AUTOR
mgr inż. Piotr Błasiak
blasiakpiotr@interia.pl
Wydział Zarządzania, Politechnika Częstochowska

PRZEDSIĘBIORSTWO W RZECZYWISTOŚCI WIRTUALNEJ, A OCHRONA JEGO DANYCH WRAŻLIWYCH

Słowa klucz: bezpieczeństwo, bezpieczeństwo informacyjne, cyberbezpieczeństwo, cyberrzeczywistość, dane osobowe, dane wrażliwe

Wstęp

Współczesna działalność przedsiębiorstwa wiąże się w znacznej mierze z koniecznością podejmowania istotnych decyzji. Nie byłoby to jednak możliwe, gdyby nie odpowiednie zarządzanie dostępną informacją. Obecnie można ją już utożsamiać z nowym zasobem, jaki trzeba umieć pozyskiwać, a także wykorzystywać w wymiarze praktycznym. W tym też celu należy istotne informacje również chronić, ponieważ mogą one warunkować powodzenie prowadzonego działania. Stąd też coraz nowsze rozwiązania dla przedsiębiorców odnoszą się w znacznej mierze do tego, by chronić kluczowe dane, ponieważ te nierzadko są źródłem przewagi konkurencyjnej, co w konsekwencji powoduje, że posiadane informacje stają się coraz częściej powodem napaści. Tym bardziej, iż specyfika rzeczywistości wirtualnej daje ku temu coraz więcej możliwości.

Społeczeństwo wirtualne i informacja

Rzeczywistość wirtualna, w której funkcjonuje przedsiębiorstwo, jest elementem społeczeństwa wirtualnego. *Stanowi ono odbicie realnego społeczeństwa, jednak część zadań jest wykorzystywana poprzez Internet*. […] *W takim też środowisku muszą również funkcjonować sami przedsiębiorcy. Jednak z określoną ofertą musi ono dojść przy wykorzystaniu rozwiązań teleinformatycznych*[1].

[1] M. Kowalski (red.), *Internet, między edukacją, bezpieczeństwem, a zdrowiem*, Maternus Media, Kraków, 2008, s. 142-145,153.

Informacja w przypadku społeczeństwa informacyjnego to potężne źródło danych, w których skład wchodzą miedzy innymi dane osobowe zwykłe i te o charakterze wrażliwym. Stanowią, więc cenny łup, dla którego warto się narażać. Trzeba tutaj jednak wyraźnie podkreślić, że problem ten stał się poważny w momencie udostępnienia Internetu, w sposób natychmiastowy przekazującego istotne informacje.

W przeszłości problem z informacjami gromadzonymi w przedsiębiorstwie zawężał się do obszaru samego przedsiębiorstwa. Obecnie jest on znacznie szerszy, a w zasadnie jego granice są zdefiniowane, jako cały system informacyjny w skład, którego wchodzi system informatyczny danego przedsiębiorstwa. Jeśli ten system w bezpośredni sposób jest powiązany z siecią globalną, to zostaje rozszerzony do niej samej.

W związku z powyższym problemy z informacją i jej bezpieczeństwem możemy rozpatrywać na bardzo wielu płaszczyznach, począwszy od kwestii technicznych czy technologicznych, a skończywszy na kwestiach prawnych, a także moralnych. Do niedawna zadawano sobie pytanie, jak gromadzić dane powiązane w informacje, aby posiąść maksymalną ilość wiedzy a co za tym idzie ile miejsca zbiory te zajmą. Biorąc pod uwagę obecny rozwój techniki, możemy już zgromadzić praktycznie każdą ilość informacji i nie muszą się one ograniczać wyłącznie do danych liczbowych. Obecnie możemy gromadzić także inne rodzaje informacji a następnie rozpatrywać je w znacznie szerszym kontekście.

Szeroki konspekt rozpatrywania informacji jest możliwy między innymi dzięki praktycznie nieograniczonym mocom obliczeniowym współczesnych komputerów, a proces gromadzenia informacji w coraz większej mierze dokonywany jest automatycznie. Jeśli mamy na myśli informacje gromadzone w przedsiębiorstwach globalnych, które dysponują dostępem do najnowszych rozwiązany technologicznych, informacja może być gromadzona za pomocom maszyn. *Te coraz częściej posiadają zdolność uczenia się i niezależnego wyciągania wniosków*[2]. Właściwie dla każdego współczesnego przedsiębiorstwa, chcącego się rozwijać, informacje są zasobem kluczowym. W tym kontekście można też stwierdzić, że jest to zasób wystawiony na liczne niebezpieczeństwa. Tym bardziej, iż zagrożenia pochodzą zarówno z wnętrza przedsiębiorstwa, jak i ze środowiska go otaczającego.

