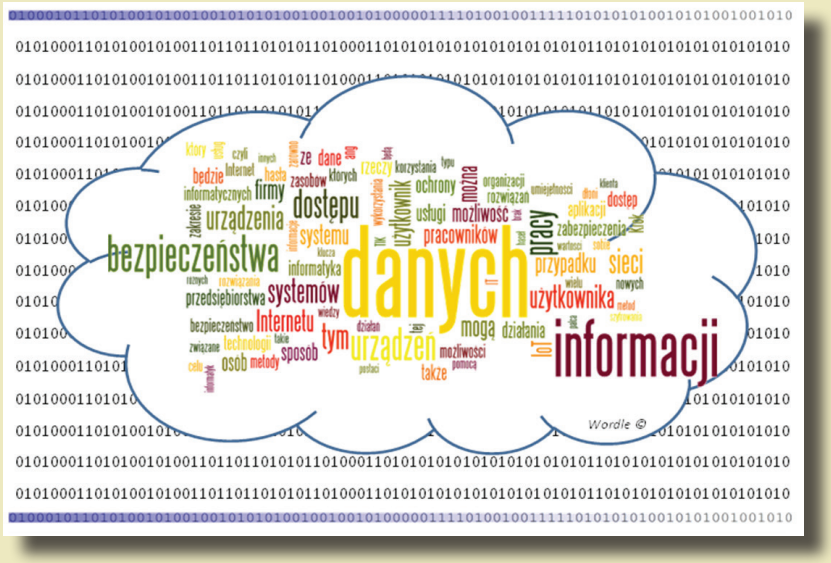
POLITECHNIKA LUBELSKA

MONOGRAFIE

Uwarunkowania prawne, informatyczne i społeczne e-obywatela w społeczeństwie informacyjnym

redakcja
Marzena Cichorzewska
Bogdan Wit



Lublin 2015

Uwarunkowania prawne, informatyczne i społeczne e-obywatela w społeczeństwie informacyjnym

Monografie – Politechnika Lubelska

Politechnika Lubelska
Wydział Zarządzania
ul. Nadbystrzycka 38
20-618 Lublin

Uwarunkowania prawne, informatyczne i społeczne e-obywatela w społeczeństwie informacyjnym

redakcja
Marzena Cichorzewska
Bogdan Wit

Politechnika Lubelska
Lublin 2015

Recenzent:
dr hab. inż. Tomasz Klepka, prof. Politechniki Lubelskiej

Redakcja i skład: Robert Skrzypa

Projekt okładki: Bogdan Wit

Publikacja wydana za zgodą Rektora Politechniki Lubelskiej

ISBN: 978-83-7947-244-4

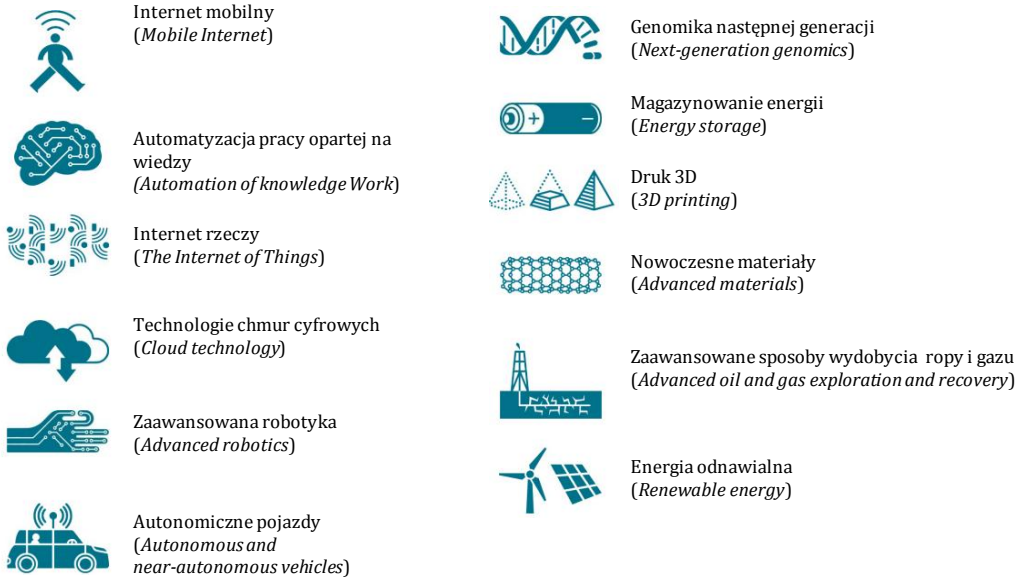
Wydawca: Politechnika Lubelska
ul. Nadbystrzycka 38D, 20-618 Lublin
Realizacja: Biblioteka Politechniki Lubelskiej
Ośrodek ds. Wydawnictw i Biblioteki Cyfrowej
ul. Nadbystrzycka 36A, 20-618 Lublin
tel. (81) 538-46-59, email: wydawca@pollub.pl
www.biblioteka.pollub.pl

