Leszczyński M. (2011). *Bezpieczeństwo społeczne a współczesne państwo*, „Zeszyty Naukowe Akademii Marynarki Wojennej", nr 2/2011, s. 4–5.

Mirska A., (2009). *Policja jako podstawowy podmiot w systemie bezpieczeństwa i porządku publicznego*. W: M. Brzeziński, S. Sulowski, (red.), *Bezpieczeństwo wewnętrzne państwa, Wybrane zagadnienia*, Dom Wydawniczy Elipsa, Warszawa, s. 208–227.

Skrabacz A. (2012). *Bezpieczeństwo społeczne. Podstawy teoretyczne i praktyczne*, Dom Wydawniczy Elipsa, Warszawa.

Sulowski S. (2009). *O nowym paradygmacie bezpieczeństwa w erze globalizacji*. W: M. Brzeziński, S. Sulowski (red.), *Bezpieczeństwo wewnętrzne państwa, Wybrane zagadnienia*, Dom Wydawniczy Elipsa, Warszawa, s. 11–21.

Tyburska A. (2006). *Działania profilaktyczne Policji*. W: J. Królikowska (red.), *Problemy społeczne w grze politycznej*, Wydawnictwo Uniwersytetu Warszawskiego, Warszawa s. 219.

Widacki J., *Kryminalistyka*, Wydawnictwo C.H. Beck, Warszawa 2008.

Ustawa o Policji z dnia 6 kwietnia 1990 r. 2015.355, tekst jednolity.

Rozporządzenie Ministra Spraw Wewnętrznych i Administracji z dnia 16 sierpnia 2007 r. w sprawie szczegółowego zakresu zadań i zasad organizacji policji sądowej. 2007. 155. 1093, ze zm.

Źródła internetowe

Grąbczewski R., *Bezpieczeństwo ludzkie*, https://pl.wikipedia.org/wiki/Bezpiecze-%C5%84stwo_ludzkie, 2013 (data dostępu: 04.03.2016).

Kaczmarczyk E., *Programy narodowe, rządowe, w ramach których Policja zobowiązana jest do przedkładania informacji do sprawozdań z ich realizacji*, 2015, http://bip.kgp.policja.gov.pl/kgp/programy-prewencyjne/8474,PROGRAMY-NARODOWE-RZADOWE-W-RAMACH-KTORYCH-POLICJA-ZOBOWIAZANA-JEST-DO-PRZEDKLAD.html?search=734, (data dostępu: 04.03.2016).

Komenda Wojewódzka Policji w Katowicach, *Coraz bezpieczniej w województwie śląskim*, 2016, http://slaska.policja.gov.pl/kat/informacje/wiadomosci/162005,Coraz-bezpieczniej-w-wojewodztwie-slaskim.html (data dostępu: 04.03.2016).

Komenda Wojewódzka Policji w Katowicach, Inauguracja kampanii „Daj znak" 2016, http://slaska.policja.gov.pl/kat/ruch-drogowy/2016-rok-pieszego/164883,Inauguracja-kampanii-quotDaj-znakquot.html (data dostępu: 04.03.2016).

Kowalczuk K., Komunikat z badań CBOS nr 65/2015, Polacy o bezpieczeństwie w kraju i miejscu zamieszkania, 2015, http://cbos.pl/SPISKOM.POL/2015/K_065_15.PDF, (data dostępu: 04.03.2016).

Surdacki R., *Bezpieczeństwo polityczne Polski – co sądzą o tym Polacy*, 2014, http://www.nowastrategia.org.pl/bezpieczenstwo-polityczne-polski-sadza-polacy (data dostępu: 04.03.2016).

We protect (and still lose?) the data and information in the organization

Chronimy (czy ciągle tracimy?) dane i informacje w organizacji

Jacek Bajorek

Instytut Zarządzania Bezpieczeństwem Informacji
jacek.bajorek@izbi.pl

Abstract

The dynamic development of technological and economic causes an increase in the importance of information, which becomes a key resource, which makes the operations of many companies Information Security is a real nut to crack for all organizations. Most start-ups to protect the power of their computers, networks, and mobile devices, forgetting the primary threat that the weakest element of the security turns out to be a man.

