co zostanie przedstawione w dalszej części artykułu).

Jednym z podstawowych zasobów wiedzy w ramach CKM jest wiedza o klientach. Jej gromadzenie przez organizację (a szczególnie danych osobowych, haseł, numerów kart kredytowych czy danych teleadresowych) stwarza ryzyko kradzieży tych danych. Wycieki z baz danych zawierających takie informacje stanowią od wielu już lat jedno z największych zagrożeń związanych z bezpieczeństwem informacji (Fundacja Bezpieczna Cyberprzestrzeń, 2013, s. 12–13). Niektóre ataki na dane klientów organizacji w ciągu ostatnich kilku lat były wręcz spektakularne. Atak



Rys. 1. Przepływy wiedzy w zarządzaniu wiedzą (KM), relacjami z klientami (CRM) i wiedzą klientów (CKM)
Źródło: opracowanie własne z wykorzystaniem koncepcji SECI (Nonaka i Takeuchi, 2000, s. 86)

Rys. 2. Zagrożenia dla bezpieczeństwa wiedzy wynikające z realizacji CKM
Źródło: opracowanie własne

na Sony w roku 2013 skończył się wyciekiem danych o 70 milionach użytkowników. Z kolei w roku 2014 zaatakowano 90 proc. serwerów Banku JPMorgan. Szacuje się, że atakujący zdążyli wykraść dane ponad 76 milionów amerykańskich gospodarstw domowych, będących klientami JPMorgan Chase (Fundacja Bezpieczna Cyberprzestrzeń, 2013, s. 6–7).

Na przełomie roku 2014 i 2015 hakerzy wykradli także informacje z 500 milionów kont użytkowników Yahoo (polsatnews.pl, 2016). W roku 2015 hakerzy przejęli dane osobowe około 15 milionów klientów T-Mobile w USA, dane osobowe i bankowe ok. 4 milionów klientów TalkTalk w Wielkiej Brytanii czy Polsce dane dłużników Getin i Noble Banku (ok. 18 tys.), które później były wystawione w Internecie na sprzedaż (Fundacja Bezpieczna Cyberprzestrzeń, 2013, s. 12–13).

W roku 2016 obserwować mogliśmy spektakularny atak na tzw. „PanamaPapers" – włamanie do systemu informatycznego obsługującego panamską firmę prawniczą Mossack Fonseca, w wyniku którego hakerzy skradli prawie 12 milionów poufnych dokumentów, które powstały w latach 1970–2015[1].

Zazwyczaj celem ataków na dane klientów jest wymuszenie okupu bądź próba skompromitowania zaatakowanej organizacji. Przykładowo w roku 2015 haker-szantażysta, który włamał się do Plus Banku, żądał od niego 200 tys. zł za nieopublikowanie wykradzionych danych (Boczoń, 2015).

Należy zaznaczyć, że dane klientów nie są narażone tylko na ataki hakerskie z zewnątrz. Doskonałym przykładem pokazującym, co może osiągnąć zdeterminowany pracownik, był w roku 2014 wyciek wrażliwych danych prawie połowy obywateli Korei Południowej posiadających rachunki w banku Korea Credit Bureau. Mając dostęp do wewnętrznych systemów, jeden z pracowników najpierw wykradł dane klientów banku, a następnie sprzedał je firmie zajmującej się telemarketingiem (Kulik, 2014).

Kradzież danych klientów z organizacji i powiązane z nią ich upublicznienie powoduje utratę wiarygodności, stanowiącą podstawę zaufania klientów. Być może właśnie dlatego utrata klientów jest najczęstszym i najpoważniejszym skutkiem wystąpienia cyberataków (PWC, 2016, s. 8).

Bardzo powszechną i groźną z perspektywy zasobów wiedzy o klientach praktyką wśród pracowników zmieniających pracodawcę jest fakt „zabierania ze sobą" danych klientów do nowego pracodawcy. Często odchodzący pracownicy nie posuwają się do nielegalnego kopiowania bazy danych. Takie dane posiadają w prywatnym telefonie komórkowym czy wizytowniku, w którym przechowują wizytówki otrzymane od klientów (Solga, 2013).

Kolejne zagrożenia dla bezpieczeństwa wynikają ze specyfiki procesu kreowania w ramach koncepcji CKM wiedzy wspólnie z klientem. Realizacja tego procesu wymaga dostępu klienta do wiedzy organizacyjnej, jak również umożliwia dostęp klienta do nowo powstałej wiedzy.