W związku z przytoczonymi wcześniej faktami *należy wyróżnić następujące fazy, a także problemy związane z informacją*[3]:

- *przetwarzanie informacji,*
- *przesyłanie danych,*

[2] R. Golat, *Internet – aspekty prawne*, Difin, Warszawa, 2003, s. 82.

[3] J. Hofmolk, *Internet jako nowe dobro wspólne*, Wydawnictwo Akademickie i Profesjonalne, Warszawa, 2009, s. 91-92.

- *gromadzenie ich*.

Dążeniem przedsiębiorstw jest jak najbardziej bezproblemowy proces obsługi informacji, który jest realizowany. Jest on możliwy w ramach specyfikacji rzeczywistości wirtualnej. Możemy tutaj wyodrębnić pewien zakres infrastruktur technicznych i technologicznych, w których procesy te zachodzą. I należy je z tego punktu widzenia zabezpieczyć.

Kolejny aspekt, jaki należy brać pod uwagę rozważając kwestie bezpieczeństwa informacji, w tym danych o charakterze wrażliwym, jest związany z problemami natury proceduralnej i prawnej. *Dlatego też wiele przedsiębiorstw, funkcjonujących na rynku, tworzy indywidualne procedury, dające odpowiednie uprawnienia tym osobom, które pracują w oparciu o nie. Ponadto eliminuje się dostęp osób trzecich do posiadanych danych, co mogłoby nastąpić na podstawie możliwości analiz baz danych przez wszystkich zatrudnionych bez względu na zajmowane przez nich stanowisko*[4].

Jeszcze inny aspekt bezpieczeństwa informacji dotyczy kwestii moralnych, związanych z ich gromadzeniem i analizowaniem wielopłaszczyznowo, a następnie wykorzystywaniem. W końcu w tym celu są one gromadzone i analizowane. Przyjmijmy, że dane o charakterze wrażliwym mogą być gromadzone przez system teleinformatyczny. W zakres tych informacji będą wchodziły takie informacje, jak słowa kluczowe, wychwytywane przez mikrofon telefonu komórkowego. Dodatkowo można tutaj wskazać na sytuację, w której gromadzone są informacje na temat sklepów, jakie odwiedzamy i to nie tylko w rzeczywistości wirtualnej, ale i w świecie rzeczywistym. Chodzi tutaj o tzw. pozycjonowanie urządzeń mobilnych. Dla przykładu, jeśli dwójka partnerów zaczyna odwiedzać sklepy z artykułami dla nowonarodzonych dzieci i osoby te rozmawiają o dziecku, to można by wyciągnąć wniosek, że planują potomstwo. Z jednej strony mogą być im serwowane informacje o potencjalnie pożytecznych dla nich produktach i potencjalnie ta informacja jest wykorzystywana z korzyścią dla nich, ale również osób trudniących się ich sprzedażą.

Możemy też w tym przypadku rozważyć inny aspekt sprawy, kiedy zbierane dane dotyczą miedzy innymi osoby pracującej w danej firmie. Firma ta zamierza awansować dla przykładu jednego ze swych pracowników, w celu dobrego dopasowania kandydata, analizuje pozyskiwane dane. Dzięki tym danym firma jest wstanie stworzyć profil osoby najbardziej pożądanej do realizacji celów firmy a następnie porównać je z profilami posiadanej kadry. I wyodrębnić profile osób, mających określone predyspozycje, niezbędne do realizacji celów nadrzędnych. Przypuśćmy, że jedno z naszych wcześniej wspominanych partnerów pasuje idealnie do awansu, ale ze względu na przypuszczalnie planowane „powiększenie

[4] Tamże, s. 93.

rodziny" zostanie zdyskwalifikowane. Ale czy firma podejmując decyzje o odstąpieniu od awansu pomijając kwestie natury prawnej, postąpi w sposób moralny?

Dane osobowe zwykłe i wrażliwe

Przedsiębiorstwo w ramach swych zasobów posiada różne kategorie informacji m.in. gromadzi dane osobowe i dane osobowe wrażliwe. Pojęcia te dla osób, które spotykają się z nimi pierwszy raz, mogą wydawać się niejasne, jednak na podstawie *Ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych* (Dz. U. z 1997 r., nr 133, poz. 883)[5], a także dzięki praktyce stosowania ochrony danych osobowych można je precyzyjnie rozdzielić.

Ustawa ta definiuje zwykłe dane osobowe w art. 6 następująco:

1. W rozumieniu ustawy za dane osobowe uważa się wszelkie informacje dotyczące zidentyfikowanej lub możliwej do zidentyfikowania osoby fizycznej.

