Sylwia Sobolewska[1]

Ochrona informacji marketingowej w przedsiębiorstwie

1. Wstęp

Potrzeba ochrony istniejącej w przedsiębiorstwie informacji marketingowej wynika z jej kluczowego znaczenia dla funkcjonowania przedsiębiorstwa na rynku. Informacje związane ze strategią marketingową, klientami przedsiębiorstwa, a także wynikami prowadzonych działań promocyjnych mogą być obiektem zainteresowania zarówno podmiotów gospodarczych (konkurentów, agencji wywiadowczych, partnerów biznesowych), jak i organizacji przestępczych czy też hakerów indywidualnych. Celem niniejszego artykułu jest przedstawienie współczesnych zagrożeń oraz czynników warunkujących ochronę informacji marketingowej.

2. Specyfika informacji marketingowej

Informacja marketingowa obejmuje „wszelkie informacje pochodzące z rynku i wnętrza firmy, poszerzające wiedzę o możliwościach i utrudnieniach jej marketingowego działania, służące menedżerom za podstawę podejmowania decyzji marketingowych i kontroli ich skutków”[2]. Informacja marketingowa dotyczy bowiem różnorodnych aspektów prowadzonych działań, ale w szczególności klientów, konkurentów i wszelkich zmian w otoczeniu.

Informacja marketingowa w pierwszej kolejności zlokalizowana jest w działach marketingu i sprzedaży. Dla bezpieczeństwa informacji istotne jest, że dział

---

[1] Szkoła Główna Handlowa, Instytut Informatyki i Gospodarki Cyfrowej, Zakład e-biznesu.

[2] J. Penc, za: R. Pieczykolan, *Informacja marketingowa*, Polskie Wydawnictwo Ekonomiczne, Warszawa 2005.

marketingu jest jednostką, która utrzymuje rozległe relacje zarówno z innymi działami przedsiębiorstwa, jak i z podmiotami zewnętrznymi (agencje marketingowe, agencje reklamowe, jednostki badawcze, wykonawcy materiałów reklamowych). Pracownicy marketingu z założenia mają być osobami kreatywnymi i kontaktowymi, ponieważ dział marketingu, łączący nierzadko w sobie funkcję działu PR, to ta część przedsiębiorstwa, która ma najwięcej relacji z otoczeniem zewnętrznym. Oznacza to, że pracownicy mogą stać się osobowym źródłem informacji dla działań wywiadowczych prowadzonych przez firmy konkurencyjne. Im więcej kontaktów, tym większe ryzyko dla bezpieczeństwa informacji. Liczne kontakty z podmiotami zewnętrznymi często wiążą się z przekazywaniem różnorodnych informacji o przedsiębiorstwie, trzeba zatem zadbać, aby nie było przypadkowych wycieków danych, a z takimi sytuacjami możemy mieć do czynienia, gdy pracownik na przykład nie jest świadomy wartości określonych informacji. W kwestii informacji marketingowych ważna jest bowiem obrona przed utratą nie tylko danych, które są w systemach informatycznych przedsiębiorstwa, lecz także w głowach pracowników. Chcąc chronić informację marketingową, trzeba zadbać o nadawanie odpowiednich klauzul informacjom tajnym czy poufnym.

Należy zauważyć, że nie wystarczy jedynie poinformować pracowników, że dane są tajne lub poufne, ponieważ – jak wynika z badań – pracownicy są skłonni do nieprzestrzegania tajemnic, jeśli mają wątpliwości co do zasadności opatrzenia informacji klauzulą „tajne", „poufne" lub uważają, że działając wbrew zasadom, mogą przynieść korzyści przedsiębiorstwu, na przykład sprzedawca, który ujawnia klientowi informację, może dzięki temu zrealizować dużą sprzedaż lub osoba odpowiadająca za design rozmawia ze swoim kolegą po fachu i dzięki temu może zrobić lepszy produkt[3]. Należy również szkolić pracowników działów posiadających informacje marketingowe z zakresu bezpiecznego przenoszenie danych oraz korzystania ze sprzętu komputerowego (np. unikanie korzystania ze sprzętu innego podmiotu ze względu na możliwość zainfekowania pendrive'a), rozpoznawania działań wywiadowczych oraz cyberbepieczeństwa i zasad bezpiecznego korzystania z urządzeń połączonych z Internetem. Do najniebezpieczniejszych miejsc z punktu widzenia bezpieczeństwa informacji należą porty USB, do których podłączamy między innymi pendrive'y. Jak pisze E. Lucas: „port USB jest jedną z istotniejszych dziur w bezpieczeństwie komputerowym", co wynika z faktu, że „komputery są tak skonfigurowane, by