Udostępnianie wiedzy może prowadzić do jej wycieku (Ritala i in., 2015, s. 24). Żadna organizacja nie jest w stanie zagwarantować dobrych intencji klienta czy jego lojalności w przyszłości. Zgodnie z powiedzeniem „okazja czyni złodzieja", klient, który uzyskał dostęp do bazy wiedzy organizacji, może tę wiedzę powielić i przekazać od razu, lub w przyszłości na zewnątrz, np. firmie konkurencyjnej.

Informacje na temat funkcjonowania konkurencyjnej organizacji są bardzo cenne. Są one kluczowym elementem systemu informacyjnego każdej organizacji, a jedną z form ich pozyskania są wywiady z klientami (Jacieczko, 2003, s. 440). Jak zauważa D. Dahl (2011), rozmowa z klientami to najlepszy i najtańszy sposób gromadzenia rzetelnych informacji o organizacji konkurencyjnej. Każda organizacja, udostępniając swoją wiedzę klientom, musi więc mieć świadomość tego, że są lub mogą być oni w przyszłości źródłem wiedzy dla konkurencji.

Zagrożenia dla bezpieczeństwa wiedzy wynikające ze stosowania technologii informatycznej wspomagającej CKM

Analizując zagrożenia dla bezpieczeństwa wiedzy wynikające z realizacji procesów CKM, należy wziąć pod uwagę także podatności przypisane poszczególnym technologiom teleinformatycznym stosowanym w tych procesach. Szczególnie wyróżnić należy: ekstranet, przetwarzanie w chmurze oraz social media.

Najbardziej naturalną technologią umożliwiającą klientom dostęp do zasobów wiedzy organizacji w ramach transferu wiedzy do klienta jest ekstranet. Jest to środowisko sieciowe skonfigurowane w taki sposób, że partnerzy zewnętrzni (klienci, dostawcy, konsultanci) mogą uzyskać dostęp do danych i/lub aplikacji wewnątrz firmowej sieci (Diks, 2001). Ekstranet jest to więc wydzielona część sieci lokalnej, otwarta na zewnątrz, która najczęściej zawiera stronę WWW danej firmy, serwer DNS bądź zapewnia dostęp do usług poczty e-mail dla klientów zewnętrznych, lub innych usługi udostępnianych firmom współpracującym czy też kontrahentom (Błoński, 2007, s. 23). Aplikacje oraz dane definiowane są w taki sposób, aby były niezależne od jakiejkolwiek platformy, co oznacza, że użytkownicy końcowi mają płynny dostęp do potrzebnych im informacji, nawet jeśli pracują w oddzielnych systemach innych organizacji (Kiełtyka, 2002, s. 371–372; Pańkowska, 2001, s. 394). Udostępnienie określonej ilości zasobów wiedzy na zewnątrz sprawia, że z perspektywy bezpieczeństwa dane te są obarczone dużym ryzykiem ich utraty (Trolan, 1998). Jednak, co gorsze, naraża w jakiś sposób część sieci firmy na przeróżne próby ataków, przeprowadzanych w celu zdobycia cennych danych czy też zakłócenia stabilności poszczególnych usług czy serwerów (Błoński, 2007, s. 23). Jeżeli zasoby ekstranetu, czyli serwery i usługi na nich udostępnione nie są w żaden sposób wydzielone – są po prostu częścią intranetu (wewnętrznej sieci organizacji). Nieuczciwy klient lub osoba działająca z konta klienta, mając dostęp do sieci ekstranet, łatwiej przedostanie się przez zabezpieczenia i uzyska dostęp do serwera niż osoba z zewnątrz. Przy niedostatecznym poziomie zabezpieczeń może udać mu się pozyskać informacje o strukturze sieci oraz o kontach użytkowników. Wówczas już nic nie będzie w stanie przeszkodzić mu w eksplorowaniu sieci oraz odczytywaniu informacji, do których nie powinien mieć dostępu (Błoński, 2007, s. 25).

