Jowita Sobczak

Przeciwdziałanie nielegalnemu wywiadowi gospodarczemu w przedsiębiorstwie

W warunkach globalnej, coraz bardziej zaostrzającej się konkurencji informacja jest postrzegana jako najważniejsze źródło zdobycia przewagi konkurencyjnej. Dzieje się tak głównie dlatego, że czynnikiem sukcesu są działania niekonwencjonalne, innowacyjne, odmienne od dotychczasowych praktyk biznesowych. Muszą one być oparte na informacji, i to takiej, która jest trudno dostępna dla konkurentów. Aby informacja spełniła warunek niepowtarzalności, nie może być powszechnie dostępna. Tak jest przede wszystkim w przypadku wiedzy tworzonej w przedsiębiorstwach. Jeśli natomiast w danej firmie brakuje dostatecznie sprawnej organizacji, zdolnej w porę zapobiec nieuprawnionemu wyciekowi know-how i wszelkiego rodzaju innych niematerialnych aktywów, to cały system zarządzania informacją okaże się mało skuteczny przy tworzeniu trwałej przewagi konkurencyjnej.

Prowadzenie działalności gospodarczej nie jest możliwe bez informacji, która wspomaga podejmowanie strategicznych decyzji, planowanie czy zarządzanie wieloma obszarami przedsiębiorstwa. Informacja jest również narzędziem walki z konkurencją. Przedsiębiorstwa, które mają istotne dla swojej działalności informacje, zwiększają swoje szanse na utrzymanie przewagi w danym sektorze działalności.

Z kolei ich utrata może prowadzić do obniżenia pozycji ekonomicznej przedsiębiorstwa, a nawet do zakończenia jego działalności. Do najważniejszych skutków naruszenia bezpieczeństwa informacji zalicza się zmniejszenie dochodów oraz obniżenie konkurencyjności.

Obecnie istnieje coraz więcej ośrodków dostarczających informacje przedsiębiorcom (tzw. dostawcy informacji), czyli firmy, które wyspecjalizowały się w określonych produktach informacyjnych. Należą do nich m.in. wywiadownie gospodarcze, biura detektywistyczne oraz systemy informacji gospodarczej – na szczeblu regionalnym, krajowym i międzynarodowym.

Na gruncie gospodarczym zdobywaniem informacji zajmują się różne podmioty:

- przedsiębiorstwa gromadzące informacje na własne potrzeby, aby konkurować na rynku,
- podmioty, które pozyskują informacje i sprzedają je innym (dostawcy usług informacyjnych, pośrednicy, brokerzy itp.),
- organizacje non profit (np. biblioteki i agendy publiczne), które pełnią określoną misję społeczną.

Przedmiotem zainteresowania tych podmiotów mogą być takie informacje, jak np. sprawozdania finansowe przedsiębiorstw, rachunki bankowe czy wyniki badań marketingowych. Zdobywanie i analizowanie informacji o osiągnięciach technicznych, planowanych działaniach i pozycji ekonomicznej podmiotów funkcjonujących na regionalnym i globalnym rynku nazywa się wywiadem gospodarczym. W polskich opracowaniach można spotkać również takie określenia, jak: „wywiad konkurencyjny", „wywiad rynkowy", „wywiad biznesowy" oraz „analiza konkurencyjności". Autorzy często posłu-

gują się oryginalnym, angielskim terminem „*competitive intelligence*”[1], co oznacza, że jest to działalność, której celem jest głównie pozyskiwanie informacji o potencjalnych konkurentach i obszarach ich aktywności biznesowej. Niniejszy artykuł jest pisany z perspektywy przedsiębiorstw i potrzeb ochrony ich własnych informacji biznesowych.

Wywiad gospodarczy – źródła pozyskiwania informacji

Początki wywiadu rozumianego jako pozyskiwanie informacji o kluczowym znaczeniu, można odnaleźć już w odległej przeszłości. Autorzy literatury przedmiotu często wskazują na czasy starożytne i na takie postacie, jak np. Mojżesz, Konfucjusz czy Sun -Tzi[2] (wspominają o nich np. L. Korzeniowski i A. Pepłoński[3] oraz E. Cilecki[4]). Istotne znaczenie dla wywiadu gospodarczego mają też źródła informacji. Autorzy publikacji charakteryzują je w różny sposób, np. jako źródła wewnętrzne i zewnętrzne, źródła formalne i nieformalne[5], źródła pierwotne i wtórne[6].