Keywords: *data, security, protection, law, politics, administrator, confidentiality*

Streszczenie

Dynamiczny rozwój technologiczny oraz gospodarczy powoduje wzrost znaczenia wartości informacji, która staje się kluczowym zasobem stanowiącym o działalności wielu przedsiębiorstw. Bezpieczeństwo informacji stanowi nie lada orzech do zgryzienia dla wszystkich organizacji. Większość nowo założonych firm zabezpiecza na potęgę swoje komputery, sieci i urządzenia mobilne, zapominając o podstawowym zagrożeniu, iż najsłabszym elementem bezpieczeństwa okazuje się człowiek.

Słowa kluczowe: *dane, bezpieczeństwo, ochrona, ustawa, polityka, administrator, poufność*

Wprowadzenie

Zarządzanie bezpieczeństwem informacji jest procesem, który nabiera coraz większego znaczenia w ochronie interesów organizacji. Informacja stanowi taki sam zasób organizacji, jak pracownicy, technologie, środki finansowe. Tym samym kluczowe staje się właściwe zabezpieczenie przetwarzanych informacji w organizacji. Należy zwrócić uwagę, że nie chodzi tutaj tylko o wdrożenie rozwiązań w obszarze teleinformatyki, która naturalnie staje się kluczowa w przetwarzaniu informacji, lecz również zapewnienie bezpieczeństwa fizycznego, organizacyjnego, osobowego, prawnego czy też ciągłości działania. Zgodnie z zasadą najsłabszego ogniwa jedynie rozwiązania kompleksowe mogą skutecznie zabezpieczyć przetwarzane w organizacji dane.

Nieodwołalnie zbliżamy się do punktu, w którym zaniedbania z zakresu bezpieczeństwa informacji będą przynosić poważne do zaakceptowania implikacje. Obecnie możemy mówić o nowej światowej gospodarce opartej na informacji – gdzie źródłem przewagi konkurencyjnej jest dostęp do informacji. Pierwotnie panowało przekonanie, że podstawą ekonomii są ludzie i materiały, ziemia i praca oraz że są to surowce potrzebne do pozyskiwania bogactwa. Obecnie informacja jest dla organizacji niezwykle wartościowym majątkiem, niezależnie czy jest to receptura, lepszy proces produkcyjny, czy lista klientów. Właściwe zarządzanie informacją przez organizację jest czymś, co decyduje o sukcesie lub porażce. Jednocześnie globalizacja gospodarki i związane z tym nowe warunki ekonomiczne, w obliczu których stoją dziś organizacje, powodują, że niektóre z nich stosują mniej etyczne metody w celu uzyskania konkurencyjnej informacji.

Podstawowe zasady bezpieczeństwa informacji i ochrony danych osobowych

Systemy Zarządzania Bezpieczeństwem Informacji (SZBI) zostały stworzone, aby chronić dane w firmach i organizacjach z nimi współpracujących. Do zadań SZBI należy nie tylko zachowanie prywatności (poufności), ale także zapewnienie jednolitości i czytelności danych. Stare przysłowie mówi, że „wiedza to siła", dlatego systemy zarządzania, które mają za zadanie chronić „wiedzę" organizacji, są ważnym i silnym narzędziem (Kępa, 2012, s. 44–47). Systemy Bezpieczeństwa Informacji są przeznaczone dla wszystkich mających związek z technologiami informacyjnymi, gdyż informacja

może być przechowywana na wiele sposobów. Na przykład SZBI sprawdza zarówno poziom zabezpieczeń fizycznych (takich jak drzwi, okna, zamki, bramy), jak i aspekt ludzki (w tym badania przesiewowe i zapewnienie odpowiedniego dostępu do informacji poufnych). Norma IEC/ISO 27001 System Zarządzania Bezpieczeństwem Informacji jest zaprojektowana jako przewodnik dla organizacji, jak chronić dane, zarówno własne, jak i swoich klientów. Informacja w dzisiejszym świecie stała się majątkiem kluczowym dla firm, a właściwe jej wykorzystanie decyduje o sukcesie firmy. Aby informacja była użyteczna, musi jednakże spełniać szereg wymagań: musi być wiarygodna, dostępna, spójna i chroniona.