2. Osobą możliwą do zidentyfikowania jest osoba, której tożsamość można określić bezpośrednio lub pośrednio, w szczególności przez powołanie się na numer identyfikacyjny albo jeden lub kilka specyficznych czynników określających jej cechy fizyczne, fizjologiczne, umysłowe, ekonomiczne, kulturowe lub społeczne.

3. Informacji nie uważa się za umożliwiającą określenie tożsamości osoby, jeżeli wymagałoby to nadmiernych kosztów, czasu lub działań.

Należy wziąć pod uwagę, że identyfikacja osoby fizycznej może odbyć się za pomocą najbardziej podstawowych danych: imienia, nazwiska, adresu zamieszkania lub zameldowania, numeru PESEL, NIP czy numeru telefonu.

Natomiast dane osobowe wrażliwe zostały zdefiniowane w art. 27 tej ustawy w sposób następujący:

1. Zabrania się przetwarzania danych ujawniających pochodzenie rasowe lub etniczne, poglądy polityczne, przekonania religijne lub filozoficzne, przynależność wyznaniową, partyjną lub związkową, jak również danych o stanie zdrowia, kodzie genetycznym, nałogach lub życiu seksualnym oraz danych dotyczących skazań, orzeczeń o ukaraniu i mandatów karnych, a także innych orzeczeń wydanych w postępowaniu sądowym lub administracyjnym[6].

[5] *Ustawa z dnia 29 sierpnia 1997 r. o ochronie danych osobowych*, Dz. U. z 1997 r., nr 133, poz. 883.

[6] Tamże.

Tak ustawodawca w sposób szczegółowy wymienił grupy danych uznane za dane wrażliwe.

Istota bezpieczeństwa

Należy zaznaczyć, że bezpieczeństwo jest stanem niemierzalnym. Co jednak potęguje fakt, iż na jego rzecz wspólnie musi pracować władza państwowa, a także społeczeństwo. W opinii D. Frei *na istotę bezpieczeństwa składa się charakterystyka obiektywnych, ale również subiektywnych aspektów zagrożenia, a zatem to osoba musi samodzielnie stwierdzić, czy w danych okolicznościach będzie ona zagrożona czy też nie*. Dlatego też aspekt ten stanowi element złożony. Ten sam autor podkreśla znaczenie stanu bezpieczeństwa. W takim przypadku mowa o zagrożeniu zewnętrznym, które ma małe prawdopodobieństwo wystąpienia. Dodatkowo jego postrzeganie ma charakter prawidłowy.

Niniejsze opracowanie odnosi się między innymi do bezpieczeństwa w wymiarze technicznym. Na tym polu *pojęcie związane zarówno z bezpieczeństwem samej informacji krążącej między węzłami sieci, jak też bazami danych dostępnych za jej pośrednictwem. Jako środki ochronne zmniejszające ryzyko uzyskania dostępu do informacji przez osoby nieuprawnione stosuje się:*

- *ograniczanie dostępu do serwerowych zasobów systemu przez restrykcyjne egzekwowanie wymagań zgodnych z obowiązującą polityką ochrony danych (filtrowanie, zapory ogniowe - firewalls, ochrona antywirusowa),*
- *identyfikację obiektów (karty elektroniczne, uwierzytelnianie),*
- *odpowiednie kodowanie informacji w sieci za pomocą metod kryptograficznych (algorytmy szyfrujące symetryczne i niesymetryczne, prywatne i publiczne klucze szyfrowe, podpis elektroniczny*.

Dlatego też ta kategoria bezpieczeństwa przekłada się bezpośrednio na dbałość, by umieszczane informacje, które znajdują się chociażby w bazach danych, odpowiednio zabezpieczać. Pozwala to na korzystanie bez obaw z dobrodziejstw techniki, przez co można ułatwiać pracę, łatwiej prowadzić działalność gospodarczą, a także maksymalizować zyski z posiadanych zasobów, itp.

Możemy wyodrębnić następujące grupy czynników wpływających na bezpieczeństwo informacji w sieciach teleinformatycznych. Z punktu widzenia poprawności funkcjonowania sieci komputerowej można zidentyfikować następujące zagrożenia[7]:

[7] K. Liderman, *Bezpieczeństwo informacyjne*, Wydawnictwo Naukowe PWN, Warszawa, 2011, s. 179-180.