Źródła zewnętrzne są potrzebne szczególnie małym i średnim przedsiębiorstwom, gdyż ocenia się, że (...) *w dużych przedsiębiorstwach 80 proc. potrzebnych informacji znajduje się na miejscu, a poszukiwania na zewnątrz obejmują tylko pozostałe 20 proc*.[7] Źródłem informacji mogą być m.in. podwykonawcy, pracownicy konkurencji, dostawcy usług czy stażyści. Ponadto takie wydarzenia, jak np. kongresy, targi, szkolenia, spotkania okolicznościowe – organizowane głównie z myślą o ułatwieniu ich uczestnikom wymiany informacji – są także doskonałym miejscem zdobywania nowej wiedzy. W tej grupie źródeł zewnętrznych mogą znajdować się tzw. wewnętrzne źródła informacji. Jak podają B. Martinet i Y.M. Marti[8], przeprowadzone badania dowiodły, że z tych właśnie źródeł pochodzi trzy czwarte informacji mających wartość gospodarczą. W dobie rozwoju nowych technologii oraz powszechnego dostępu do informacji wywiadownie gospodarcze zdobywają znaczną część wiedzy ze źródeł ogólnodostępnych (ten rodzaj źródeł nie jest wcześniej wymieniony). Jej uzyskanie nie wymaga zastosowania skomplikowanych metod, ponieważ są to informacje umieszczane w internecie, prasie, książkach, oficjalnych publikacjach różnych instytucji oraz w dostępnych bazach danych itp. Wielu pracowników różnych firm ujawnia informacje służbowe na forach internetowych, portalach społecznościowych, ułatwiając tym samym pracę wywiadowniom. Nie wszystkie jednak informacje, które mają wartość dla przedsiębiorcy, są ogólnie dostępne, dlatego wywiadownie w celu ich zdobycia często wykorzystują powiązania personalne. Metoda dotarcia do informacji bazuje na kontaktach międzyludzkich. Według T. Aleksandrowicza cechą wyróżniającą tę grupę źródeł jest to, że dostęp do nich wymaga poniesienia określonych nakładów, np. w postaci uzyskania praw dostępu do określonych baz danych[9].

---

[1] A. Moryś, *Geneza i ewolucja wywiadu gospodarczego,* cz. 2, Kielce 2011–2014, http://www.ujk.edu.pl.

[2] C.S. Fleischer, D.L. Blenkhorn, „ *Managing Frontiers in Competitive Intelligence*, Westport 2001, s. 3–4.

[3] L. Korzeniowski, A. Pepłoński, *Wywiad gospodarczy: historia i współczesność*, Kraków 2005, s. 12–13.

[4] E. Cilecki, *Penetracja rynków zagranicznych: wywiad gospodarczy*, Warszawa 1997, s. 76.

[5] Zob. B. Martinet, Y.M. Marti, *Wywiad gospodarczy: pozyskiwanie i ochrona informacji*, Warszawa 1999, s. 41–49; M. Kaliski, P. Mrozik, *Tworzenie efektywnego systemu wywiadu gospodarczego*, w: *Informacja w zarządzaniu przedsiębiorstwem. Pozyskiwanie, wykorzystanie i ochrona*, R. Borowiecki, M. Kwieciński (red.), Kraków 2003, s. 381–382.

[6] E. Cilecki, *Penetracja rynków…*, s.18.

[7] B. Martinet, Y.M. Marti, *Wywiad gospodarczy…*, s. 50.

[8] Tamże, s. 41.

[9] Zob. T. Aleksandrowicz, *Analiza informacji w administracji i biznesie*, Warszawa 1999.

Wywiad legalny czy nielegalny?

Wywiad jest przedsięwzięciem legalnym, jeżeli działa w granicach prawa i na zasadach określonych przez unormowania prawne. Bardzo często zdarza się jednak, że osoby realizujące zlecenie przeprowadzenia wywiadu gospodarczego wykorzystują źródła w sposób bezprawny i sięgają po nielegalne metody, np. podsłuch, podgląd, wnikanie w cyberprzestrzeń bądź pozyskiwanie osobowych źródeł informacji. Osobowe źródła informacji są rekrutowane spośród byłych pracowników przedsiębiorstwa konkurencyjnego lub nowo przyjmowanych, przy założeniu, że stanowią oni najłatwiejszy cel. Nierzadko stosuje się bardziej wyrafinowaną praktykę, jaką jest zatrudnienie swojego pracownika w rozpracowywanym przedsiębiorstwie. Niekiedy próbuje się również pozyskać osobowe źródła informacji wywodzące się ze sfrustrowanych pracowników konkurencyjnej firmy, niezadowolnych z wysokości zarobków, braku perspektyw awansu czy panujących stosunków międzyludzkich w miejscu ich pracy. W typowaniu kandydatów na informatorów uwzględnia się ich aktualny status majątkowy, nałogi i cechy charakterologiczne.