Spis treści

Wstęp

Uwarunkowania prawne, informatyczne i społeczne e-obywatela w społeczeństwie informacyjnym to pozycja monograficzna poruszająca istotną problematykę budowania, funkcjonowania i rozwoju technologii cyfrowych w społeczeństwie opartym o zasoby informacyjne. Technologie cyfrowe określane technologie informacyjno-komunikacyjne (ICT) stają się fundamentami rozwoju kraju. Poziom ich wykorzystania we wszystkich sektorach i podsektorach instytucjonalnych gospodarki stanowi istotny wyznacznik rozwiniętego społeczeństwa informacyjnego. Zaawansowane techniczne i programowe rozwiązania cyfrowe wdrożone w gospodarce implikują rozwój gospodarki cyfrowej, ale również przyczyniają się do rozwoju gospodarki tradycyjnej. Gospodarka elektroniczna będzie się rozwijała do określonego poziomu, ponieważ nie wszystkie rzeczy wykorzystywane przez człowieka mogą być cyfrowe. Do życia i funkcjonowania człowieka potrzebną są również rzeczy fizyczne. Gospodarka oparta na rzeczach będzie miała duże znaczenie, dlatego że również stanowi podstawę dla funkcjonowania gospodarki elektronicznej. Aby korzystać z gospodarki elektronicznej należy posiadać urządzenia dostępowe, urządzenia przetwarzające, gromadzące dane, a więc przedmioty dostosowane do przetwarzania cyfrowych danych oraz oprogramowanie umożliwiające sterowanie tymi urządzeniami. Jak podaje raport McKinsey Global Institute przyszłością gospodarki kraju i świata będzie dwanaście ekonomicznie potencjalnych przełomowych technologii (rys. 1). Wśród których można

wymienić: Internet mobilny, automatyzacja pracy opartej na wiedzy, Internet rzeczy, technologie chmur cyfrowych.



Rys. 1. Dwanaście ekonomicznie potencjalnych przełomowych technologii na świecie według McKinsey Global Institute

Źródło: Disruptive technologies: Advances that will transform life, business, and the global economy. McKinsey Global Institute, May 2013, s. 4

Podstawą rozwoju dla ICT są działania w poszerzaniu zakresu dostępności łączy szerokopasmowych, wprowadzanie szybkich sieci internetowych oraz upowszechniania nowych technologii i sieci dla gospodarki cyfrowej, co ma wzmocnić zastosowania ICT przez obywateli w ich codziennym życiu oraz w życiu zawodowym. Dotyczy to przede wszystkim zastosowań na poziomie przedsiębiorstwa, w którym następują procesy biznesowe wpływające na całokształt działalności i postrzegania przedsiębiorstwa na rynku. Od ochrony danych i informacji oraz od profesjonalizmu zawodowego w dużym stopniu zależy sukces przedsiębiorstwa na rynku.