1. ***Siły wyższe*** *(np. klęski żywiołowe, katastrofy finansowe, zmiany prawa).*

2. ***Działania przestępcze*** *(**Nieuprawnione i przestępcze działania ludzi**).*

3. ***Błędy personelu*** *obsługującego system komputerowy.*

4. ***Skutki złej organizacji pracy*** *- np. brak jasno sprecyzowanych zakresów odpowiedzialności, nieprzestrzeganie i/lub brak odpowiednich przepisów itd. (zagrożenia związane z błędami ochronie fizycznej, możliwość utraty dostępności, integralności i poufności).*

5. ***Awarie sprzętu i wady oprogramowania (Awarie i uszkodzenia sprzętu oraz wady oprogramowania)***[8]**.**

Administratorzy sieci przeważnie znają wszystkie te zagrożenia, jednakże można spotkać się z różnym ich nazewnictwem. Znamienny jest fakt, że mimo z jednej strony, powszechnej wiedzy na temat możliwości ich wystąpienia, z drugiej - mamy do czynienia z równie powszechną ignorancją personelu, który może w sposób mniej lub bardziej świadomy przyczynić się do ich wystąpienia. W szczególności odnosi się to do punktu 4 – Skutki złej organizacji pracy.

Co prawda współczesne systemy dają wszelkie możliwości zabezpieczenia stacji roboczych (do niedawna mówiło się najczęściej o komputerach klasy PC teraz coraz częściej są to tablety czy smartfony dające praktycznie pełne spektrum możliwości użytkowych). Czyni się to np. za pomocą haseł, czytników linii papilarnych czy nawet systemów inteligentnego rozpoznawania twarzy osoby, której dostęp ma być uprawniony. Niemniej jednak niezmiernie istotne jest także wypracowanie schematów zachowań właściwych, co do obsługi codziennej, jak i w przypadku wystąpienia zjawiska niepożądanego tak, aby nie dochodziło na przykład do przenoszenia oprogramowania złośliwego na inne stacje robocze. Na rynku odnaleźć można wiele systemów bezpieczeństwa, oferujących różny stopień ochrony. Co więcej działania popularyzacji takich rozwiązań prowadzone są już na poziomie kupna samego sprzętu komputerowego, co jest w interesie firm je wytwarzających i sprzedających. Są one oferowane na przykład w formie zapór systemowych oraz programów antywirusowych.

Wskazane powyżej rozwiązania umożliwiają skanowanie systemów oraz autoryzację dostępu do danych. Ale to na administratorze baz ciąży odpowiedzialność za ochronę zgromadzonych tam informacji, gdyż to on podejmuje decyzje, co do formy ochrony oraz w jaki sposób zabezpieczać poszczególne informacje. Podejmowane decyzje nie mogą ograniczać się do zakupu odpowiedniego sprzętu, gdyż na nic zdadzą się nawet najlepsze zabezpieczenia techniczne a nawet regulaminy pracy, jeśli nie będą

[8] M. Wróbel*, Metody zapewniania bezpieczeństwa systemów operacyjnych*, Rozprawa doktorska, Politechnika Gdańska Wydział Elektroniki, Telekomunikacji i Informatyki, Gdańsk, 2010, s. 11-32.

przestrzegane przez pracowników. Z punktu widzenia ochrony danych osobowych zarówno tych zwykły, jak i wrażliwych administrator sieci informatycznej podlega pod administratora danych osobowych i z tego punktu widzenia jego zadaniem jest nadzór nad bezpieczeństwem danych osobowych, które przetwarzane są za pośrednictwem systemów teleinformatycznych np. laptopy, telefony komórkowe, tablety. W hierarchii ochrony danych osobowych podlega on administratorowi danych osobowych jak ABI.

Aspekt norm prawnych oraz obowiązujących przepisów odnoszących się do bezpieczeństwa informacji

Kwestie związane z bezpieczeństwem w świetle polskich norm są regulowane przez Polski Komitet Normalizacyjny. Jednostka ta odpowiada za określanie norm PN (Polska Norma). Z chwilą wstąpienia Polski do Unii Europejskiej w 2004r., normę PN za sprawą rozszerzenia o standardy unijne, zastąpiono PN PN-ENem. Co w praktyce spowodowało, że normy o charakterze techniczny zostały zasadniczo ujednolicone wzajemnie z normami międzynarodowymi, mowa tu o PN-ISO i PN-IEC[9]. By osiągnąć stosowny certyfikat, trzeba zrealizować określone założenia.

Rozpatrując organizację, jako pewną społeczną strukturę organizacyjną, możemy zaryzykować stwierdzenie, że posiada ona świadomość grupową. Kształtowanie tej świadomości powinno kłaść szczególny nacisk na znaczenie bezpieczeństwa i ochrony informacji. Konieczność zapewnienia bezpieczeństwa informacji z kolei musi być nierozłącznym elementem wpisanym w proces realizacji misji i celów danej organizacji, a następnie we wszelkie czynności związane z obsługą klienta.