Nielegalny wywiad gospodarczy stwarza szczególne i coraz powszechniejsze zagrożenie dla funkcjonowania przedsiębiorstw, nie tylko w Polsce, lecz także na świecie. Nie można bowiem wykluczyć, że przynajmniej część wywiadowni gospodarczych realizuje działania, które można określić jako szpiegostwo przemysłowe. I chociaż ten rodzaj aktywności nie jest przedmiotem tego opracowania, to należy zauważyć, że zjawisko to występuje prawie we wszystkich dziedzinach gospodarki i nie ogranicza się jedynie do firm wdrażających zaawansowane technologie. Dotyczy praktycznie każdej działalności, która zapewnia osiągnięcie wymiernych korzyści ekonomicznych. Dawno już minęły czasy, gdy szpieg potrzebował dotrzeć do dokumentu, aby go wykraść, skopiować lub sfotografować. Nowoczesna technologia umożliwia globalny dostęp do zasobów informacji przetwarzanych chociażby przez systemy informatyczne. Bardzo często zdarza się, że przedsiębiorstwa nie zdają sobie sprawy, że już padły ofiarą szpiegostwa przemysłowego. Dotyczy to zwłaszcza dużych koncernów przetwarzających strategiczne informacje, chronione na podstawie przepisów prawa, np. informacje niejawne, których ujawnienie mogłoby spowodować szkody dla ważnych interesów państwa (w 2013 r. w Stanach Zjednoczonych 3 tys. organizacji otrzymało od rządu oficjalne powiadomienie o ataku hakerskim[10]). Przedsiębiorstwa powinny współpracować w tym zakresie z odpowiednimi organami, których zadaniem jest przeciwdziałanie szpiegostwu przemysłowemu, zwłaszcza jeśli jest ono dokonywane przez służby specjalne innych państw.

Według FBI Rosja i Chiny regularnie od lat zajmują się wykradaniem tajemnic ekonomicznych i technologicznych w przedsiębiorstwach – szczególnie przez ich aktywną działalność w cyberprzestrzeni. Fakt agresywnego pozyskiwania informacji gospodarczych przez Chiny potwierdza Monika Wasiewicz[11], przedstawiciel FBI w Polsce, która od lat współpracuje z przedsiębiorstwami w Stanach Zjednoczonych i Polsce w zakresie przeciwdziałania szpiegostwu gospodarczemu. Straty poniesione przez go-

[10] Zob. Raport: *The economic impact of cybercrime and cyber espionage*, Center for Strategic and International Studies, (CSIS), McAfee, Intel Security, 2013 [online], http://csis.org/event/2014-mcafee-report-global-cost-cybercrime.

[11] Zob. wywiad z M. Wasiewicz *Chiny i Rosja hakują tajne dane rządowe i biznesowe USA*, przeprowadzony podczas IV Konferencji Bezpieczeństwa Narodowego zorganizowanej przez Krajowe Stowarzyszenie Ochrony Informacji Niejawnych oraz Stowarzyszenie Wspierania Bezpieczeństwa Narodowego w dniach 8–10 X 2014 r. w Spale, Ewa Chyra Polskie Radio.

spodarkę amerykańską z tytułu szpiegostwa gospodarczego w 2011 r. wyniosły łącznie ponad 13 mld dolarów. W kolejnym, 2012 r., straty te zamknęły się już kwotą 19 mld dolarów[12]. Okazuje się zatem, że pomimo działań podejmowanych przez służby specjalne Stanów Zjednoczonych, proceder ten nie ulega zmniejszeniu, lecz wręcz przeciwnie, w ciągu dwóch lat zwiększył się on blisko o 50 proc.