[3] D.R. Hannah, K. Robertson, *Why and How Do Employees Break and Bend Confidential Information Protection Rules?*, „Journal of Management Studies" 2015, vol. 52, issue 3, s. 409.

akceptować USB nawet, gdy zachowuje się w sposób dziwny, ponieważ urządzenia z tym złączem często mają wiele funkcji"[4].

Informacja marketingowa znajduje się również w dziale sprzedaży, który obejmuje handlowców pracujących najczęściej w terenie, mających bezpośredni kontakt z dystrybutorami oraz klientami, a jednocześnie stanowią grupę pracowników odznaczających się wysoką fluktuacją, co również rodzi zagrożenie dla bezpieczeństwa informacji. W tym względzie istotne jest zatem zbudowanie lojalnej kadry pracowników, a także odpowiednie przeszkolenie w zakresie zasad bezpiecznego korzystania z danych na urządzeniach mobilnych (systemy mobilnej sprzedaży to podstawowe programy dla handlowców).

Kolejna kwestia to rozwój innych urządzeń podłączonych do Internetu. Zgodnie z prognozami Gartnera do 2020 roku z Internetem zostanie połączonych ponad 20 mld urządzeń, co oczywiście daje nowe możliwości również w sferze informacyjnej przedsiębiorstw, natomiast stwarza też ogromne zagrożenia. Rzeczy podłączone do Internetu to dla specjalistów od marketingu możliwość zdobywania informacji o sposobie korzystania z rzeczy przez użytkowników, co jest bezcenne nie tylko dla działu R&D, lecz także istotne w ustalaniu strategii komunikacji przedsiębiorstwa z klientami. Jednak rzeczy podłączone do Internetu to także pokusa dla przestępców, którzy mogą próbować pozyskać informacje na przykład o tym, kiedy danej osoby nie ma w domu (urządzenia sterujące zużyciem prądu, ogrzewanie). Dla przedsiębiorstw rodzi to obowiązek dbania o zabezpieczenie oprogramowania rzeczy podłączonych do Internetu, ponieważ dopuszczenie do włamania może oznaczać brak sprzedaży kolejnych egzemplarzy produktu.

3. Wymogi prawne dotyczące bezpieczeństwa informacji marketingowych

Jednym z podstawowych źródeł informacji marketingowej, które musi być chronione, są bazy danych przedsiębiorstwa, a szczególnie bazy z danymi klientów. W wypadku danych i informacji dotyczących klientów, ochrona danych jest wymogiem ustawowym, ponieważ od 1997 roku obowiązuje Ustawa o ochronie danych osobowych. Zgodnie z artykułem 36 punkt 1 Ustawy: „Administrator danych jest obowiązany zastosować środki techniczne i organizacyjne

[4] E. Lucas, *Oswoić cyberświat*, Kurhaus Publishing, Warszawa 2017, s. 185.

zapewniające ochronę przetwarzanych danych osobowych odpowiednią do zagrożeń oraz kategorii danych objętych ochroną, a w szczególności powinien zabezpieczyć dane przed ich udostępnieniem osobom nieupoważnionym, zabraniem przez osobę nieuprawnioną, przetwarzaniem z naruszeniem ustawy oraz zmianą, utratą, uszkodzeniem lub zniszczeniem"[5].