W procesie realizowania koncepcji zarządzania przedsiębiorstwem z uwzględnieniem zapewnienia wysokiego poziomu bezpieczeństwa informacji, czyli System zarządzania bezpieczeństwem informacji (ang. ***I**nformation **S**ecurity **M**anagement **S**ystem*), należy oprzeć się na 2 podstawowych standardach:

1. ISO/IEC 17799: 2005 – norma stanowiąca zbiór wytycznych, zaleceń, dobrych praktyk w zakresie utworzenia i utrzymania ISMS; definiuje go jako *część całościowego systemu zarządzania, opracowana na podejściu wynikającym z ryzyka biznesowego, odnosząca się do ustanawiania, wdrażania, eksploatacji, monitorowania, utrzymania i doskonalenia bezpieczeństwa informacji*[10].

[9] https://www.nik.gov.pl/o-nik/ [dostęp: 31.03.2016].

[10] http://yadda.icm.edu.pl/yadda/element/bwmeta1.element.baztech-530a21a8-5dbb-445f-8c4c-e86cb0b2410f [dostęp: 08.03.2018].

2. ISO/IEC 27001: 2005 – norma ta zawiera zestaw niezbędnych wymagań, jakim organizacja jest zobligowana sprostać, ubiegając się o certyfikat ISMS.

Zaimplementowanie jej do systemu bezpieczeństwa informacji ma na celu zagwarantowanie jego niezawodności. W swojej konsekwencji ma zapewnić bezpieczeństwo klientom, dostawcom i osobom trzecim oraz innym organizacjom pozostającym w relacjach z podmiotowym przedsiębiorstwem. Wdrożenie owej normy dodatkowo jest informacją zarówno dla otoczenia organizacji, jak i dla pracowników jej samej, mówiącą o świadomej dbałości o zachowanie wysokiej, jakości informacji. Obejmuje ona swoim zakresem strukturę organizacyjną, politykę, zakres odpowiedzialności, zasady, procedury, procesy oraz zasoby.

Ustawy o ochronie informacji niejawnych a tajemnica informacji firmowych oraz tajemnica zawodowa

W trakcie procesów biznesowych pracownicy różnych szczebli organizacji mają dostęp do informacji stanowiących tajemnicę pracodawcy, pracowników lub osób trzecich. Może to stanowić poważne zagrożenie dla pracodawcy, ponieważ poufne wiadomości mogą wyjść na zewnątrz i dotrzeć do niepowołanych osób. Ustawodawca dostrzegając powagę tego zagrożenia, zaklasyfikował przestrzeganie tajemnicy pracodawcy do katalogu podstawowych obowiązków pracowniczych, określonych w art. 100 § 1 pkt 4 Kodeksu pracy. Obowiązek zachowania tajemnicy pracodawcy nie może być zniesiony nawet na mocy zapisów układu zbiorowego czy zapisów w regulaminie pracy, a nawet w umowie o pracę.

Jednakże nie zostało sprecyzowane, czym w szczególności jest tajemnica pracodawcy. W praktyce, zatem przyjmuje się, że tajemnica pracodawcy obejmuje wszystkie informacje niejawne, nieudostępnione przez pracodawcę nie tylko na zewnątrz zakładu, ale także ogółowi pracowników, a których ujawnienie mogłoby narazić go na szkodę. Obowiązek zachowania poufności obciąża każdego podwładnego. Na mocy wskazanych przepisów pracownik musi zachować w tajemnicy wszelkie informacje, których upowszechnienie mogłoby spowodować szkodę dla pracodawcy. Dotyczy to głównie tajemnicy produkcji, organizacji pracy czy informacji handlowych. Tajemnica obowiązuje pracownika gównie w zakresie procesu produkcji, organizacji pracy oraz informacji handlowych. *Jak wynika z orzecznictwa sądowego przedsiębiorca nie musi ponieść faktycznej szkody wystarczy, aby został narażony na jej poniesienie, aby można było stwierdzić naruszenie obowiązku zachowania tajemnicy informacji. Karze może podlegać sam fakt uzyskaniu wiedzy o takich informacjach przez*

nieuprawnionego pracownika lubi inny niezgodny z zamiarem pracodawcy sposób ich wykorzystania[11].

W trakcie procesu zarządzania działaniami w sferze wirtualnej musimy brać pod uwagę czy metody, jakimi jest ono prowadzone, nie naruszają szeregu przepisów prawnych. Do tych przepisów należy także zaliczyć *Ustawę z dnia 18 lipca 2002 r. o świadczeniu usług drogą elektroniczną (Dz. U. z 2002 r., nr 144, poz. 1204),* według której *świadczenie usługi drogą elektroniczną - wykonanie usługi, które następuje przez wysyłanie i odbieranie danych za pomocą systemów teleinformatycznych, na indywidualne żądanie usługobiorcy, bez jednoczesnej obecności stron, przy czym dane te są transmitowane za pośrednictwem sieci publicznych w rozumieniu ustaw*[12].