Głównym celem bezpieczeństwa informacji jest (PN-ISO/IEC 27001:2007 Polski Komitet Normalizacyjny):

- poufność informacji (ang. *Confidentiality*) – zabezpieczane informacje powinny być dostępne tylko dla jednostek upoważnionych do ich dostępu,
- integralność (ang. *Integrity*) – upoważnione jednostki mogą modyfikować dane tylko w określony dla tych jednostek sposób,
- dostępność (ang. *Availability*) – zabezpieczane informacje muszą być dostępne dla uprawnionych jednostek w określonych granicach czasowych.

Spełnienie powyższych warunków nie jest zadaniem łatwym dla organizacji z uwagi na konflikt zachodzący pomiędzy poufnością a integralnością i dostępnością.

Bezpieczeństwo informacji oznacza jej ochronę przed zagrożeniami w celu zapewnienia ciągłości działania organizacji, minimalizacji ryzyka, maksymalizacji zwrotu poniesionych wydatków i zwiększania możliwości organizacji. Dla niektórych instytucji (np. wojskowych) bezpieczeństwo informacji jest wpisane w podstawową działalność. Istnieją także uregulowania prawne stawiające wymogi np. ochrony danych osobowych lub ochrony informacji niejawnych.

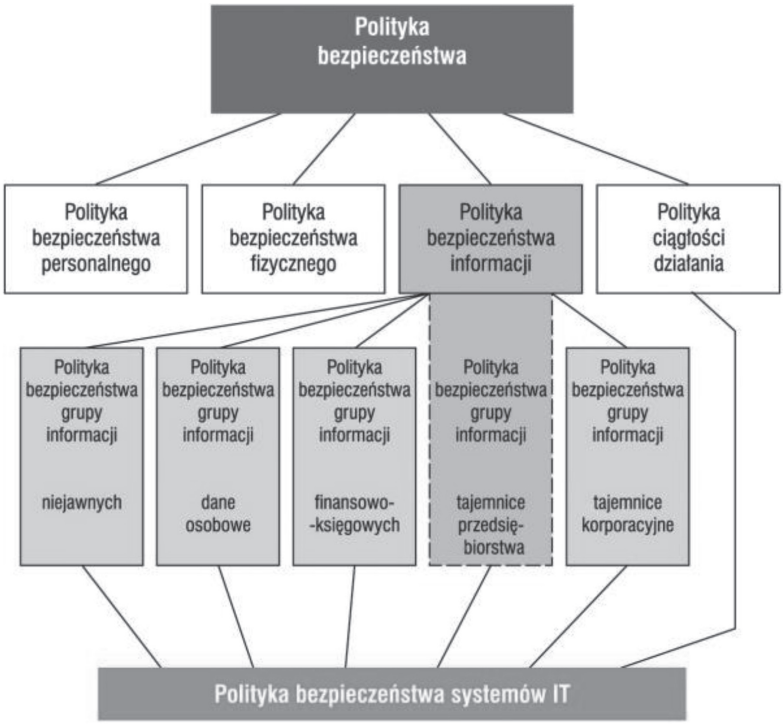
W Polsce istnieje szereg uregulowań prawnych dotyczących bezpieczeństwa informacji – ustawy, rozporządzenia, normy, na podstawie których można wszcząć postępowanie wobec osób naruszających zasady bezpieczeństwa informacji (w tym przestępców komputerowych). W miarę jak nasze społeczeństwo ewoluuje w stronę społeczeństwa informacyjnego, a biznes w stronę e-biznesu, administracja w kierunku e-administracji, informacja staje się jednym z najcenniejszych współczesnych dóbr. Nowoczesne korporacje, zdając sobie

sprawę z wagi przesyłanych informacji, skłonne są wydawać fortuny w celu ich zabezpieczenia (Barta, Markiewicz, Fajgielski, 2011, s. 112–121). Rozwój technologii informatycznych sprawił, że informacja przechowywana jest w większym stopniu w formie elektronicznej, wewnątrz systemów bezpieczeństwa.