Innym – obok ekstranetu – sposobem udostępniania wiedzy klientom jest technologia przetwarzania w chmurze (*Cloud Computing*), która stała się jednym z coraz częściej stosowanych rozwiązań w wielu obszarach biznesowych (PWC, 2016, s. 12). Najprościej ujmując, jest to świadczenie usług informatycznych za pośrednictwem infrastruktury sieciowej. Z perspektywy technologicznej jest to takie przetwarzanie, które poprzez dogodny dostęp sieciowy dostarcza współdzielony zestaw konfigurowalnych zasobów przetwarzania, np. dostarcza sieci, serwery – Infrastructure as a Service (IaaS), przestrzeń do składowania danych – Platform as a Service (PaaS), oprogramowanie i usługi – Software as a Service (SaaS). Zasoby te są dostarczane szybko (*on-demand*) z minimalnym wysiłkiem zarządzania i z minimalnym udziałem dostawcy (Grance, Mell, 2011; Cloud Standards Customer Council, 2017, s. 4). Całość tak rozproszonej, ale powiązanej ze sobą zaawansowanej technologicznie infrastruktury informatycznej nazywa się potocznie „chmurą". Chmurą jest więc cały zbiór serwerów, oprogramowania, światłowodów itd., do którego uzyskuje się dostęp za pośrednictwem Internetu (Łapiński, Wyżnikiewicz, 2011, s. 5). Organizacja korzystająca z takiej usługi swoje zasoby wiedzy przechowuje na zewnętrznych serwerach, do których częściowy dostęp przydziela również klientom.

Pomimo wielu zalet takiego rozwiązania, organizacja godzi się na przynajmniej częściową utratę kontroli nad zasobami wiedzy oraz sposobami jej zabezpieczenia. Przechowywanie wiedzy na zewnętrznych serwerach sprawia, że są one narażone na wyciek lub utratę oraz łatwiejsze staje się przejęcie konta albo aplikacji przez osoby nieuprawnione. Pojawiają się problemy z kompatybilnością wspólnie używanych narzędzi, serwery przeciążają się, zabezpieczenia interfejsów są niedostateczne (Hołyński, 2012, s. 119). Według międzynarodowego badania, w którym wzięło 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 respondentów, którzy zidentyfikowali wykorzystanie zasobów cloud computing jako główny problem, wzrósł w ciągu roku z 28 do 44% (2014 State of Endpoint Risk Report, s. 4).

Według Cloud Security Alliance (2016), największe zagrożenia dla danych w chmurze są następujące:

1. Naruszenie danych (kradzież, oglądane lub używane przez osobę do tego nieupoważnioną).
2. Niedostateczna identyfikacja tożsamości i zarządzanie dostępem.
3. Niebezpieczne interfejsy API.
4. Luki w systemie.
5. Przejęcie konta.
6. Ataki od wewnątrz (*malicious insiders*).
7. Zaawansowane długotrwałe ataki (APT).
8. Utrata danych.
9. Brak należytej staranności przy wyborze odpowiedniej technologii.
10. Nadużywanie oraz niefrasobliwe korzystanie z usług Cloud.

Wystąpienie incydentu dotyczącego wiedzy przechowywanej w chmurze skutkować może utratą reputacji, wyższymi kosztami i potencjalnie nawet likwidacją firmy (Cloud Standards Customer Council, 2017, s. 4).

Stosunkowo nowym kanałem umożliwiającym rozpowszechnianie wiedzy lub/i dzielenie się wiedzą z klientem są media społecznościowe. Coraz powszechniejsze korzystanie z takiego sposobu utrzymywania relacji niesie ze sobą nowe niebezpieczeństwa.

Pomimo że w ciągu ostatniego roku odnotowano 150% wzrost ataków hakerskich z wykorzystaniem phishingu w mediach społecznościowych, to zaledwie 29,6% respondentów uważa, że ryzyko związane z mediami społecznościowymi należy do grupy największych wyzwań w zakresie bezpieczeństwa informacji i wiedzy. Wskazuje to na brak zrozumienia znaczenia nowych rodzajów zagrożeń społecznościowych oraz sposobów skutecznego ograniczania i zarządzania nimi (McClure, Parkinson, 2017, s. 6).