Ustawa ta określa między innymi obowiązki, jakim musi sprostać usługodawca świadczący wyżej wymienione usługi. Wskazuje się tutaj także na zasady ochrony zgromadzonych danych osób fizycznych, które korzystają z owych usług przez usługodawcę. Dlatego też oba te podmioty współpracują ze sobą, realizują względem siebie określone obowiązki, a wszystko na podstawie odpowiednich umocowań prawnych.

Ustawa ta ponadto precyzuje pojęcia związane z usługami świadczonymi drogą elektroniczną. Znajdują się tam prawne wyjaśnienia pojęć takich jak: adres elektroniczny, informacja handlowa, system teleinformatyczny, świadczenie usług drogą elektroniczną, środki komunikacji elektronicznej, usługodawca, usługobiorca. Ustawa ta nakłada także obowiązek posiadania zgody na wysyłanie informacji handlowych drogą elektroniczną – tj. za pośrednictwem maila lub smsa (art. 10 ust. 2 *ustawy o świadczeniu usług drogą elektroniczną*).

Przedsiębiorca, chcący świadczyć usługi drogą elektroniczną zgodnie z bieżącym stanem prawnym, musi zwrócić także uwagę na przepisy ustawy *Ustawa z 30 maja 2014 r. o prawach konsumenta* (Dz. U. 2014 r., poz. 827), która weszła w życie 25 grudnia 2014 r.

Niewłaściwe przetwarzanie danych osobowych może narazić przedsiębiorców na szereg konsekwencji prawnych. Wpływ na to ma bardzo wiele złożonych czynników, które są od siebie niezależne. Mamy dla przykładu do czynienia z różnego rodzaju formami odpowiedzialności. Polski system prawny stanowi, że osobom niewłaściwie chroniącym dane osobowe, grozi zarówno odpowiedzialność karna, jak i administracyjna, dyscyplinarna oraz cywilna.

[11] http://kadry.infor.pl/kadry/indywidualne_prawo_pracy/odpowiedzialnosc_prawa_i_obowiazki/648424,Jaka-odpowiedzialnosc-wobec-pracodawcy-ponosi-pracownik-ktory-ujawnia-tajemnice-firmy.html [dostęp: 08.10.2017].

[12] *Ustawa z dnia 18 lipca 2002 r. o świadczeniu usług drogą elektroniczną*, Dz. U. z 2002 r., nr 144, poz. 1204.

Organem czuwającym nad bezpieczeństwem danych osobowych jest **Generalny Inspektor Ochrony Danych Osobowych** (w skrócie **GIODO**), który działa na mocy *Ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych*. W tej ustawie zawarte są między innym zasady przetwarzania i zabezpieczenia danych osobowych, a także zasady rejestracji zbiorów danych osobowych oraz administracji bezpieczeństwa informacji. Ochroną objęte są wszelkie dane osobowe zgromadzone w zasobach firmy, także te zgromadzone w zasobach informatycznych, bez względu na to do kogo te dane należą - do pracownika firmy czy też do klienta. Nakłada ona na przykład obowiązek posiadania podstawy do przetwarzania danych osobowych w celach marketingowych (art. 23 *ustawy o ochronie danych osobowych*) i dopełnienia obowiązku informacyjnego (art. 24 lub 25 ustawy o ochronie danych osobowych). Na szczególną uwagę zasługuje fakt odpowiedzialności karnej, będącej konsekwencją nieprzestrzegania wymogów wspomnianego ustawodawstwa:

Art. 49 *ustawy o ochronie danych osobowych*:

1. Kto przetwarza w zbiorze dane osobowe, choć ich przetwarzanie nie jest dopuszczalne, albo do których przetwarzania nie jest uprawniony, podlega grzywnie, karze ograniczenia wolności albo pozbawienia wolności do lat 2.

2. Jeżeli powyższy czyn dotyczy danych ujawniających pochodzenie rasowe lub etniczne, poglądy polityczne, przekonania religijne lub filozoficzne, przynależność wyznaniową, partyjną lub związkową, danych o stanie zdrowia, kodzie genetycznym, nałogach lub życiu seksualnym, sprawca podlega grzywnie, karze ograniczenia wolności albo pozbawienia wolności do lat 3[13].

Punkt 2 przytoczonego artykułu wskazuje ściśle na fakt ochrony elementów będących składowymi kultury globalnej takich jak: pochodzenie rasowe, pochodzenie etniczne, poglądy polityczne, przekonania religijne, przekonania filozoficzne, przynależność wyznaniowa, przynależność, partyjna etc. W procesie świadomego kształtowania kultury organizacyjnej należ zwrócić uwagę czy wewnętrzne normy lub co gorsza procedury nie naruszają praw poszczególnych pracowników w tym zakresie.