W celu zapewnienia bezpieczeństwa informacji, a tym samym jej jakości, należy podjąć środki zabezpieczenia systemów bezpieczeństwa. Zagrożeń bezpieczeństwa systemów jest wiele. Do najważniejszych klas zagrożeń należą:

- siły wyższe (np. klęski żywiołowe, zmiany prawa),
- działania przestępcze,
- błędy personelu obsługującego system komputerowy,
- zła organizacja pracy (np. brak jasno sprecyzowanych zakresów odpowiedzialności, nieprzestrzeganie lub brak odpowiednich przepisów itd.),
- awarie sprzętu i oprogramowania.

Rysunek 1. Więzi polityki bezpieczeństwa informacji stosowane w organizacji



Źródło: opracowanie własne

Skuteczność zaprojektowanych zabezpieczeń zależy od ludzi: żaden system bezpieczeństwa nie obroni systemu komputerowego, jeśli człowiek zawiedzie zaufanie. Polityka bezpieczeństwa firmy powinna wspierać podstawową działalność i cele firmy. Zarządzanie bezpieczeństwem informacji w systemach informatycznych powinno wiązać się z powołaniem zespołu fachowców odpowiedzialnych za opracowanie dokumentów, takich jak: „Polityka bezpieczeństwa teleinformatycznego", „Plan bezpieczeństwa teleinformatycznego", „Instrukcja bezpieczeństwa" czy „Plan ciągłości działania", oraz wdrożenie i egzekwowanie zasad w nich zawartych.

Edukacja w zakresie bezpieczeństwa informacji i ochrony danych osobowych

Informacje w postaci elektronicznej przesyłane lub przetwarzane w systemach informatycznych organizacji mają dla instytucji wartość i dlatego muszą być odpowiednio chronione. Bezpieczeństwo informacji elektronicznej oznacza, że jest ona chroniona przed różnymi zagrożeniami lub zakłóceniami, tak aby zapewnić ciągłość działalności i zminimalizować straty (Iwaszko, 2012, s. 46).

W celu zminimalizowania zagrożeń w organizacji prowadzony jest audyt bezpieczeństwa informacji, rozumiany jako całość działań zmierzających do kontroli zabezpieczeń w systemie informatycznym, sprawdzenie obiegu informacji oraz zasobów ludzkich. Celem audytu jest wskazanie słabych punktów w sieci oraz przedstawienie planu działań naprawczych. Ponadto audyt powinien usprawnić ochronę informacji tworzonej, przetwarzanej, przechowywanej i przesyłanej nie tylko za pomocą systemów komputerowych (Kępa, 2014, s. 99–109).

Jednym z rezultatów przeprowadzenia audytu bezpieczeństwa informacji jest wzrost odporności systemów teleinformatycznych przedsiębiorstwa na zagrożenia działaniami zewnętrznymi, takimi jak szkodliwe oprogramowanie:

- wirusy:
  - mogą uszkodzić system,
  - kasować dane;
- konie trojańskie:
  - przejmują kontrolę nad zainfekowanym systemem i powodują w nim rozległe szkody,
  - mogą uruchamiać i zamykać programy,

  - przerywać sesje online,
  - manipulować danymi,
  - prowadzić podsłuch sesji online,
  - sczytywać hasła (np. do rachunków internetowych banków itp.),
  - prowadzić do skanowania portów;
- robaki:
  - same się powielają i rozsyłają za pomocą poczty elektronicznej.

Do zabezpieczenia informacji chronionych z mocy ustaw oraz wskazanych przez organizację, jako posiadających istotne znaczenie i przesyłanych w sieciach teleinformatycznych, należy stosować metody i środki zabezpieczające, polegające na szyfrowaniu informacji lub zastosowaniu innych mechanizmów kryptograficznych, gwarantujących integralność i ochronę przed nieuprawnionym ujawnieniem tych informacji lub uwierzytelnieniem. Urządzenia i systemy kryptograficzne, kodowe, dokumenty szyfrowe i kodowe oraz przepisy o posługiwaniu się nimi ewidencjonuje się w oddzielnych dziennikach (Wiewiórowski, 2013, s. 11–12). Nadzór nad ochroną i bezpieczeństwem urządzeń oraz systemów kryptograficznych i kodujących sprawuje komórka bezpieczeństwa.

Techniki Inżynierii Społecznej „Social Engineering", które umożliwiają zdobycie informacji, wykorzystują ludzkie ułomności, takie jak lenistwo, chęć upraszczania sobie wszelkich zadań czy bezkrytyczna wiara w uczciwość kolegów (Mitnick, 2003, s. 67).