Niepokojąca w tym kontekście jest także wypowiedź Steve'a Durbina, wiceprezesa Forum Bezpieczeństwa Informacji, który zauważył, że (...) *wspierane przez państwo cyberszpiegostwo nie jest już ograniczone tylko i wyłącznie do Chin czy Korei Północnej, w pełnym zakresie zajmują się nim także państwa demokratyczne*[13]. W tej sytuacji z dużą dozą prawdopodobieństwa, graniczącą z pewnością, można stwierdzić, że i polskie przedsiębiorstwa są narażone na takie działania. Według Symantec[14] w Polsce od 2011 r. działa grupa hakerów o nazwie „Dragonfly", która dokonuje ataków szpiegowskich na firmy z sektora energetycznego w różnych krajach na świecie[15]. Na przykład w 2011 r. straty poniesione w wyniku cyberprzestępczości szacowano w USA na 1,52 mld dolarów[16], a w skali globu wyniosły one 221 mld dolarów[17]. W 2013 r. straty związane z cyberprzestępczością szacowano już w świecie na 445 mld dolarów[18]. Przedstawione dane dowodzą, jak duży wpływ na gospodarkę, w tym na działalność przedsiębiorstw, mają tego rodzaju zagrożenia. Według szacunków zawartych w raporcie Center for Strategic and International Studies (CSIS) globalne straty związane z cyberszpiegostwem okazują się niższe od podanych powyżej, ale i tak zawierają się w przedziale od 70 do 140 mld dolarów[19].

Przedmiotem zainteresowania wywiadu gospodarczego są w dużej części tajemnice przedsiębiorstwa dotyczące nowych technologii, produkcji, patentów, praw własności, znaków towarowych i tajemnicy handlowej (tzw. *know-how*). Tajemnica przedsiębiorstwa została zdefiniowana w art. 11 *Ustawy z 16 kwietnia 1993 r. o zwalczaniu nieuczciwej konkurencji*[20] jako (...) *nieujawnione do wiadomości publicznej informacje techniczne, technologiczne, organizacyjne przedsiębiorstwa lub inne informacje posiadające wartość gospodarczą, co do których przedsiębiorca podjął niezbędne działania w celu zachowania ich poufności*. Pozyskanie tajemnicy przedsiębiorstwa w sposób nieuprawniony, w myśl art. 3 tej ustawy, stanowi czyn nieuczciwej konkurencji, czyli działanie sprzeczne z prawem lub dobrymi obyczajami, jeżeli zagraża interesowi innego przedsiębiorcy lub klienta lub go narusza. Oznacza to, że zdobywanie informacji dotyczących np. produkcji prowadzonej przez konkurencyjny podmiot jest czynem nieuczciwej konkurencji. Polskie prawodawstwo nie reguluje działalności wywiadu gospodarczego, dlatego nie ma aktu prawnego, który określałby, jakiego rodzaju informacje mogą być pozyskiwane w ramach takiego wywiadu. Należy zatem przyjąć, że są to informacje, których pozyskiwania nie zabrania prawo powszechnie obowią-

[12] http://www.fbi.gov.

[13] *Top 10 zagrożeń bezpieczeństwa informacji do 2016 roku*, Computerworld Online/DP, 28 V 2014 r. [online], http://www.computerworld.pl [dostęp: 13 V 2015].

[14] Symantec Corporation – międzynarodowe przedsiębiorstwo sprzedające oprogramowanie komputerowe, koncentrujące się na dziedzinie bezpieczeństwa danych i zarządzania informacjami, za: https://pl.wikipedia.org/wiki/Symantec (przyp. red.).

[15] www.symantec.pl

[16] *Identity Theft Cost Americans $1.52B in 2011*, Reuters 2012 [online], www.huffingtonpost.com.

[17] *How much does identity theft cost?* [online], www.mashable.com [dostęp: 20 XII 2014].

[18] *The economic impact…*

[19] Tamże, s. 16.

[20] Tekst jednolity: Dz.U. z 2003 r. Nr 153, poz. 1503, z późn. zm.

zujące. Wywiad gospodarczy jest coraz powszechniejszym działaniem realizowanym przez polskich przedsiębiorców, dlatego dziedzina ta wymaga uregulowania w drodze legislacyjnej. Prawo powinno określać, jakie działania są dozwolone w ramach prowadzonego wywiadu gospodarczego, a jakie stanowią czyn nieuczciwej konkurencji lub są już szpiegostwem gospodarczym.