Dodatkowo należy zwrócić uwagę na ciągle rosnącą świadomość społeczną własnych praw zarówno w śród pracowników, jak i klientów. Skutkiem wzrostu tej świadomości jest wzrost liczby procesów sądowych związanych z naruszeniem danych osobowych czy danych wrażliwych.

[13] *Obwieszczenie Marszałka Sejmu Rzeczypospolitej Polskiej z dnia 13 czerwca 2016 r. w sprawie ogłoszenia jednolitego tekstu ustawy o ochronie danych osobowych*, Por. Dz. U. z 2016 r., poz. 922.

Zabezpieczenie baz danych

Na rynku odnaleźć można wiele systemów bezpieczeństwa oferujących różny stopień ochrony. Co więcej działania marketingowe prowadzone są już na poziomie kupna samego sprzętu komputerowego. O tego rodzaju działaniach świadczyć mogą choćby zapory systemowe, a także programy antywirusowe, które są preinstalowane na tym sprzęcie*. Ponadto rozwiązania te umożliwiają skanowanie systemów oraz autoryzację dostępu do danych, dlatego to na administratorze baz ciąży odpowiedzialność za ochronę, gdyż to on podejmuje decyzję, co do formy ochrony oraz w jaki sposób zabezpieczać poszczególne informacje*[14].

Dostępne na rynku rozwiązania pozwalają również na halsowanie systemów oraz plików. W wielu przypadkach udostępnia się też czytniki linii papilarnych. Wówczas zamiast hasła stosuje się odcisk palca. Jednak tego rodzaju zabezpieczenie nie jest praktyczne, gdy chodzi o organizację. Wówczas z danych może korzystać tylko jedna osoba, a nie cały zespół, co z kolei blokuje pracę

Do ochrony danych sieciowych oraz baz danych zastosowanie mają systemy szyfrujące. Pozwala to prezentować informacje, ale w sposób nieczytelny. Wyjątek stanowią tutaj osoby, które mają dostęp do danych. Posiadają one stosowne hasło. Takie zabezpieczenie znacznie utrudnia dostęp do informacji w sposób nieautoryzowany. Konieczne staje się posiadanie odpowiedniej wiedzy w zakresie programowania, ponieważ tego rodzaju zabezpieczenie nie jest komercyjne.

Internautów, a tym samym umieszczane przez nich dane, można także chronić w inny sposób. Poniższe rozwiązania są jednak przeznaczone dla administracji oraz podmiotów gospodarczych (tab. 1.).

[14] L. Jason, M. Pepe, K. Mandia, *Incydenty bezpieczeństwa. Metody reagowania w informatyce śledczej*, Wydawnictwo Helion, Gliwice, 2016, s. 74-75.

Tabela 1. Różne formy zabezpieczeń swoich systemów

Lp.	Forma zabezpieczeń	Specyfika	Obszary objęte ochroną
1.	Materialne	Do ochrony stosuje się różnego rodzaju: • programy antywirusowe; • szyfrowanie; • protokoły dostępu; • certyfikaty	• komputery, • bazy, • dostępy do sieci; • systemy operacyjne; • dane klientów
2.	Proceduralne	Określone zostają standardy, które stosuje się w przypadku zagrożenia lub prawdopodobieństwa jego wystąpienia. Dzięki czemu wiadomo jak postępować w takim przypadku lub kto, za co jest odpowiedzialny	
3.	Organizacyjne	Wyznaczenie osób odpowiedzialnych za określone zadania, dzięki czemu np. w firmie zawsze znajduje się osoba odpowiedzialna za podjęcie decyzji i działań, gdyby doszło do zagrożenia atakiem.	

Źródło: opracowanie własne na podstawie P.Sienkiewicz, Kraków, 2003[15].

Równie popularnym zabezpieczeniem danych jest tzw. zabezpieczenie poprzez sieć. Wówczas w każdej chwili można dokonać namierzenia sprzętu, ewentualnie sprawdzić w sposób niezauważalny, kto w danym momencie korzysta z danych informacji. Wszystkie czynności wykonuje się zdalnie. Tego rodzaju zabezpieczenie, co prawda odnosi się do samego sprzętu komputerowego. W ten sposób również chroni się dostęp do baz danych, dokumentów, kont bankowych, itp.

W związku z tym widać, że istnieje wiele możliwości technicznych, by zabezpieczyć posiadane dane, jak również i samą sieć. Pomimo mnogości zabezpieczeń wciąż jednak nie wypracowano pełnego zabezpieczenia, co wiąże się bezpośrednio z faktem ciągłego postępu technologicznego. W związku z tym aktualnie dostępne zabezpieczenia są do złamania, chociaż w różnej perspektywie czasowej.