W rozporządzeniu do ustawy określono wymogi, jakie spełnić musi podmiot przetwarzający dane osobowe, aby można było uznać, że dane klienta są chronione. Jednak od maja 2018 roku zaczną obowiązywać nowe przepisy dotyczące podmiotów przetwarzających dane osobowe. 25 maja 2018 roku obowiązywać zacznie jednolite dla wszystkich krajów Unii Europejskiej Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 roku w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych (ogólne rozporządzenie o ochronie danych), popularnie nazywane RODO. Największą zmianą, jaka wiąże się z wejściem w życie nowych przepisów, jest uczynienie administratora danych, odpowiedzialnego za określenie, jakie procedury muszą być przyjęte w przedsiębiorstwie i jak ma przetwarzać dane, aby były bezpieczne. Jest to znacząca zmiana, która wymaga od podmiotów przemyślenia, jakie dane chcą zbierać, jak i gdzie przetwarzać, aby były bezpieczne. Umowa o powierzeniu danych (np. przeniesienie do chmury Microsoftu) nie zdejmuje z przedsiębiorstwa powierzającego dane odpowiedzialności za ich bezpieczne przetwarzanie. Nowe rozporządzenie kładzie na barki administratorów danych całą odpowiedzialność za bezpieczeństwo przetwarzanych danych, bez podpowiedzi, co ma być wykonane (brak dodatkowych wytycznych podobnych do tych znajdujących się w obecnym rozporządzeniu do ustawy z 1997 r.).

Z kontroli GIODO wynika, że administratorzy danych mają problem z odpowiednim opracowaniem dokumentacji dotyczącej przetwarzanych danych, a także z zapewnieniem odpowiednich środków technicznych i organizacyjnych[6]. „Nowe przepisy zaostrzają również obowiązki informacyjne podmiotów, które doświadczą nieuprawnionego dostępu do danych. Zgodnie z nowymi przepisami administratorzy danych są zobowiązani do informowania organów nadzorujących

[5] Art. 36, pkt 1 Ustawy z 29 sierpnia 1997 r. o ochronie danych osobowych, www.giodo.gov.pl (dostęp: 20.12.2017).

[6] I. Jackowska, *GIODO nie wyręczy administratora danych*, https://www.pb.pl/giodo-nie-wyreczy-administratora-danych-834747#&gid=1&pid=16863251951 (dostęp: 20.08.2017).

o uchybieniach bez zbędnej zwłoki, w miarę możliwości nie później niż w terminie 72 godzin po stwierdzeniu naruszenia"[7].

Ponadto administratorzy muszą dokumentować wszelkie naruszenia w zakresie ochrony danych osobowych, ich następstwa i podjęte działania naprawcze[8]. Zgodnie z informacją GIODO w roku 2015 wpłynęły jedynie 24 zawiadomienia o podejrzeniu popełnienia przestępstwa[9]. Wydaje się, że liczba ta może być niedoszacowana, ponieważ w wielu przedsiębiorstwach, jeśli nie zostanie stwierdzona kradzież danych, sprawa nie jest zgłaszana. Jak mówi jeden z ekspertów PwC, P. Skrzypczyński: „Dla firm działających w Polsce cyberataki są nadal rzeczą wstydliwą. Nie przyznają się, że padły ich ofiarą w obawie przed utratą dobrego wizerunku i zaufania klientów"[10].

4. Zagrożenia dla bezpieczeństwa informacji

Zagrożenia związane z bezpieczeństwem informacji, nie tylko marketingowej, można podzielić na dwa podstawowe rodzaje: wewnętrzne i zewnętrzne.

Zagrożenia wewnętrzne odnoszą się do transferu informacji do innych stron niż upoważnione przez pracowników, którzy mają dostęp do wrażliwych informacji[11]. Oczywiście transfer ten może być umożliwiony przez pracownika celowo lub nieświadomie. W pierwszym wypadku najczęściej wiąże się to z chęcią otrzymania od zleceniodawcy odpowiedniej zapłaty za dostarczone informacje, chociaż motyw finansowy nie musi być jedynym. Do innych przyczyn świadomego udostępnienia informacji można zaliczyć: zemstę, złość, obawę o stratę pracy, przyjemność i rozrywkę, przekupstwo, sprzeniewierzenie, szpiegostwo, sabotaż[12].

---

[7] M. Cwener, *Zgłaszanie incydentów bezpieczeństwa do organu nadzorczego. Analiza art. 33 GDPR*, http://gdpr.pl/zglaszanie-incydentow-bezpieczenstwa-organu-nadzorczego-analiza-art-33-gdpr (dostęp: 20.08.2017).