Sztuka podstępu

Haker przeprowadza rozmowę, bezpośrednią lub telefoniczną, w trakcie której uzyskuje od rozmówcy poufne dane. Następnym sposobem uzyskania poufnych danych jest przeglądanie dokumentów w koszach, do których pracownicy często wrzucają niezniszczone dokumenty. Występowanie zagrożeń losowych zewnętrznych (np. klęsk żywiołowych, przerw w zasilaniu) może prowadzić do utraty integralności danych, ich zniszczenia i uszkodzenia infrastruktury technicznej systemu; ciągłość systemu zostaje zakłócona, nie dochodzi do naruszenia poufności danych. W wyniku zagrożeń losowych wewnętrznych (np. niezamierzone pomyłki operatorów, administratora, awarie sprzętowe, błędy oprogramowania, pogorszenie jakości sprzętu i oprogramowania) może dojść do zniszczenia danych, może zostać zakłócona ciągłość

pracy systemu, może też nastąpić naruszenie poufności danych. Zagrożenia zamierzone to z kolei świadome i celowe działania powodujące naruszenia poufności danych (zazwyczaj nie następuje uszkodzenie infrastruktury technicznej i zakłócenie ciągłości pracy). Zagrożenia te możemy podzielić na:

- nieuprawniony dostęp do systemu z zewnątrz (włamanie do systemu),
- nieuprawniony dostęp do systemu z jego wnętrza,
- nieuprawnione przekazanie danych,
- bezpośrednie zagrożenie materialnych składników systemu (np. kradzież sprzętu).

Naruszenie lub podejrzenie naruszenia systemu informatycznego, w którym przetwarzane są dane osobowe, następuje w sytuacji (Kępa, 2014, s. 174–182):

- losowego lub nieprzewidzianego oddziaływania czynników zewnętrznych na zasoby systemu, jak:
  - wybuch gazu,
  - pożar,
  - zalanie pomieszczeń,
  - katastrofa budowlana,
  - napad,
  - działania terrorystyczne,
  - itp.;
- niewłaściwych parametrów środowiska, jak:
  - nadmierna wilgotność lub wysoka temperatura,
  - oddziaływanie pola elektromagnetycznego,
  - wstrząsy lub wibracje pochodzące od urządzeń przemysłowych,
  - awarie sprzętu lub oprogramowania, które wyraźnie wskazują na umyślne działanie w kierunku naruszenia ochrony danych,
  - pojawienie się odpowiedniego komunikatu alarmowego,
  - podejrzenie nieuprawnionej modyfikacji danych w systemie lub innego odstępstwa od stanu oczekiwanego,
  - naruszenie lub próby naruszenia integralności systemu bądź bazy danych w tym systemie,
  - praca w systemie wykazująca odstępstwa uzasadniające podejrzenie przełamania lub zaniechania ochrony danych osobowych – np. praca osoby, która nie jest formalnie dopuszczona do obsługi systemu,

– ujawnienia nieautoryzowanych kont dostępu do systemu,
– naruszenie dyscypliny pracy w zakresie przestrzegania procedur bezpieczeństwa informacji (np. niewylogowanie się przed opuszczeniem stanowiska pracy, pozostawienie danych osobowych w drukarce itp.).

Za naruszenie ochrony danych uważa się również stwierdzone nieprawidłowości w zakresie zabezpieczenia fizycznego miejsc przechowywania i przetwarzania danych, np.:

- niezabezpieczone pomieszczenia,
- nienadzorowane, otwarte szafy, biurka, regały,
- niezabezpieczone urządzenia archiwizujące,
- pozostawianie danych w nieodpowiednich miejscach – kosze, stoły itp.

Najprostszym i najpopularniejszym przykładem, o którym warto wspomnieć w kontekście bezpieczeństwa systemów informatycznych, jest problem z nieodpowiednimi zasadami postępowania z hasłami dostępowymi. Zadaniem tych ostatnich jest ochrona informacji przed nieuprawnionym dostępem. Hasła i kody numeryczne są często jedyną stosowaną metodą zabezpieczania czynności wykonywanych przez użytkowników systemu teleinformatycznego (PN-ISO/IEC 27001:2007 Polski Komitet Normalizacyjny).