[15] P. Sienkiewicz, *Wizje i modele wojny informacyjnej*, [w:] Haber Lesław H. (red.), *Społeczeństwo informacyjne – wizja czy rzeczywistość?*, Uczelniane Wydawnictwa Naukowo-Dydaktyczne AGH, Kraków, 2003.

Podsumowanie

Współcześnie przedsiębiorstwa funkcjonują w dynamicznie zmieniającej się rzeczywistości rynkowej. Chcąc się do niej dostosować, konieczne staje się gromadzenie odpowiedniej ilości, kluczowych informacji. Dlatego też przedsiębiorcy prześcigają się, by pozyskiwać istotne informacje. Nie mniej jednak samo pozyskiwanie informacji nie daje gwarancji powodzenia, ponieważ informacje te należy pozyskać, potem przeanalizować, by na koniec wyciągnąć odpowiednie wnioski.

Na tej też podstawie konieczne staje się wprowadzenie rozwiązań, które pozwolą na zabezpieczanie odpowiednich informacji. Tutaj można wskazać na różne rozwiązania, gdyż organizacje dysponują wieloma danymi. Zwykle jednak tego rodzaju działania tworzą unikalne struktury, pozwalające optymalnie zarządzać informacją, ale również strzec jej, by nie dostała się ona do osób trzecich.

Bibliografia

1. Białas Andrzej*, Bezpieczeństwo informacji i usług*, Wydawnictwo Naukowo-Techniczne, Warszawa, 2006.
2. Dickey Jeff*, Nowoczesne aplikacje internetowe. MongoDB, Express, AngularJS, Node.js*, Helion, Gliwice, 2015.
3. Golat Rafał*, Internet – aspekty prawne*, Difin, Warszawa, 2003.
4. Hofmokl Justyna*, Internet jako nowe dobro wspólne*, Wydawnictwo Akademickie i Profesjonalne, Warszawa, 2009.
5. Jason Luttgens, Matthew Pepe, Kevin Mandia, *Incydenty bezpieczeństwa. Metody reagowania w informatyce śledczej*, Helion, Gliwice, 2016.
6. Kowalski Mirosław (red.), *Internet, między edukacją, bezpieczeństwem, a zdrowiem*, Maternus Media, Kraków, 2008.
7. Liderman Krzysztof*, Bezpieczeństwo informacyjne*, Wydawnictwo Naukowe PWN, Warszawa, 2011.
8. *PN-ISO/IEC 1779: 2007 Praktyczne zasady zarządzania bezpieczeństwem informacji*, *Wymagania,* PKN, Warszawa, 2007.
9. Sienkiewicz Piotr*, Wizje i modele wojny informacyjnej,* [w:] Haber Lesław (red.), *Społeczeństwo informacyjne – wizja czy rzeczywistość?*, Uczelniane Wydawnictwa Naukowo-Dydaktyczne AGH, Kraków, 2003.
10. Stańczyk Jerzy*, Współczesne pojmowanie bezpieczeństwa*, Wydawnictwo Studiów Politycznych Polskiej Akademii Nauk, Warszawa, 1996.
11. *Ustawa z dnia 29 sierpnia 1997 r. o ochronie danych osobowych*, Dz. U. z 1997, nr 133, poz. 883.

12. Wróbel Michał*, Metody zapewniania bezpieczeństwa systemów operacyjnych*, Rozprawa doktorska, Politechnika Gdańska Wydział Elektroniki, Telekomunikacji i Informatyki, Gdańsk, 2010.

Źródła internetowe

1. http://kadry.infor.pl/kadry/indywidualne_prawo_pracy/odpowiedzialnosc_prawa_i_obowiazki/648424,Jaka-odpowiedzialnosc-wobec-pracodawcy-pono si-pracownik-ktory-ujawnia-tajemnice-firmy.html.
2. http://yadda.icm.edu.pl/yadda/element/bwmeta1.element.baztech-530a 21a8-5dbb-445f-8c4c-e86cb0b2410f.
3. https://www.nik.gov.pl/o-nik/.

THE COMPANY IN VIRTUAL REALITY AND THE PROTECTION OF ITS SENSITIVE DATA

In order to successfully operate on the market, modern enterprises are forced to collect information from different areas, which needs to undergo subsequent verification. Therefore, more and more companies must also invest in newer solutions, which later become an effective “firewall” against various threats on the Web. The paper aims to discuss the security of information collected by companies with reference to virtual reality.

Keywords: security, cybersecurity, cyberreality, personal sensitive data