W niniejszej monografii przedstawione zostaną przede wszystkim zagadnienia z obszarów ICT, według zasady od ogółu do szczegółu. Rozdział pierwszy *E-obywatel w społeczeństwie informacyjnym – możliwości, potrzeby, zagrożenia* tematycznie

dotyczy poziomu kompetencji obywatela z zetknięciu się z technologiami ICT w życiu osobistym, zawodowym, publicznym i społecznym. Obywatel nie może czuć się wykluczony, dlatego w funkcjonowaniu gospodarki cyfrowej stają się ważne jego umiejętności, podwyższanie kompetencji oraz potwierdzanie jego kompetencji przez niezależne podmioty certyfikujące.

Wybrane zagadnienia dotyczące zarządzania ochroną informacji w przedsiębiorstwie przedstawiono w rozdziale drugim *Wybrane problemy zarządzania ochroną informacji w przedsiębiorstwie*. Zagrożenia związanych z utratą danych to nie tylko aspekt finansowy, ale również jak podkreśla autorka to aspekt strat praw własności i zajmowania się czynnościami naprawczymi. W rozdziale tym również zaprezentowano przykładową politykę bezpieczeństwa informacyjnego przedsiębiorstwa w obszarze ICT w postaci etapów i kroków postępowania zmierzającego do zachowania tajemnicy przedsiębiorstwa.

Zasady profesjonalnej praktyki zawodowej oraz zasady etyczne i odpowiedzialność w zawodzie informatyka została przedstawiona w rozdziale trzecim *Profesjonalizm i odpowiedzialność w zawodzie informatyka*. Stosowanie się do skodyfikowanej wiedzy (kompendiów wiedzy, standardów, specyfikacji oraz innych branżowych przepisów i zasad) jest wyrazem wysokiego poziomu dojrzałości informatyka, ale jest to zaledwie wstępny warunek profesjonalizmu zawodowego. Informatyk w przedsiębiorstwie powinien kierować się zasadami etycznymi, polityką równości i prywatności oraz odpowiedzialnością zawodową i społeczną za swoje poczynania. Przedstawienie odpowiedzialności zawodu informatyka w różnych aspektach ze szczególnym uwypukleniem etyki to główny przekaz treści tego rozdziału. Stosowanie się do branżowej skodyfikowanej wiedzy oraz włączanie się informatyków do branżowych towarzystw, np. PTI (Polskie Towarzystwo Informatyczne) umożliwia wzrost zaufania użytkowników do ich pracy i ma wpływ na budowę społeczeństwa informacyjnego, co przynosi wymierne korzyści społeczne i ekonomiczne.

Rozdział czwarty *Internet rzeczy w e-gospodarce – wyzwania i perspektywy* dotyczy potencjalnie przełomowej technologii jakimi są rzeczy komunikujące się między sobą lub człowiekiem za pomocą sieci komputerowej. Internet rzeczy, czyli

połączone za pośrednictwem sieci Internet fizyczne przedmioty i możliwość komunikacji z innymi przedmiotami, zmienia stosunek człowieka do tych przedmiotów[1]. Automatyzacja w komunikacji przedmiotów, która następuje pod wpływem określonych bodźców i wzajemna komunikacja to główna treść tego rozdziału. Również autor przedstawia aspekty bezpieczeństwa opisywanej technologii w kwestiach prawa, uregulowań oraz polityk poszczególnych państw, regionów i sektorów przemysłu.

Aspekt praktyczny bezpieczeństwa informacji na poziomie przedsiębiorstwa na przykładzie międzynarodowej organizacji handlowej został przedstawiony w rozdziale piątym *Bezpieczeństwo informacji na przykładzie międzynarodowej organizacji handlowej*. Autorka będąca pracownikiem opisuje sposób podejścia dużej organizacji do bezpieczeństwa danych i problemy związane z szybkością reakcji na zagrożenia również w kontekście różnic kulturowych.