Polskie przepisy prawne dokładnie regulują, w jaki sposób oraz kto może uzyskać dostęp do określonych rodzajów informacji, np. do danych osobowych, informacji niejawnych, tajemnicy bankowej. Zbieranie informacji o pracownikach konkretnego przedsiębiorstwa musi odbywać się zgodnie z przepisami prawa. Oznacza to, że dostęp do takich informacji mają określone podmioty, takie jak: organy ścigania i sądowe oraz służby specjalne a także niektóre organy administracji publicznej. Również Kodeks pracy w art. 22 zawiera zamknięty katalog informacji, których pracodawca, i tylko pracodawca, może żądać od pracownika.

Przykładem innych informacji, do których dostęp regulują przepisy prawa, są:

- informacje o zadłużeniach w urzędzie skarbowym – art. 298 i 299 *Ustawy z dnia 29 sierpnia 1997 r. – Ordynacja podatkowa*[21], art. 15 *Ustawy z dnia 13 października 1998 r. o systemie ubezpieczeń społecznych*[22],
- połączenia telefoniczne – art. 80 ust. 1 i art. 179 ust. 3 *Ustawy z dnia 16 lipca 2004 r. – Prawo telekomunikacyjne*[23],
- zadłużenia w ZUS – art. 50 *Ustawy z dnia 13 października 1998 r. o systemie ubezpieczeń społecznych*.

Istnieją także informacje, których pozyskiwanie wymaga przedstawienia interesu prawnego. Należą do nich m.in. dane z centralnej ewidencji pojazdów i centralnej ewidencji kierowców (art. 100c i art. 80c *Ustawy dnia 20 czerwca 1997 r. – Prawo o ruchu drogowym*[24]), informacje z ewidencji gruntów i budynków (art. 24 ust. 5 *Ustawy z dnia 17 maja 1989 r. – Prawo geodezyjne i kartograficzne*[25]).

Dotyczy to także rejestrów dłużników prowadzonych przez biura informacji gospodarczej, określonych na podstawie *Ustawy z dnia 9 kwietnia 2010 r. o udostępnianiu informacji gospodarczych i wymianie danych gospodarczych*[26]. Zgodnie z art. 26. ust. 2 tej ustawy *Podmiot, który otrzymał od biura informacje gospodarcze dotyczące dłużnika będącego konsumentem, nie może ich ujawnić innym osobom*. Nieuprawnione pozyskiwanie informacji może skutkować sankcjami karnymi oraz finansowymi nie tylko dla podmiotu realizującego taką usługę, lecz także dla zlecającego jej wykonanie.

Przeciwdziałanie utracie informacji

Informacja jest zasobem łatwym do wytworzenia i rozpowszechniania, lecz trudnym do ochrony i kontroli. Nigdy nie można mieć pewności, że tajemnice są całkowicie chronione, można jednak podjąć działania, aby ryzyko ich utraty znacznie zminimalizować. Wdrożenie systemu bezpieczeństwa w przedsiębiorstwie wiąże się z wprowadzeniem ograniczeń w poszczególnych obszarach jego działalności, co może wydłużyć

[21] Tekst jednolity Dz.U. z 2015 r. poz. 613.
[22] Tekst jednolity Dz.U. z 2015 r. poz. 121, z późn. zm.
[23] Tekst jednolity Dz.U. z 2014 r. poz. 243, z późn. zm.
[24] Tekst jednolity Dz.U. z 2012 r. poz. 1137, z późn. zm.
[25] Tekst jednolity Dz.U. z 2015 r. poz. 520.
[26] Tekst jednolity Dz.U. z 2014 r. poz. 1015, z późn. zm.

czas pracy niezbędny do osiągnięcia zamierzonych wyników. Brak odpowiedniej ochrony oraz nieprzestrzeganie wewnętrznych procedur dotyczących bezpieczeństwa mogą jednak mieć nieodwracalne, negatywne dla przedsiębiorstwa skutki. Ponemon Institute LLC przeprowadził badanie na temat kosztów związanych z utratą informacji, które ponoszą przedsiębiorstwa[27]. Badanie przeprowadzono w dziewięciu państwach, w których dokonano analizy kosztów dotyczących naruszenia bezpieczeństwa i utraty informacji. Największe straty w wyniku wycieku informacji poniosły Niemcy i Stany Zjednoczone, odpowiednio: 199 dolarów i 188 dolarów za rekord baz danych. Łącznie Stany Zjednoczone poniosły 5,4 mld dolarów strat, a Niemcy 4,8 mld dolarów. Najmniejsze koszty poniesiono w Brazylii i Indiach (odpowiednio: 58 dolarów i 42 dolary za rekord). Brazylia poniosła straty w wysokości 1,3 mld dolarów, a Indie 1,1 mld dolarów. Przedstawione statystyki pokazują, jak wielkie straty ponosi gospodarka narodowa w wyniku utraty informacji przez przedsiębiorstwa. Dlatego tak ważne są działania wyprzedzające podejmowane przez przedsiębiorstwa, a związane z wdrażaniem zabezpieczeń w celu ochrony zasobów informacyjnych. System bezpieczeństwa musi być dostosowany do specyfiki konkretnego podmiotu. Powinien przy tym uwzględniać wszelkie aspekty zabezpieczenia i ochrony informacji związane z przeciwdziałaniem utracie informacji spowodowanej zarówno przez aktywność obcych służb specjalnych, wywiadowni gospodarczych, a także w sposób nieumyślny zawinione działania pracowników oraz przez nieprzewidziane oddziaływanie czynników pozaludzkich (tzn. takich zdarzeń losowych jak pożar czy powódź).