[8] M. Kołodziej, M. Kluska, G. Wanio, *Vademecum administratora bezpieczeństwa informacji*, C.H. Beck, Warszawa 2016, s. 121.

[9] I. Jackowska, op. cit.

[10] P. Skrzypczyński, *Cyberprzestępcy atakują. Zagrożone firmy, zagrożeni zwykli obywatele*, http://superbiz.se.pl/firma/cyberprzestepcy-atakuja-zagrozone-sa-firmy-zagrozeni-zwykli-obywatele_814060.html (dostęp: 20.08.2017).

[11] N. Sohrabi Safa, C. Maple, T. Watson, *The information security landscape in the supply chain*, „Computer Fraud &Security" June 2017, vol. 2017, issue 6, s. 16.

[12] Ibidem.

Z kolei wśród przyczyn niezamierzonego transferu można wymienić: ignorancję, brak świadomości, niedbalstwo.

Człowiek jest najsłabszym ogniwem w walce z bezpieczeństwem informacji. W wypadku pracowników marketingu są to najczęściej osoby, które systemy informatyczne znają jedynie jako użytkownicy i często wierzą, że nad bezpieczeństwem ich działań czuwają pracownicy IT instalujący odpowiednie *firewalle* i inne rozwiązania zapewniające bezpieczeństwo. Tymczasem oprócz zabezpieczeń ze strony działu IT, ważne jest odpowiednie zachowanie pracowników. Do najczęstszych błędów popełnianych przez pracowników przedsiębiorstw należą[13]:

- przenoszenie niezaszyfrowanych informacji przedsiębiorstwa na dyskach zewnętrznych i pendrive'ach;
- udostępnianie nazwy użytkownika oraz hasła współpracownikom;
- pisanie informacji dotyczących konta na kartce, a następnie umieszczanie jej na monitorze lub biurku;
- pozostawianie stanowiska pracy w trybie zalogowania do systemu;
- otwieranie e-maili od nieznanych nadawców i instalowanie załączników;
- instalowanie oprogramowania z Internetu.

Oprócz zagrożeń związanych z nieprzestrzeganiem zasad bezpieczeństwa informacji, istnieje wiele zagrożeń wynikających z korzystania z urządzeń podłączonych do Internetu, które należą do zagrożeń zewnętrznych. Codziennie odkrywane są nowe sposoby atakowania komputerów przez przestępców cybernetycznych, natomiast już znane metody to na przykład *phishing*, *keylogger* i inne zawarte w tabeli 1.

Ciągły postęp technologiczny zmienia praktycznie każdy aspekt funkcjonowania przedsiębiorstwa. Dostęp do informacji jest możliwy z poziomu urządzeń mobilnych, dzięki czemu z jednej strony łatwiejszy jest do niej dostęp w każdym miejscu i czasie, kiedy jest potrzebna, a z drugiej stwarza to zagrożenie dla bezpieczeństwa informacji. Rosnąca liczba urządzeń mobilnych powoduje, że wzrasta zagrożenie dla danych dostępnych z poziomu smartfona, tabletu czy też laptopa, zabieranego do domu przez pracownika. M. Chudy (dyrektor ds. operacyjnych Integrated Solutions) zauważa: „z naszych badań wynika, że tylko 4 proc. polskich firm chroni informacje przetwarzane na urządzeniach mobilnych swoich pracowników. To ogromne ryzyko, zwłaszcza jeśli na służbowym smartfonie przechowujemy wrażliwe dane, listę klientów, umowy lub faktury"[14]. Specjalista

[13] Ibidem.

[14] S. Kaczmarek, *Dane mobilne coraz bardziej zagrożone, ale ich analiza bardzo pomaga w biznesie*, http://it-filolog.pl/dane-mobilne-coraz-bardziej-zagrozone-ale-ich-analiza-bardzo-pomaga-w-biznesie/ (dostęp: 20.08.2017).

w zakresie cyberprzestępczości G. Lucas wskazuje, że producenci telefonów komórkowych jak na razie przegrywają walkę z mobilnym złośliwym oprogramowaniem, z czego bardziej na ataki narażone są komórki z systemem Androida niż Ios, ponieważ Apple wnikliwiej ocenia aplikacje, które będą dostępne do zainstalowania na ich urządzeniach[15].