Rozdział szósty *Sprzętowe rozwiązania informatyczne zapewniające bezpieczeństwo tożsamości cyfrowej* oraz rozdział siódmy *Programowe rozwiązania informatyczne zapewniające bezpieczeństwo tożsamości cyfrowej* są komplementarne. Pierwszy z nich dotyczy rozwiązań sprzętowych będących w użyciu z zapewnieniu bezpieczeństwa tożsamości cyfrowej. Drugi rozdział zamykający monografię dotyczy dostępnych do zastosowania rozwiązań programowych w powiązaniu z rodzajem systemu operacyjnego zainstalowanego na urządzeniu. Autor przedstawia poszczególne funkcjonalności systemów operacyjnych: ANDROID, Ios, WINDOWS 8.X, LINUX, CHROME OS.

Monografia powstała dzięki zaangażowaniu i pasji współautorów, którzy przekazali swoją wiedzę i doświadczenie zawodowe. W ten sposób została stworzona unikalna monografia członków koła PTI w Lublinie wpisująca się w działania Polskiego Towarzystwa Informatycznego.

Marzena Cichorzewska
Bogdan Wit

[1] Internet przedmiotów obejmuje trzy rodzaje komunikacji: rzeczy do osoby (*things-to-person*), rzeczy do rzeczy (*thing-to-thing*), maszyna do maszyny (*Machine-to-Machine*, M2M).

1

E-obywatel w społeczeństwie informacyjnym – możliwości, potrzeby, zagrożenia

1.1. SPOŁECZEŃSTWO INFORMACYJNE I JEGO PODSTAWOWA JEDNOSTKA

Termin społeczeństwo informacyjne (SI) pojawiło się wraz z intensywnym rozwojem technologii informacyjno-komunikacyjnych (TIK lub ICT – *Information and communications technology*) i upowszechnieniem Internetu, pierwszy raz został użyty w raporcie Bangemanna 1994 r. "Europa i społeczeństwo globalnej informacji. Zalecenia dla Rady Europy". J. Nowak uporządkował terminologię, przedstawił 22 definicje społeczeństwa informacyjnego, z których jedna przyjęta na I Kongresie Informatyki Polskiej w 1994 definiuje społeczeństwo informacyjne jako:

„Społeczeństwo charakteryzujące się przygotowaniem i zdolnością do użytkowania systemów informatycznych, skomputeryzowane i wykorzystujące usługi telekomunikacji do przesyłania i zdalnego przetwarzania informacji" [NOW].

Syntetyczne ujęcie tak szerokiego tematu społeczeństwa informacyjnego można przedstawić w następujących aspektach:

Społeczeństwo informacyjne to społeczeństwo które:

- wykorzystuje technologie sieciowe i komunikacyjne, w tym mobilne, technologie przechowywania i przetwarzania danych, technologie gromadzenia i prezentowania danych oraz techniczne narzędzia komunikacji, magazynowania i przekształcania informacji,

- traktuje informację i wiedzę jako podstawowy zasób, towar, wartość dodaną, źródło utrzymania, podstawowy czynnik wytwórczy, kluczowy element społeczno-ekonomicznej działalności i zmian, znaczący czynnik wzrostu gospodarczego,
- wykorzystuje Internet jako środek komunikacji obywatelskiej i informacji publicznej, narzędzie biznesu, nauki i kultury.

Determinantami rozwoju społeczeństwa informacyjnego są:

- *Infrastruktura*: rozbudowana terytorialnie sieć telekomunikacyjna.
- *Zasoby*: rozbudowane zasoby informacyjne dostępne publicznie w dobie gospodarki opartej na wiedzy i informacji.
- *Kompetencje:* umiejętność wykorzystania tych zasobów przez społeczeństwo.

Rozwój społeczeństwa informacyjnego można rozpatrywać w kilku przekrojach:

- Technologicznym – jak rozwój nowoczesnych TIK wpływa na rozwój SI.
- Ekonomicznym – informacja i wiedza staje się towarem w gospodarce, usługi dystrybuowane są drogą elektroniczną.
- Zawodowym – jak przekształcenia na rynku pracy (elastyczny czas pracy, zdalny dostęp) zmieniają życie zawodowe.
- Społecznym – jakie nowe możliwości aktywnego udziału w życiu społecznym oferują TIK (serwisy społecznościowe, fora, blogi).
- Kulturowym – jak współczesna kultura staje się rodzajem wirtualnej rzeczywistości.