System bezpieczeństwa informacji wymaga spełnienia co najmniej trzech warunków, aby można było mówić o jego skuteczności, którymi są:

- wysoka świadomość pracowników, poczynając od najwyższego kierownictwa,
- efektywne zarządzanie informacjami w taki sposób, aby zapewnić ich bezpieczeństwo,
- stworzenie odpowiednich rozwiązań technologicznych, które zapewniają realizację polityki bezpieczeństwa informacji.

W związku z powyższym kierownictwo spółek powinno kompleksowo zarządzać zasobami informacyjnymi, a wdrożony w przedsiębiorstwie system bezpieczeństwa musi zapewnić ich efektywną ochronę i obronę przed szpiegostwem, cyberatakami i przestępczością komputerową. Zarządzanie zasobami informacyjnymi należy rozumieć jako określony zestaw sposobów postępowania dotyczących tego, jak przedsiębiorstwo zdobywa, dystrybuuje i używa informacji oraz wiedzy. System bezpieczeństwa musi uwzględniać przede wszystkim kontrolę pozyskiwania, wytwarzania i przetwarzania informacji, ich bezpieczną dystrybucję oraz monitorowanie „ścieżki" obiegu informacji w strukturze danego przedsiębiorstwa. Zarządy spółek powinny przeprowadzać okresowe analizy ryzyka utraty informacji oraz sporządzać plany postępowania z tym ryzykiem. Działania, które trzeba podjąć, to rozpoznanie i natychmiastowe reagowanie na pojawiające się zagrożenia. Bardzo ważne jest też określenie i zidentyfikowanie, jakiego rodzaju informacje mają podlegać szczególnej ochronie, z czym wiąże się ograniczenie do nich dostępu. Oznacza to konieczność opracowania listy dokumentów, które wymagają ochrony w przedsiębiorstwie. Każdy pracownik powinien wiedzieć, które zasoby informacyjne i jak należy chronić. Przedsiębiorca powinien wprowadzić zasady organizacyjne dotyczące oznaczania, udostępniania, publikowania, kopiowania i niszczenia informacji, które są jego własnością. Główną rolę odgrywają również procedury

[27] Ponemon Institute LLC, Cost of Data Breach Study: Global Analysis Benchmark research sponsored by Symantec Independently Conducted by Ponemon Institute LLC, USA, 2013.

kadrowe podczas weryfikacji i rekrutacji pracowników identyfikujące wewnętrzne zagrożenia, których źródłem może być np. niezadowolony pracownik. Polskie przepisy prawa, w tym i kodeks pracy, jasno precyzują, jakiego rodzaju informacji może zażądać pracodawca od pracownika. Oznacza to, że pracodawca ma, niestety, ograniczone możliwości dotarcia do informacji o przyszłym pracowniku podczas procesu rekrutacji. Nie może np. żądać od kandydata do pracy (tak samo jak i od pracownika) oświadczenia o niekaralności, chyba, że przepisy szczególne na to pozwalają.

Zarządy spółek powinny zatwierdzić i wdrożyć własną strategię działań ochronnych i opublikować ją pod nazwą *Polityka bezpieczeństwa informacji*. Jest to zbiór zasad i procedur dotyczących ochrony i zabezpieczenia informacji, w którym powinny być uwzględnione cele, sposoby i środki ochrony informacji.