Tabela 1. Cybernetyczne zagrożenia i ich definicje

Zagrożenia	Definicje
Atak DDoS	Atak mający na celu wykorzystanie całej przepustowości systemu; polega na zaśmiecaniu danego komputera – na przykład serwera, który obsługuje stronę internetową, wielokrotnie powtarzanymi żądaniami połączenia, przez co uniemożliwia użytkownikom korzystanie z niego
Atak przy wodopoju	Wstawianie złośliwego oprogramowania na stronę internetową celem zainfekowania konkretnej kategorii odwiedzających (atak *driver-by*)
Atak SQL	Sposób na infekowanie komputera za pośrednictwem strony internetowej, z której korzysta użytkownik
Browser hijackers	Programy, które uruchamiają się za każdym razem, gdy użytkownik uruchamia przeglądarkę, aby zbierać informacje dotyczące zachowania użytkownika w Internecie
Keylogger	Programy, które umożliwiają śledzenie znaków wpisywanych na klawiaturze
Konie trojańskie	Złośliwe programy, których celem może być kradzież danych lub zniszczenie systemu
Malware	Złośliwe oprogramowanie wykorzystywane do ataków na komputery i sieci
Phishing	Wysyłanie e-maili zawierających linki lub załączniki, które po otworzeniu mogą zainfekować komputer ofiary
Rogueware	Złośliwe oprogramowanie sprawiające wrażenie legalnego
Scumware	Programy, które zmieniają zawartość stron, na które wchodzi internauta, zmieniają normalne linki przez dodanie odnośników, przekierowują na inne strony

Źródło: opracowanie własne na podstawie: E. Lucas, *Oswoić cyberświat*, Kurhaus Publishing, Warszawa 2017, s. 292–293; N. Sihrabi Safa, C. Maple, T. Watson, *The information security landscape in the supply chain*, „Computer Fraud &Security" June 2017, vol. 2017, issue 6, s. 16 oraz *Złośliwe oprogramowanie – choroba systemu komputerowego*, http://websecurity.pl/zlosliwe-oprogramowanie-choroba-systemu-komputerowego/ (dostęp: 3.08.2017).

W badaniach przeprowadzonych w 2013 roku przez firmę Intel wśród przedsiębiorstw polskich, węgierskich, słowackich i czeskich okazało się, że w przypadku polskich przedsiębiorstw 45% nie zabezpiecza danych na laptopie w żaden

[15] E. Lucas, op. cit., s. 184.

sposób, 17% traci laptopy podczas podróży pracowników, a 29,6% laptopów zostaje skradzionych w firmach[16].

Zgodnie z raportem badań poświęconych bezpieczeństwu informacyjnemu przeprowadzanych przez Ernst&Young na próbie 1735 CIO's, do obszarów, które w przedsiębiorstwach mają najwyższy priorytet w sferze bezpieczeństwa, należy zaliczyć: zapewnienie ciągłości działania przedsiębiorstwa/odporność na awarie (57%), zapobieganie utracie danych/zapobieganie wyciekom danych (57%), świadomość i szkolenie w zakresie bezpieczeństwa (55%)[17]. Kwestia bezpieczeństwa informacji jest o tyle istotna, że dla 46% przedsiębiorstw utrata danych tylko z trzech dni stanowiłaby krytyczne zagrożenie dla biznesu, w przypadku utraty danych z tygodnia odsetek ten zwiększyłby się do 66%, a utrata danych z miesiąca byłaby krytyczna dla 86% przedsiębiorstw[18]. Wynika to z faktu, że dziś większość danych jest gromadzona w formie cyfrowej. Trudno byłoby dzisiaj znaleźć średnie przedsiębiorstwo, które ma klientów zapisanych na kartkach w segregatorze.