Serwisy społecznościowe umożliwiają nielegalne zdobywanie różnych informacji: od danych osobowych i profili osób po wiadomości archiwalne, które mogłyby pomóc cyberprzestępcom w tworzeniu fałszywych e-maili lub witryn sieciowych (bardziej znanych jako stron phishingowych) w celu dalszego wyłudzenia poufnych informacji (Tomkiewicz, 2011). Pozwalają również na umieszczanie wirusów w przesyłanych wiadomościach. Nieświadomi zagrożenia pracownicy organizacji klikają w link otrzymany od klienta, gdy w rzeczywistości nadawcą jest haker, a link został zainfekowany. Celem takiego ataku jest zazwyczaj kradzież danych, w tym danych służących do uwierzytelniania. Kradzież hasła może mieć poważne konsekwencje, zwłaszcza w przypadku osób, które używają tego samego hasła do logowania się do różnych systemów w swojej organizacji („Gazeta prawna", 2014).

Przykładem takiego działania był atak phishingowy „fałszywy przyjaciel" skierowany do użytkowników Facebooka w roku 2016. Według Kaspersky Lab, tysiące użytkowników otrzymało wiadomość o tym, że zostali wymienieni przez znajomego w komentarzu. Po kliknięciu wiadomość instalowany był złośliwy program, który przejmował konto użytkownika Facebooka (Russel, 2017).

Kolejnym zagrożeniem związanym z mediami społecznościowymi jest ludzka skłonność do udostępniania zbyt wielu danych osobowych w Internecie, dotyczących nie tylko życia prywatnego, ale również miejsca pracy. Informacje te są następnie wykorzystywane np. do kradzieży tożsamości, a potem do ataku na daną korporację.

Należy zwrócić uwagę, że informacje publikowane na oficjalnym profilu organizacji mogą zostać wykorzystane przez klientów w ramach prowadzonej w przyszłości kampanii przeciwko tej organizacji. Wystarczy kilka sekund, by użytkownicy blogosfery czy serwisów społecznościowych zdecydowali się podjąć protest lub bojkot. Za pośrednictwem swoich miejsc w Internecie połączeni konsumenci zamieszczają szczegółowe informacje na temat firm i produktów oraz prowadzą różne akcje i kampanie (Szumniak-Samolej, 2010).

Podsumowanie

CKM to pomysł na wykorzystanie zewnętrznego źródła wiedzy, jakim jest klient, a w szczególności jego potencjału twórczego. Praca na zasobach wiedzy w ramach CKM i wykorzystanie techniki komputerowej w procesach objętych CKM niesie wiele zagrożeń dla przedsiębiorstwa i jego klientów, które związane są z nieuprawnionym pozyskaniem wiedzy przez któryś z podmiotów współdziałających lub stronę trzecią. Realizacja poszczególnych procesów w ramach CKM zwiększa ryzyko utraty zgromadzonej przez organizację wiedzy o klientach czy utraty wiedzy organizacyjnej na skutek nieuczciwych działań związanych z dzieleniem się wiedzą z klientami. Także ze względu na powszechność stosowania w ramach CKM narzędzi teleinformatycznych oraz korzystania ze środowiska sieciowego zwiększa się ilość zagrożeń dla wiedzy organizacyjnej. Spowodowane jest to rozpowszechnieniem stosowania między innymi chmury czy mediów społecznościowych oraz rokrocznie zwiększającą się ilością ataków na zgromadzone w nich zasoby wiedzy. Dlatego też:

- dobór technologii wspierających CKM nie może być przypadkowy i oparty jedynie o kryterium kosztów. Uwzględnione muszą zostać potencjalne zagrożenia dla zasobów wiedzy przedsiębiorstwa, relacji i jego reputacji;
- pracownicy współpracujący z klientami muszą być świadomi możliwości utraty przez przedsiębiorstwo wartościowej wiedzy (kluczowej i wyróżniającej), w normalnych warunkach chronionej;
- zasoby wiedzy mające zostać udostępnione klientom muszą być poddane analizie i ocenie z punktu widzenia ich wartości dla przedsiębiorstwa oraz skutków nieodwracalnej ich utraty lub niekontrolowanego ich rozpowszechnienia;
- analizowane muszą być zagrożenia będące skutkiem możliwego niekontrolowanego wypływu wiedzy wykorzystywanej podczas współpracy z klientami, a konsekwencją tej analizy powinna być decyzja, czy dany zasób wiedzy udostępnić klientom, czy go chronić (np. wiedzę o ukrytych wadach racjonalizowanego produktu);
- przepływy wiedzy do klientów powinny być sterowane, aby uniknąć przypadkowego przekazania wiedzy chronionej lub udostepnienia wiedzy podmiotom trzecim;
- przedsiębiorstwo na bieżąco gromadzić musi wiedzę o istniejących i nowych zagrożeniach wobec zasobów wiedzy, a następnie rozpowszechniać ją wśród pracowników. Realizowany musi być systematyczny proces szkolenia pracowników i racjonalizacji wykorzystywanych procedur oraz narzędzi ochrony;
- zaangażowani do współpracy klienci muszą być informowani o możliwych zagrożeniach utraty wiedzy w zależności od wykorzystywanych metod i technologii;
- współpracujący z przedsiębiorstwem klienci muszą być poinformowani o potencjalnych skutkach prawnych i finansowych w przypadku przekazania udostępnionej wiedzy podmiotom trzecim;
- tworzony system CKM musi uwzględniać i przestrzegać istniejące regulacje prawne.