Oprócz podjęcia środków ochrony o charakterze organizacyjnym istotne są zabezpieczenia techniczne i fizyczne. W systemie bezpieczeństwa w przedsiębiorstwie musi zostać uwzględniona ochrona systemu teleinformatycznego, uzależnienie od skomputeryzowanych systemów wszystkich aspektów działalności przedsiębiorstw zwiększa bowiem ryzyko utraty cennych informacji. Przedsiębiorstwa, opracowując system bezpieczeństwa, mogą posiłkować się „dobrymi praktykami" zawartymi w normie ISO/IEC 27001:2013, która umożliwia zarządzanie bezpieczeństwem informacji w sposób całościowy i usystematyzowany. Wskazana norma dotyczy całości funkcjonowania przedsiębiorstwa, ponieważ uwzględnia jego strukturę organizacyjną, politykę działania, zakres odpowiedzialności, praktyki, procedury, procesy i zasoby. Norma ta szczegółowo opisuje także wymaganą dokumentację i sposób jej prowadzenia. ISO/IEC 27001 jest normą zawierającą model systemu zarządzania bezpieczeństwem informacji, który może być zastosowany przez każdą organizację, niezależnie od specyfiki jej działalności, wielkości, realizowanych procesów, statusu prawnego i struktury organizacyjnej. Norma pozwala na ustanowienie, wprowadzenie, eksploatowanie, monitorowanie, przegląd i doskonalenie systemu. Wdrożenie systemu bezpieczeństwa informacji w przedsiębiorstwie musi uwzględniać przepisy szczególne które przedsiębiorstwa – z uwagi na prowadzoną działalność – są zobowiązane przestrzegać. Przykładem mogą być przedsiębiorstwa energetyczne, które oprócz zastosowania się do przepisów dotyczących bezpieczeństwa informacji, takich jak np. *Ustawa z dnia 29 sierpnia 1997 r. o ochronie danych osobowych*[28] czy *Ustawa z dnia 16 kwietnia 1993 r. o zwalczaniu nieuczciwej konkurencji*[29], są zobligowane do przestrzegania przepisów dotyczących bezpieczeństwa informacji określonych w *Ustawie z dnia 10 kwietnia 1997 r. – Prawo energetyczne*[30]. Wprowadzenie systemu zarządzania bezpieczeństwem informacji powinno być postrzegane w przedsiębiorstwie jako decyzja strategiczna i powinny wypływać z potrzeb biznesowych.

Podsumowanie

Przedsiębiorcy niechętnie planują środki budżetowe na modernizację i rozbudowę systemów bezpieczeństwa. Przyczyną tego rodzaju postawy może być problem z prawidłowym oszacowaniem korzyści, jakie niosą z sobą tego typu inwestycje. Uwzględniając obecne uwarunkowania, ochrona przed kradzieżą informacji stała się jeszcze

[28] Tekst jednolity Dz.U. z 2014 r. poz. 1182, z późn. zm.
[29] Dz.U. z 2003 r. Nr 153, poz. 1503, z późn. zm.
[30] Tekst jednolity Dz.U. z 2012 r. poz. 1059, z późn. zm.

trudniejsza, niż miało to miejsce w przeszłości. Stosowanie kompleksowych strategii ochrony własnych zasobów informacyjnych może zwiększyć koszty prowadzenia działalności, jednak ryzyko utraty informacji na rzecz konkurencji wiąże się z nieporównywalnie większymi kosztami i stratami. Właściwa ochrona opisywanych zasobów ma istotne znaczenie dla sprostania wymaganiom prawnym i wywiązania się z biznesowych zobowiązań. Zarządy spółek muszą mieć świadomość znaczenia informacji, które są realnym wsparciem dla prowadzenia działalności gospodarczej i budowania silnej, konkurencyjnej marki w danej branży.

Należy pamiętać, że nie tylko jedna strona chce pozyskać informacje ułatwiające jej podejmowanie strategicznych decyzji. Firma konkurencyjna, kierując się pragnieniem uzyskania dostępu do cennych dla niej, lecz zastrzeżonych przez pierwszą firmę informacji, może sięgnąć po metody nielegalne, ze szpiegostwem gospodarczym włącznie. Przedsiębiorstwa, które zbyt lekkomyślnie kierują się zasadami otwartości, ignorując przestrzeganie zasad bezpieczeństwa w obiegu informacji chronionych, mogą narazić się na istotne, niepowetowane straty.

Bibliografia:

Aleksandrowicz T., *Analiza informacji w administracji i biznesie*, Warszawa 1999, Wyższa Szkoła Handlu i Prawa.

Analiza konkurencyjności, w: Wikipedia, http://pl.wikipedia.org/wiki/.