5. Możliwości zwiększania bezpieczeństwa informacyjnego

Tworząc bezpieczny system informacyjny, należy uwzględnić uwarunkowania ludzkie, technologiczne, zarządcze, edukacyjne, społeczne, kulturowe oraz środowiskowe[19]. Przedsiębiorstwa działają w otoczeniu organizacyjnym, w którym łączą je relacje z różnymi podmiotami (partnerami, dostawcami, odbiorcami). Im więcej połączeń między systemami różnych przedsiębiorstw, tym większe ryzyko dla bezpieczeństwa informacji. Z tego względu należy łączyć swoje doświadczenia w zakresie walki z nieuprawnionym dostępem do danych przedsiębiorstwa. W amerykańskich przedsiębiorstwach często w strukturach organizacyjnych przedsiębiorstw występują jednostki wywiadu gospodarczego

---

16 Intel, *Polacy najwięcej tracą na zgubieniu firmowych laptopów*, https://biznes.newseria.pl/komunikaty/intel_polacy_najwiecej,b1390747873 (dostęp: 4.08.2017) oraz Informacja prasowa Intel, *Polacy najwięcej tracą na zgubieniu firmowych laptopów* (dostęp: 20.12.2017).

17 *Path to cyber resilience: Sense, restrict, react, EY's 19th Global Information Security Survey 2016–2017*, http://www.ey.com/Publication/vwLUAssets/ey-global-information-security-survey-2016-pdf/%24FILE/GISS_2016_Report_Final.pdf (dostęp: 20.12.2017).

18 P. Grabiec, *Bezpieczeństwo, ryzyko i dostępność, czyli jak do bezpieczeństwa IT podchodzą polskie małe i średnie firmy*, http://www.spidersweb.pl/2015/08/hp-polska-raport-bezpieczenstwo-ryzyko-dostepnosc.html (dostęp: 12.08.2017).

19 N. Sohrabi Safa, C. Maple, T. Watson, op. cit., s. 16.

czy też wywiadu marketingowego. W Polsce samo słowo „wywiad" ma najczęściej negatywne konotacje, kojarzące się z nielegalną działalnością, podsłuchami, szpiegowaniem[20]. Tymczasem jednostka wywiadu znajdująca się w przedsiębiorstwie ma za zadanie stale monitorować zmiany w otoczeniu, aby dostarczać decydentom informacje istotne dla decyzji podejmowanych w kwestii przyszłości przedsiębiorstwa. W związku z rosnącym zagrożeniem przestępstwami w cyberprzestrzeni w amerykańskiej teorii zarządzania pojawiła się koncepcja *strategic cyber intelligence*[21], która oznacza wywiad ukierunkowany na bezpieczeństwo w cyberprzestrzeni. Działania w ramach tego wywiadu mają pomóc przedsiębiorstwu w zdiagnozowaniu, kto może zaatakować przedsiębiorstwo, jakie informacje mogą przestępcy chcieć wykraść, jakie informacje są kluczowe dla przedsiębiorstwa[22]. Do tego przydaje się współpraca z komórkami wywiadu, a także działami marketingu, które mają rozeznanie w krajobrazie konkurencji.

Częstym problem związanym z zapewnieniem bezpieczeństwa jest przeznaczanie odpowiednich środków budżetowych na ten cel. Niepokojące może być, że jak wynika z raportu *Path to cyber resilience: Sense, resist, Reach, EY's 19th Global Information Security Survey 2016–17*, 58% firm nie zwiększyłoby wydatków na bezpieczeństwo, nawet jeśli zostałby zaatakowany główny konkurent[23]. Tymczasem trzeba zauważyć, że przestępcy lubią atakować firmy z tej samej branży, o podobnej infrastrukturze, ponieważ posiadają wiedzę z sukcesem zakończonego ataku i mogą ją wykorzystać do włamania do kolejnego podmiotu. Z tego względu warto wymieniać się doświadczeniami w zakresie ataków i obrony, ponieważ można uniknąć kosztownych błędów. Jak podkreślają autorzy raportu, system bezpieczeństwa jest silniejszy, jeśli bierze się pod uwagę wydarzenia z otoczenia[24].

Powszechnym problemem jest również brak ekspertów w zakresie cyberbezpieczeństwa. Ekspertów takich brakuje nie tylko na polskim rynku, ale w większości krajów. W jednym z artykułów autorzy podkreślają, że brakuje specjalistów w zakresie bezpieczeństwa informacyjnego (*cyber-security*), a także brakuje młodych ludzi zajmujących się tą profesją, a co gorsza – brakuje kadry,

---

[20] M. Ciecierski, R. Nogacki, *Bezpieczeństwo współczesnej firmy*, Studio Emka, Warszawa 2016, s. 80–81.