Z kolei łatwe do odgadnięcia, najczęściej bazujące na wyrazach ze słownika, hasła to częsta przyczyna wycieku danych. W związku z tym weryfikuje się je na samym początku testów penetracyjnych, których zadaniem jest symulowanie ataków prowadzonych przez sieciowych intruzów.

Metody socjotechniki i uzyskiwania informacji

Czasami, żeby ułatwić sobie życie, idziemy na skróty i po prostu nie uświadamiamy sobie, w jaki sposób nasze działania wpłyną na nasze bezpieczeństwo. Dotyczy to haseł – podczas transakcji biznesowych coraz częściej dokonujemy online zakupów, transakcji bankowych, płacenia rachunków itd. Nierzadko posiadamy 10, 20 lub więcej kont online, dlatego zapamiętanie (a nawet wybranie) unikatowego hasła dla każdego z nich jest bardzo trudne (Mitnick, 2003, s. 108–111).

Hakerzy dobrze znają sposoby tworzenia haseł przez użytkowników i pozornie trudne do odgadnięcia kombinacje, takie jak na przykład 1qazxsw23edc (odwzorowanie kształtu przez wciskanie odpowiednich klawiszy) czy 19750503 (data urodzenia), są bardzo często sprawdzane przez kom-

puterowych włamywaczy (Kluska, 2013, s. 99–109). Warto z jednej strony pamiętać o odpowiednim poziomie skomplikowania hasła, czyli używaniu znaków specjalnych oraz cyfr. Z drugiej strony, jeśli będzie ono zbyt skomplikowane (i trudne do zapamiętania), istnieje ryzyko, że użytkownik zapisze je na umieszczonej w pobliżu klawiatury kartce (Kępa, 2012, s. 201–208). Należy więc z rozwagą planować wymogi odnośnie do stopnia skomplikowania haseł dostępu. Można to osiągnąć, na przykład konfigurując odpowiednio urządzenia i systemy, tak aby wymuszały na użytkownikach zarówno ustawianie trudnych do odgadnięcia haseł, jak i ich systematyczną zmianę. Warto też pamiętać o automatycznym blokowaniu dostępu do konta w sytuacji powtarzających się prób logowania, z których każda zakończona jest niepowodzeniem (Barta, Markiewicz, Fajgielski, 2011, s. 43–54).

System pozwalający na wielokrotne testowanie poprawności haseł dostępowych jest łatwym celem dla intruza, który w zależności od zasobów i konfiguracji będzie w stanie sprawdzić setki tysięcy haseł w ciągu doby. Jednym z problemów związanych z atakami wykorzystującymi socjotechnikę jest to, że stanowią ruchomy cel: kolejne oszustwa nigdy nie wyglądają tak samo. Z tego powodu zwykłym użytkownikom trudno jest określić, co jest bezpieczne, a co nie. Naturalnie, brak świadomości to niejedyny problem. Darmowe treści audio, wideo lub zdjęcia nagich gwiazd to popularny chwyt, za pomocą którego oszuści próbują nakłonić ludzi do kliknięcia odsyłacza, który powinni zignorować. Zdrowy rozsądek często podpowiada, że jeżeli coś wydaje się zbyt piękne, żeby było prawdziwe, prawdopodobnie nie jest prawdziwe (Mitnick, 2003, s. 186–192). Jednak ten sam zdrowy rozsądek czasami zostaje uśpiony, właśnie wtedy gdy powinien ostrzec Cię, że podjęcie działania – w tym przypadku kliknięcie odsyłacza – może być szkodliwe.

Cyberprzestępcy nadal wykorzystują powszechnie socjotechnikę, tj. próbują nakłonić ludzi, aby zrobili coś, co zmniejszy ich bezpieczeństwo w sieci. Mimo wielu apeli wciąż skuteczne są oszustwa phishingowe (Iwaszko, 2012, s. 35–45). Ich celem jest zwabienie użytkowników na fałszywe strony internetowe i nakłonienie do tego, by ujawnili tam swoje dane osobowe – hasła, numery PIN i inne, które mogą zostać wykorzystane przez cyberprzestępców. Klasyczne oszustwo phishingowe przybiera postać spekulacyjnej wiadomości e-mail, wysyłanej na miliony adresów w nadziei, że wystarczająca liczba osób złapie się na „haczyk" i kliknie zawarty w e-mailu odsyłacz. Podobnie jak kieszonkowcy, oszuści internetowi również podążają za modą.