Wskaźniki rozwoju społeczeństwa informacyjnego w Polsce w 2013 r. przedstawiane są corocznie jako wyniki badań GUS [GUS13], diagnozy społecznej [BAT13] w obszarach:

Infrastruktura:

- Wykorzystywanie komputerów: 95% przedsiębiorstw, 70% gospodarstw domowych (49% laptopy).
- Dostęp do Internetu: 94% przedsiębiorstw (83% łącza szerokopasmowe, 44% mobilne łącza szerokopasmowe), 72% gospodarstw domowych (69% łącza szerokopasmowe).

Zasoby:

- Własna strona internetowa: 66% przedsiębiorstw.
- Handel elektroniczny: 22% przedsiębiorstw, 32% gospodarstw domowych.

- Wyszukiwanie informacji o towarach lub usługach: 45% gospodarstw domowych.
- Poczta elektroniczna: 51% gospodarstw domowych.
- Wykorzystanie administracji: 90% przedsiębiorstw, 23% gospodarstw domowych.
- Wykorzystanie mediów społecznościowych: 16% przedsiębiorstw.

Kompetencje, umiejętności, motywacje:

- umiejętność wykorzystania komputera: 69% osób,
- umiejętność korzystania z Internetu: 63% osób (w tym 97% osób młodych 16–24, 14% starych 65 i więcej),
- umiejętność korzystania z TIK (komputer, Internet, komórka): 61%.

Badania wskazują również na zmiany struktury populacji internautów: maleje odsetek ludzi młodych, uczących się, mieszkańców dużych miast, rośnie udział osób w wieku średnim, osób z wykształceniem zawodowym, mieszkańców wsi. Maleje poziom umiejętności wykorzystania możliwości komputera: komputer (laptop, smartfon) stanowią się głównym narzędziem dostępu do Internetu, komunikacja staje się ważniejsza niż umiejętność korzystania z podstawowych aplikacji np. pakietów biurowych [BAT13].

Podstawową jednostką społeczeństwa informacyjnego jest e-obywatel. Jednak termin e-obywatel może być określany na kilka sposobów jako:

- jednostka w e-społeczeństwie, która ma prawa i obowiązki określone przez konstytucję, angażuje się w życie społeczne, polityczne,
- aktywny użytkownik komputera i Internetu (posiadający smartfon lub tablet i śledzący non stop facebooka),
- portal społecznościowy: Facebook (https://www.facebook.com/eObywatel), Twitter (https://twitter.com/#!/eObywatel), G+ (https://plus.google.com/u/0/b/112569645975630064700/), polskie forum (http://eobywatel.com),
- standard kształcenia e-obywateli – certyfikat umiejętności korzystania z Internetu https://ecdl.pl/e-citizen,
- system elektronicznego potwierdzenia poparcia dla obywatelskich projektów ustaw http://www.portalsamorzadowy.pl/spoleczenstwo-informacyjne/e-obywatel-dopiero-zaczyna-raczkowac,48770.html.

1.2. MOŻLIWOŚCI UCZESTNICTWA E-OBYWATELA W ŻYCIU OSOBISTYM, ZAWODOWYM, PUBLICZNYM I SPOŁECZNYM

Społeczeństwo informacyjne tworzą jego obywatele. Poziom ich kompetencji pozwala mniej lub bardziej aktywnie uczestniczyć w życiu demokratycznego państwa, w życiu społecznym, zawodowym. W erze społeczeństwa informacyjnego kształtowanie kompetencji e-obywatela powinno obejmować dwa obszary [SIE13]:

- szeroko rozumiana wiedza o społeczeństwie dotycząca problemów prawnych, politycznych, międzynarodowych czy socjologicznych,
- wiedza i praktyczne umiejętności wykorzystania TIK w procesie komunikacji w grupach społecznych lub partycypacji obywatelskiej (relacja obywateli z władzą lub relacja obywateli między sobą) w zakresie informowania, konsultowania czy współdecydowania.