[21] R. Borum, J. Felker, S. Kern, K. Dennensen, T. Feyes, *Strategic cyber intelligence*, „Information&Computer Security" 2015, vol. 23, no. 3, s. 319 (s. 317–330).

[22] Ibidem.

[23] *Path to cyber resilience: Sense, resist, Reach, EY's 19th Global Information Security Survey 2016–17*, http://www.ey.com/Publication/vwLUAssets/ey-global-information-security-survey-2016-pdf/%24FILE/GISS_2016_Report_Final.pdf (dostęp: 12.08.2017).

[24] Ibidem.

która mogłaby takich młodych ludzi kształcić[25]. W Polsce kierunek „Kryptologia i cyberbezpieczeństwo" dostępny jest jedynie na Wydziale Cybernetyki Wojskowej Akademii Technicznej[26], natomiast w ofercie studiów podyplomowych możemy znaleźć już więcej kierunków na różnych uczelniach[27]. Fakt, że tematyka bezpieczeństwa systemów informatycznych znajduje odbiorców na studiach podyplomowych świadczyć może o tym, że praktycy dostrzegają problem bezpieczeństwa i szukają kierunków pozwalających uzupełnić wiedzę w tym zakresie. W dokumencie *Strategia cyberbezpieczeństwa Rzeczpospolitej Polskiej na lata 2016–2020* zwraca się uwagę na konieczność kształcenia w zakresie cyberbezpieczeństwa od najmłodszych lat, czyli jeszcze w szkole podstawowej, a także na „uruchamianie w szkołach wyższych nowych kierunków studiów kładących większy nacisk na zagadnienia związane z cyberbezpieczeństwem"[28]. Niedostatki w zakresie specjalistów od bezpieczeństwa cybernetycznego powodują, że na przykład w Wielkiej Brytanii prawie połowa przedsiębiorstw ma poczucie, że brakuje im umiejętności, aby przeciwstawić się zagrożeniom cybernetycznym, przed których obliczem stoją[29].

6. Podsumowanie i kierunki dalszych badań

Ochrona informacji marketingowej ma dla każdego przedsiębiorstwa znaczenie strategiczne. Wciąż najsłabszym ogniwem w obszarze bezpieczeństwa informacyjnego przedsiębiorstwa są pracownicy. W przypadku pracowników działów marketingu i sprzedaży, którzy mają rozległe kontakty z otoczeniem zewnętrznym, co wynika z charakteru ich pracy, należy zwrócić szczególną uwagę na ich edukację w sferze zasad bezpieczeństwa związanego z korzystaniem z systemów informatycznych przedsiębiorstwa, a także informacji tajnych i poufnych.

---

[25] S. Furnell, P. Fischer, A. Finch, *Can't get the staff? The growing need for cyber – security skills*, „Computer Fraud&Security", February 2017, s. 5–6.

[26] http://www.otouczelnie.pl/studia/kierunki_studiow?slowo=bepziecze%C5%84stwo+http://www.otouczelnie.pl/studia/kierunki_studiow?slowo=KRYPTOLOGIA+I+CYBERBEPIECZE%C5%83STWO (dostęp: 8.08.2017).

[27] Na przykład „Bezpieczeństwo systemów informacyjnych wraz z technikami biometrycznymi", „Bezpieczeństwo systemów informatycznych" „Bezpieczeństwo w środowiskach sieci teleinformatycznych", „Administracja i bezpieczeństwo systemów sieciowych".

[28] *Strategia cyberbezpieczeństwa Rzeczpospolitej Polskiej na lata 2016–2020*, http://m.mc.gov.pl/files/strategia_v_29_09_2016.pdf (dostęp: 8.08.2017).

[29] S. Furnell, P. Fischer, A. Finch, op. cit.

W dalszych badaniach warto przyjrzeć się rozwiązaniom przyjmowanym w polskich przedsiębiorstwach, ponieważ dostępna literatura dotyczy w większości rynku amerykańskiego, gdzie obowiązują zupełnie inne przepisy związane chociażby z ochroną danych osobowych, a także inna jest kultura organizacyjna, inaczej funkcjonują jednostki wywiadu gospodarczego/marketingowego w przedsiębiorstwach. Należy również objąć badaniami kwestie bezpieczeństwa związane z korzystaniem z urządzeń mobilnych oraz internetu rzeczy.