Zważywszy na coraz większą liczbę osób korzystających z portali społecznościowych, takich jak Facebook, MySpace, LinkedIn czy Twitter, nie dziwi fakt, że serwisy te stają się celem licznych ataków. Hakerzy włamują się na konta na Facebooku, a następnie wykorzystują je do rozsyłania wiadomości zawierających odsyłacze do szkodliwych programów. Mogą też rozsyłać „tweety" z odsyłaczami, ukrywając ich rzeczywisty adres za pomocą usługi skracania adresów URL, lub po prostu udawać przyjaciela, który zgubił się w odległym kraju i desperacko potrzebuje pieniędzy na powrót do domu. Żadna z tych metod nie jest specyficzna dla portali społecznościowych. Cyberprzestępcy po prostu wykorzystują metody, które już wcześniej okazały się skuteczne. Biorąc pod uwagę fakt, że systemy informatyczne wspierają działalność przedsiębiorstw każdej wielkości, działających we wszystkich branżach, okresowe audyty bezpieczeństwa informatycznego stają się elementem budującym skuteczną ochronę systemów informatycznych (Krasuski, 2010, s. 87).

Korzyści wynikające z przeprowadzania audytu bezpieczeństwa informacji dla organizacji to:

- wzrost bezpieczeństwa informacji i systemów informatycznych,
- ograniczenie ryzyka utraty poufnych danych, ich zniekształcenia, niepowołanego dostępu do nich,
- ograniczenie strat materialnych wynikających np. z przedostania się informacji poufnych do konkurencji, utraty danych i niepożądanej modyfikacji danych przechowywanych w systemach,
- wzrost bezpieczeństwa działania i wiarygodności,
- możliwość precyzyjnego określania miejsc oraz prawdziwych przyczyn utraty danych,
- usprawnienie przepływu i dostępu do informacji przy jednoczesnym wzroście ich bezpieczeństwa,
- określenie nakładów inwestycyjnych potrzebnych do zabezpieczenia informacji i informatyki,
- wdrożenie polityki bezpieczeństwa,
- możliwość pozyskania certyfikatu ISO.

W opinii resortów, Ministerstwa Cyfryzacji i Ministerstwa Finansów, nie należy automatycznie przypisywać zadania audytu w zakresie bezpieczeństwa informacji komórce audytu wewnętrznego, gdyż punktem odniesienia

dla omawianych przepisów był System Zarządzania Bezpieczeństwem Informacji, a nie przepisy ustawy o finansach publicznych dotyczące audytu wewnętrznego. Ministerstwo Finansów opracowało wytyczne dotyczące wydzielania od odrębnej komórki organizacyjnej zakresu System Zarządzania Bezpieczeństwem Informacji i ochrony danych osobowych. Przewidują one, że przede wszystkim przypisanie tego zadania powinno odbyć się w sposób formalny poprzez odpowiednie uzupełnienie karty audytu lub innego dokumentu wewnętrznego opisującego cel, zakres i uprawnienia audytu wewnętrznego w jednostce poprzez jednoznaczne wskazanie komórki bezpieczeństwa informacji jako odpowiedzialnej za realizację tego zadania (Barta, Markiewicz, Fajgielski, 2011, s. 87–95).

Kierownik jednostki powinien także brać pod uwagę fakt, że powierzenie prowadzenia corocznego audytu wewnętrznego w zakresie bezpieczeństwa informacji może oznaczać ograniczenie realizacji zadań zapewnianych w innych obszarach ryzyka. Ponadto kierownik jednostki powinien brać pod uwagę, czy pracownicy komórki audytu wewnętrznego posiadają odpowiednie kwalifikacje, doświadczenie i znajomość metodyki prowadzenia audytu w obszarze bezpieczeństwa informacji. W przypadku stwierdzenia braku odpowiedniej wiedzy i doświadczenia należy rozważyć skorzystanie z pomocy ekspertów wewnętrznych lub zewnętrznych. W wyniku przeprowadzonego audytu bezpieczeństwa informacji tworzony jest raport wskazujący na słabe i mocne strony organizacji w zakresie audytowanych obszarów, identyfikujący ryzyka, dostarczający informacje dotyczące poszanowania norm i procedur bezpieczeństwa oraz określający zasoby ludzkie, informatyczne i techniczne, konieczne do tego, by działając wspólnie, zachować odpowiedni poziom bezpieczeństwa dla danych, systemów operacyjnych oraz całej organizacji.