Ciecierski M., *Wywiad biznesowy w korporacjach transnarodowych: teoria i praktyka*, Toruń 2009, Adam Marszałek.

Ciecierski M., *Wywiad gospodarczy (rynkowy) – wybrane aspekty*, „Wiek XXI" 2003, nr 3.

Cilecki E., *Penetracja rynków zagranicznych: wywiad gospodarczy*, Warszawa 1997, PWSzBiA.

Cilecki E., *Penetracja rynku a metody uzyskiwania informacji gospodarczych ze źródeł zagranicznych*, w: *System informacji strategicznej*, R. Borowiecki, M. Romanowska (red.), Warszawa 2001, Difin.

Fleischer C.S., Blenkhorn D.L., *Managing Frontiers in Competitive Intelligence*, Westport 2001, Conn.

http://www.paulo.pl/pulapki.html.

Identity Theft Cost Americans $1.52B in 2011 [online], Reuters 2012, 28 February 2012, www.huffingtonpost.com.

Kaliski M., Mrozik P., *Tworzenie efektywnego systemu wywiadu gospodarczego*, w: *Informacja w zarządzaniu przedsiębiorstwem: pozyskiwanie, wykorzystanie i ochrona. Wybrane problemy teorii i praktyki*, R. Borowiecki, M. Kwieciński (red.), Kraków 2003.

Korzeniowski L., Pepłoński A., *Wywiad gospodarczy: historia i współczesność*, Kraków 2005, EAS.

Martinet B., Marti Y.M., *Wywiad gospodarczy: pozyskiwanie i ochrona informacji*, Warszawa 1999, Polskie Wydawnictwo Ekonomiczne.

Mashable, Jolie O'Dell, *How much does identity theft cost?*, 28 January 2011, www.mashable.com.

Surma, J., *Business Intelligence. Systemy wspomagania decyzji biznesowych*, Warszawa 2009, Wydawnictwo Naukowe PWN.

Szczepanik R., Krzyżowska O., *Nietypowe przypadki Public Relations*, Gliwice 2003, Onepress.

Abstrakt

Artykuł opisuje działania podejmowane przez przedsiębiorstwa w celu ochrony zasobów informacyjnych przed zagrożeniem związanym z nielegalnym wywiadem gospodarczym. Autorka podkreśla wagę i znaczenie informacji, która jest zasobem łatwym do wytworzenia i rozpowszechniania, lecz trudnym do ochrony i kontroli. Nigdy nie można mieć pewności, że tajemnice są skutecznie chronione, można jednak podjąć działania, aby ryzyko utraty informacji znacznie zminimalizować. W artykule wskazano dobre praktyki oraz standardy, które służą zarządzaniu i doskonaleniu systemu bezpieczeństwem informacji w przedsiębiorstwie. Ponadto wyjaśniono pojęcie „wywiadu gospodarczego" oraz opisano początki jego funkcjonowania. Wskazano przykładowe metody działań podmiotów zajmujących się pozyskiwaniem zasobów informacyjnych oraz określono rodzaje informacji, które mogą być przedmiotem zainteresowania wywiadowni gospodarczych. Podjęto także próbę wyznaczenia granicy pomiędzy legalnym a nielegalnym wywiadem gospodarczym. Jak podkreśla autorka nierzadko zdarza się, że osoby realizujące zlecenie przeprowadzenia wywiadu gospodarczego sięgają po nielegalne metody. Przed takimi działaniami powinny zabezpieczać się przedsiębiorstwa.

Słowa kluczowe: wywiad gospodarczy, przedsiębiorstwo, informacja, bezpieczestwo, zarządzanie.

Abstract

The article describes actions taken by enterprises to protect information resources against the risks associated with illegal business intelligence. The author emphasizes the importance of information, which is an easy resource to produce and distribute, but difficult to protect and control. You can never be sure that the secrets are effectively protected, but you can take steps to significantly minimize the risk of losing information. The author identifies good practices and standards, which are used to manage and improve information security system in the enterprise. The article explains the concept of business intelligence and describes the beginnings of its operation. It indicates exemplary methods of operation of entities dealing with the acquisition of information resources and defines the types of information that may be of interest for the business intelligence agency. An attempt is made to draw the line between legal and illegal business intelligence. As pointed out by the author, it often happens that individuals carrying out the order of conducting business intelligence resort to illegal methods. Enterprises should protect themselves against such actions.

Keywords: business intelligence, enterprise, information, security, management.