Zastosowania TIK w procesie rozwoju demokracji i kompetencji obywatelskich dotyczą następujących rozwiązań [SIE13]:

- budowy e-biurokracji (e-administracji) jako alternatywy dla tradycyjnej,
- budowy platformy sieciowej do zarządzania informacją polityczną w skali globalnej i lokalnej,
- projektowanie skutecznych procedur demokracji bezpośredniej (możliwość wypowiadania się drogą elektroniczną, e-wybory, ...),
- wykorzystania sieci do zwiększenia udziału e-obywatela w życiu politycznym – wzmocnienie społeczeństwa obywatelskiego.

Kompetencje są szerszym pojęciem od kwalifikacji. Kompetentny e-obywatel powinien mieć odpowiednie przygotowanie (wiedza, umiejętności, postawa, motywacja, odpowiedzialność) do realizacji zadań w życiu zarówno jednostki jak i ogółu społeczeństwa. Rozwój kompetencji realizowany jest na 3 poziomach (rys. 1):

- Nabycie podstawowych umiejętności w zakresie podstaw obsługi komputera, wykorzystania prostych programów użytkowych, wykorzystania Internetu.
- Nabycie umiejętności wyszukiwania informacji w globalnej sieci związanej z wiadomościami ze świata polityki, gospodarki, edukacji, zdrowia, grup zainteresowań.

- E-uczestnictwo – umiejętność świadomego korzystania z usług świadczonych on-line za pośrednictwem Internetu dotyczących różnych obszarów życia e-obywatela. Świadome korzystanie z internetowych zasobów związane jest z wiedzą na temat bezpieczeństwa w sieci i praktyką stosowania odpowiednich procedur postępowania i programów komputerowych.

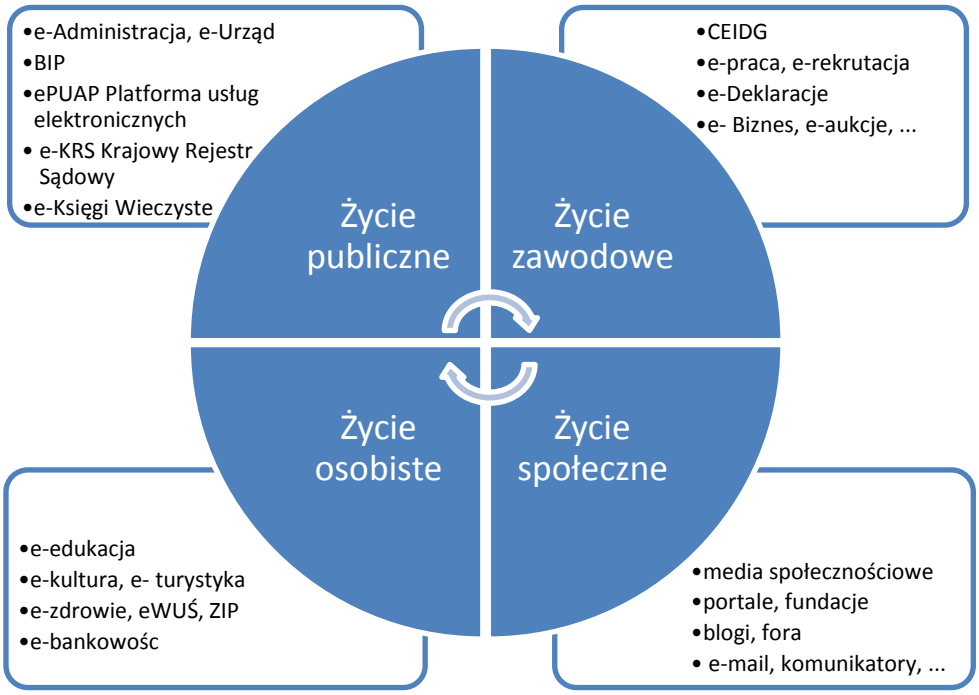
Rys. 1. Kompetencje e-Obywatela

Źródło: opracowanie własne na podstawie http://docplayer.pl/7407985-Etapy-rozwoju-e-obywatela.html

E-uczestnictwo wprowadza wartość dodaną do różnych obszarów życia modyfikując sposób realizacji różnego rodzaju potrzeb na wersję elektroniczną (rys.2).