Podsumowanie

W obecnych czasach istnieje duże zapotrzebowanie na stosowanie zabezpieczeń w zakresie bezpieczeństwa informacji. Wdrażanie bezpieczeństwa informacji jest niezmiernie ważne dla dzisiejszego globalnego świata biznesu, który chce w bezpieczny i zaufany sposób wymieniać informacje, korzystać w pełni z dobrodziejstw globalnej sieci, pragnie również być konkurencyjny i szybko reagować na zmieniający się rynek. Nawet optymalnie procedury i regulaminy czy inwestycje w najnowsze technologie bezpie-

czeństwa systemów informatycznych nie ochronią informacji, jeżeli kultura ochrony informacji nie będzie priorytetem wśród pracowników organizacji.

Jednym z elementów kultury nowoczesnych organizacji jest Polityka Bezpieczeństwa Informacji wdrażana w ich strukturach. Aby jednak ten ambitny cel został osiągnięty, zasady Polityki Bezpieczeństwa Informacji muszą stać się normami przestrzeganymi przez wszystkich pracowników organizacji. Podstawowym problemem jest brak wiedzy pracowników o tym, jaka jest wartość informacji przetwarzanych w organizacji, które informacje i dlaczego należy szczególnie chronić. Sens ochrony informacji, jako najcenniejszego dobra w organizacji, jest bardzo mało uchwytny. Ochrona informacji jest normą nowoczesnej organizacji. Pokazuje siłę organizacji i jej pewność, co przynosi najcenniejszą nagrodę w postaci zaufania klientów i prestiżu. Tej normy nie da się narzucić, trzeba ją wybudować w strukturze organizacji. Organizacje, które bagatelizują tę normę, mogą w wyniku incydentów bezpieczeństwa nie tylko stracić wiarygodność, ale również zakończyć działalność.

Bibliografia

ABC bezpieczeństwa danych osobowych przetwarzanych przy użyciu systemów informatycznych (2007). Warszawa: www.giodo.gov.pl.

Barta J., Markiewicz R., Fajgielski P. (2011). *Ochrona danych osobowych. Komentarz*. Warszawa: Wolters Kluwer Polska.

Iwaszko B. (2012). *Ochrona informacji niejawnych w praktyce*. Wrocław: PRESSCOM.

Kępa L. (2012). *Dane osobowe w firmie*. Warszawa: Difin.

Kępa L. (2014). *Ochrona danych osobowych w praktyce*. Warszawa: Difin.

Kluska M., Wanio G. (2013). *Ochrona danych osobowych w działach kadr.* Wrocław: PRESSCOM.

Krasuski A. (2010). *Outsourcing danych osobowych w działalności przedsiębiorstw*. Warszawa: LexisNexis.

Mitnick K. (2003). *Sztuka podstępu*. Warszawa: Helion.

Wiewiórowski W.R. (2013). *Prywatność pacjenta musi być chroniona*, „IT w Administracji" z 2013 r. nr 2.

Akty prawne

Konstytucja RP z 2 kwietnia 1997 r. (Dz.U. z 1997 r. nr 78, poz. 483).

PN-ISO/IEC 27001:2007 Polski Komitet Normalizacyjny – Technika informatyczna – Techniki bezpieczeństwa – Systemy zarządzania bezpieczeństwem informacji.

Rozporządzenie Ministra Spraw Wewnętrznych i Administracji z dnia 29 kwietnia 2004 r. w sprawie dokumentacji przetwarzania danych osobowych oraz warunków technicznych i organizacyjnych, jakim powinny odpowiadać urządzenia i systemy informatyczne służące do przetwarzania danych osobowych (Dz.U. z 2004 r. nr 100, poz. 1024).

Ustawa z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (Dz.U. z 2014 r. poz. 1182 ze zm.).