Wszystkie wskazane działania są pracochłonne, czasochłonne i kosztowne, ale niezbędne dla poprawnego funkcjonowania systemu CKM oraz ochrony zasobów wiedzy.

dr hab. Bogusz Mikuła, prof. UEK
Uniwersytet Ekonomiczny w Krakowie
Wydział Zarządzania
e-mail: mikulab@uek.krakow.pl

dr inż. Tomasz Stefaniuk
Uniwersytet Przyrodniczo-Humanistyczny w Siedlcach
Wydział Nauk Ekonomicznych i Prawnych
e-mail: tomasz.stefaniuk@uph.edu.pl

Przypis

1) Ich ogólna pojemność to 2,6 TB. Nigdy wcześniej nikt nie ukradł z systemu IT aż tak dużej porcji danych. Wśród skradzionych dokumentów znalazło się 4,8 mln wiadomości e-mail, 3 mln rekordów znajdujących się w bazach danych, 2,2 mln dokumentów, 1,1 mln plików graficznych oraz 320 tysięcy dokumentów tekstowych. dokumenty skradzione z firmy Mossack Fonseca zawierają informacje obciążające wielu prominentnych polityków z 40 krajów (w tym z Polski), którzy rejestrowali w Panamie firmy, chcąc w ten sposób uniknąć płacenia w swoim macierzystym kraju wysokich podatków (Chustecki, 2016).

Bibliografia

[1] *2014 State of Endpoint Risk Report*, Ponemon Institute LLC, Traverse City, 2014.

[2] Błoński E. (2007), *Bezpieczny ekstranet – strefy DMZ*, „Hakin9", Nr 11, https://nfsec.pl/hakin9/dmz.pdf, access date: 12.11.2016.

[3] Boczoń W. (2015), *Policja zatrzymała hakera, który włamał się do Plus Banku*, https://www.bankier.pl/wiadomosc/Policja-zatrzymala-hakera-ktory-wlamal-sie-do-Plus-Banku-7281790.html, data dostępu: 12.06.2017 r.

[4] Chustecki J. (2016), *Panama Papers – największa w historii IT kradzież danych*, http://www.computerworld.pl/news/405011/Panama.Papers.najwieksza.w.historii.IT.kradziez.danych.html, data dostępu: 3.12.2016 r.

[5] Cloud Security Alliance (2016), *Top Threats in 2016*, https://cloudsecurityalliance.org/group/top-threats/, access date: 12.11.2016.

[6] Cloud Standards Customer Council (2017), *Security for Cloud Computing Ten Steps to Ensure Success. Version 3.0*, http://www.cloud-council.org/deliverables/CSCC-Security-for-Cloud-Computing-10-Steps-to-Ensure-Success.pdf, access date: 14.04.2018.

[7] Dahl D. (2011), *10 Tips on How to Research Your Competition*, http://www.inc.com/guides/201105/10-tips-on-how-to-research-your-competition.html, access date: 27.11.2016.

[8] Desouza K.C. (2006), *Knowledge Security: An Interesting Research Space*, „Journal of Information Science & Technology", Vol. 3, No. 1., https://pdfs.semanticscholar.org/26ae/0412577758ddc58272decd826c472032f5a1.pdf, access date: 15.09.2018.

[9] Diks A.K.K. (2001), *Security Considerations for Extranets*, https://www.sans.org/reading-room/whitepapers/basics/security-considerations-extranets-527, access date: 4.09.2016.