Bibliografia

Furnell S., Fischer P., Finch A., *Can't get the staff? The growing need for cyber – security skills*, „Computer Fraud&Security", February 2017.

Borum R., Felker J., Kern S., Dennensen K., Feyes T., *Strategic cyber intelligence*, „Information&Computer Security" 2015, vol. 23, no. 3.

M. Ciecierski, R. Nogacki, *Bezpieczeństwo współczesnej firmy*, Studio Emka, Warszawa 2016.

Hannah D.R., Robertson K., *Why and How Do Employees Break and Bend Confidential Information Protection Rules?*, „Journal of Management Studies" 2015, vol. 52, issue 3.

Kołodzie M., Kluska M., Wanio G., *Vademecum administratora bezpieczeństwa informacji*, C.H. Beck, Warszawa 2016.

Lucas E., *Oswoić cyberświat*, Kurhaus Publishing, Warszawa 2017.

Pieczykolan R., *Informacja marketingowa*, Polskie Wydawnictwo Ekonomiczne, Warszawa 2005.

Sohrabi Safa N., Maple C., Watson T., *The information security landscape in the supply chain*, „Computer Fraud &Security" June 2017, vol. 2017, issue 6.

Ustawa o ochronie danych osobowych z 29 sierpnia 1997 r. (Dz.U. 1997, nr 133, poz. 883).

Źródła sieciowe

Cwener M., *Zgłaszanie incydentów bezpieczeństwa do organu nadzorczego. Analiza art. 33 GDPR*, http://gdpr.pl/zglaszanie-incydentow-bezpieczenstwa-organu-nadzorczego-analiza-art-33-gdpr (dostęp: 20.08.2017).

Cyberprzestępcy atakują. Zagrożone firmy, zagrożeni zwykli obywatele, http://superbiz.se.pl/firma/cyberprzestepcy-atakuja-zagrozone-sa-firmy-zagrozeni-zwykli-obywatele_814060.html (dostęp: 20.08.2017).

Grabiec P., *Bezpieczeństwo, ryzyko i dostępność, czyli jak do bezpieczeństwa IT podchodzą polskie małe i średnie firmy*, http://www.spidersweb.pl/2015/08/hp-polska-raport-bezpieczenstwo-ryzyko-dostepnosc.html (dostęp: 12.08.2017).

Intel, *Polacy najwięcej tracą na zgubieniu firmowych laptopów*, https://biznes.newseria.pl/komunikaty/intel_polacy_najwiecej,b1390747873 (dostęp: 4.08.2017).

Jackowska I., *GIODO nie wyręczy administratora danych*, https://www.pb.pl/giodo-nie-wyreczy-administratora-danych-834747#&gid=1&pid=16863251951 (dostęp: 20.08.2017).

Kaczmarek S., *Dane mobilne coraz bardziej zagrożone, ale ich analiza bardzo pomaga w biznesie*, http://it-filolog.pl/dane-mobilne-coraz-bardziej-zagrozone-ale-ich-analiza-bardzo-pomaga-w-biznesie/ (dostęp: 20.08.2017).

Path to cyber resilience: Sense, resist, Reach, EY's 19th Global Information Security Survey 2016–17, http://www.ey.com/Publication/vwLUAssets/ey-global-information-security-survey-2016-pdf/%24FILE/GISS_2016_Report_Final.pdf (dostęp: 12.08.2017).

Strategia cyberbezpieczeństwa Rzeczpospolitej Polskiej na lata 2016–2020, http://m.mc.gov.pl/files/strategia_v_29_09_2016.pdf (dostęp: 8.08.2017).

* * *

Protection of Marketing Information

Summary

Marketing information is crucial for each company market activity, that is why its security is really important. Protection of marketing information needs not only IT solutions but also employees' awareness of cyber and other threats like, for example intelligence activities. Sales and marketing departments' employees should be trained in the field of cyber security and should be informed which information is confidential and why.

Keywords: marketing information, cyber security, employee behavior.