[10] Fundacja Bezpieczna Cyberprzestrzeń (2013), *Największe zagrożenia dla bezpieczeństwa Internecie w roku 2013*, https://www.cybsecurity.org/pl/508/, data dostępu: 5.07.2014 r.

[11] Fundacja Bezpieczna Cyberprzestrzeń (2016), *Największe zagrożenia dla bezpieczeństwa w Internecie w roku 2016*, https://www.cybsecurity.org/pl/raport-najwieksze-zagrozenia-dla-bezpieczenstwa-w-internecie-w-2016-roku/, data dostępu: 20.09.2016 r.

[12] „Gazeta prawna" (2014), *Groźne wirusy atakują serwisy społecznościowe. Sprawdź, jak bezpiecznie korzystać z Facebooka i Twittera*, http://serwisy.gazetaprawna.pl/nowe-technologie/artykuly/778909,grozne-wirusy-atakuja-serwisy-spolecznosciowe-sprawdz-jak-bezpiecznie-korzystac-z-facebooka-i-twittera.html, data dostępu: 23.08.2016 r.

[13] Gebert H., Geib M., Kolbe L., Brenner W. (2003), *Knowledge-enabled Customer Relationship Management: Integrating Customer Relationship Management and Knowledge Management Concepts*, „Journal of Knowledge Management", Vol. 7, No. 5, pp. 107–123.

[14] Grance T., Mell P. (2011), *The NIST Definition of Cloud Computing. National Institute of Standards and Technology U.S. Department of Commerce. Special Publication 800 – 809 145*, http://csrc.nist.gov/publications/nistpubs/800–145/SP800–145.pdf, access date: 3.07.2014.

[15] Hołyński M. (2012), *Bezpieczeństwo w chmurach*, „Elektronika" Vol. 53, Nr 8, s. 119–120.

[16] Ilvonen I., Alanne A., Helander N., Väyrynen H. (2016) *Knowledge Sharing and Knowledge Security in Finnish Companies*, [in:] T.X. Bui, R.H. Sprague Jr. (eds.), Proceedings of the 49th Annual Hawaii International Conference on System Sciences HICSS 2016, Los Alamitos, California, Washington, Tokyo, pp. 4021–4030.

[17] Ilvonen I. (2013). *Knowledge Security – A Conceptual Analysis*, Tampere University of Technology. Publication; Vol. 1175, Tampere University of Technology, https://tutcris.tut.fi/portal/files/5468721/ilvonen.pdf, access date: 14.05.2017.

[18] Jacieczko J. (2003), *Źródła informacji wykorzystywane w systemie informacji o konkurencji*, Prace Naukowe Akademii Ekonomicznej w Katowicach, Tom *Systemy wspomagania organizacji SWO*, s. 435–442.

[19] Kiełtyka L. (2002), *Komunikacja w zarządzaniu. Techniki, narzędzia i formy przekazu informacji*, Agencja Wydawnicza Placet, Warszawa.

[20] Kulik W. (2014), *Największe i najdotkliwsze wycieki i włamania 2014 roku*, http://www.benchmark.pl/aktualnosci/wheel-systems-najwieksze-wycieki-wlamania-2014.html, data dostępu: 3.09.2015 r.

[21] Łapiński K., Wyżnikiewicz B. (2011), *Cloud Computing wpływ na konkurencyjność przedsiębiorstw i gospodarkę Polski. Raport*, Instytut Badań nad Gospodarką Rynkową, Gdańsk.

[22] McClure J., Parkinson A. (2017), *The State of Digital and Social Media Risk Management 2017 Edition*, https://www.conference-board.org/retrievefile.cfm?filename=TCB-The-State-of-Digital-and-Social-Media-Risk-Management1.pdf&type=subsite, access date: 12.10.2016.

[23] Mikuła B. (2016), *Zarządzanie wiedzą klienta jako narzędzie poprawy konkurencyjności przedsiębiorstwa*, „e-mentor", Nr 1(63), s. 40–48.

[24] Nonaka I., Takeuchi H. (2000) *Kreowanie wiedzy w organizacji. Jak spółki japońskie dynamizują procesy innowacyjne*, Poltext, Warszawa.

[25] Owen-Smith J., Powell W.W. (2004), *Knowledge Networks as Channels and Conduits: The Effects of Spillovers in the Boston Biotechnology Community*, „Organization Science" Vol. 15, No. 1, pp. 5–21.

[26] Pańkowska M. (2001), *Zarządzanie zasobami informatycznymi*, Difin sp. z o.o, Warszawa.

[27] Pereira T., Santos H., (2017*), Knowledge Security an Empirical Use of IT – Child Abuse Monitor System Model*, ICT4AWE 2017 – 3rd International Conference on Information and Communication Technologies for Ageing Well and e-Health, Porto, Portugal.

[28] PN-ISO/IEC 27001:2014–12 *Technika informatyczna, Techniki bezpieczeństwa Systemy zarządzania bezpieczeństwem informacji – Wymagania*.

[29] Polsatnews (2016), *Prawdopodobnie największy wyciek w historii. Dane z 500 mln kont Yahoo wykradzione*, http://www.polsatnews.pl/wiadomosc/2016–09–22/prawdopodobnie-najwiekszy-wyciek-w-historii-dane-z-500-mln-kont-yahoo-wykradzione/, data dostępu: 5.11.2016 r.

[30] Porębska-Miąc T. (2005), *Wiedza i zarządzanie wiedzą w systemie CRM*, Prace Naukowe Akademii Ekonomicznej w Katowicach, Tom *Systemy wspomagania organizacji SWO*, s. 354–361.

[31] PWC (2016) *W obronie cyfrowych granic, czyli 5 rad, aby realnie wzmocnić ochronę firmy przed Cyber ryzykiem*, https://www.pwc.pl/pl/pdf/raport-pwc-gsiss-cyberzagrozenia-2016.pdf, data dostępu: 26.11.2016 r.

[32] Ritala P., Olander H., Michailova S., Husted K. (2015), *Knowledge sharing, knowledge leaking and relative innovation performance: An empirical study*, „Technovation", No. 35, pp. 22–31.

[33] Rowley J. (2006), *Customer Knowledge Management*, [in:] Academy of Management Best Papers Proceedings, http://www.aom-iaom.org/pdfs/jms/JSM-18–06_rowley.pdf, access date: 11.11.2015.

[34] Russel J. (2017), *Social Media Security Risks and How to Avoid Them*, https://blog.hootsuite.com/social-media-security-for-business/, access date: 16.10.2016.

[35] Solga R. (2013), *Pracownik z własną listą klientów*, http://tajemnica-przedsiebiorstwa.pl/pracownik-z-wlasna-lista-klientow/, data dostępu: 23.11.2016 r.

[36] Szumniak-Samolej J. (2010), *Cyfrowy aktywizm. Zagrożenie dla biznesu, czy szansa dla CSR?* http://odpowiedzialnybiznes.pl/artykuly/cyfrowy-aktywizm-zagrozenie-dla-biznesu-czy-szansa-dla-csr/, data dostępu: 4.09.2016 r.

[37] Tomkiewicz M. (2011), *5 głównych zagrożeń związanych z serwisami społecznościowymi*, http://www.internet-standard.pl/news/374491/5.glownych.zagrozen.zwiazanych.z.serwisami.spolecznosciowymi.html, data dostępu: 28.05.2016 r.

[38] Trolan S. (1998), *Extranet security: What's Right for Your Business?* http://www.ittoday.info/AIMS/DSM/87–10–17, pdf, access date: 12.10.2016.

Threats to Knowledge Security in the Area of Customer Knowledge Management

Summary

The article focuses on the issues of threats to knowledge safety that occur while implementing customer knowledge management (CKM). This modern method of knowledge acquisition allows for making use of the creative potential of clients. Compared to classic CRM, CKM focuses on knowledge possessed by clients, and their potential to use that knowledge in the process of new knowledge creation. Unfortunately, working with knowledge resources under the CKM and application of computer technology in CKM processes produce a number of risks for the company and its customers. Threats to knowledge resources security arise from the very fact of implementing individual processes within the CKM (gaining knowledge about the client, gaining knowledge from the client, creating knowledge with the client or transferring knowledge to the client). Also tools used in CKM, as well as working in the network environment, result in greater or lesser possibilities of incidents that may constitute threats to knowledge resources security.

Keywords

knowledge management, customer knowledge management, customer relationship management, knowledge security, threats to the knowledge security