E-Uczestnictwo wymaga odpowiedniej infrastruktury sprzętowej i programowej: powszechnego wyposażenia e-obywateli w sprzęt z dostępem do Internetu oraz wdrożonych aplikacji internetowych realizujących określone usługi internetowe.

Aktywne e-uczestnictwo w życiu publicznym umożliwiają takie aplikacje jak: ***Biuletyn Informacji Publicznej*** (BIP) do powszechnego udostępniania informacji publicznej, ***Elektroniczna Platforma Usług Administracji Publicznej*** (ePUAP) umożliwiająca załatwianie różnych spraw urzędowych przez Internet z pozycji obywatela (bezpłatny profil zaufany ePUAP potwierdzający tożsamość) oraz udostępnianie swoich usług w formie elektronicznej z pozycji podmiotów publicznych, ***Krajowy Rejestr Sądowy*** (KRS), ***Monitor Sądowy i Gospodarczy***, ***Księgi Wieczyste*** i inne.



Rys.2. Obszary życia e-Obywatela

Źródło: opracowanie własne

Prowadzenie działalności zawodowej, biznesowej zostało usprawnione za pomocą portali takich jak: ***Centralna Ewidencja i Informacja o Działalności Gospodarczej*** (CEIDG), rejestr ***REGON***, Platforma Usług Elektronicznych ZUS – ***e-Płatnik***, ***e-Deklaracje*** do składania deklaracji podatkowych. Wdrożono w życie wiele aplikacji do prowadzenia biznesu elektronicznego, zmodyfikowano formy rekrutacji pracowników i świadczenia pracy dodając drogę elektroniczną.

Prawdziwa rewolucja w życiu społecznym realizowana jest przez media społecznościowe. Zaistnienie na popularnych serwisach jak Facebook czy Twitter to być lub nie być tak dla jednostek jak i firm. Możliwość dwustronnego przekazu informacji między wybranymi grupami osób z każdego miejsca, o każdej porze, na każdy temat, zrzeszanie się obywateli, aktywność na forach internetowych, w powoływanych Fundacjach to zdobycze demokracji naszego wieku.

Możliwości zaspokojenia potrzeb osobistych drogą elektroniczną bez wychodzenia z domu realizowane są za pomocą aplikacji w obszarze ochrony zdrowia: Elektroniczna Weryfikacja Uprawnień Świadczeniobiorców (eWUŚ), Zintegrowany Informator Pacjenta (ZIP), w obszarze ubezpieczeń: Platforma Usług Elektronicznych ZUS. E-bankowość, e-edukacja, e-kultura, e-turystyka to kolejne obszary do wykorzystania przez obywatela za pomocą Internetu.

1.3. UMIEJĘTNOŚCI E-OBYWATELA

TIK z roku na rok ewoluują w kierunku nowych rozwiązań, nowych możliwości. Interaktywna technologia Web 2.0 (mechanizm Wiki, blogi, serwisy współdzielenia i wymiany plików, serwisy społecznościowe), technologie mobilne, technologie chmurowe, wirtualna rzeczywistość wymagają ciągłego dokształcania się w zakresie umiejętności ich stosowania.

Edukacja informatyczna realizowana jest na poziomie szkolnictwa podstawowego, gimnazjalnego, średniego, wyższego a także w ramach wielu programów szkoleniowych przeciwdziałających cyfrowemu wykluczeniu części społeczeństwa, głównie słabo wykształconych, mieszkańców wsi, osób w starszym wieku. Wykluczenie cyfrowe to współczesna forma wykluczenia społecznego. Wykluczenie społeczne oznacza, że "dana jednostka lub jakaś grupa społeczna będąc członkami wspólnoty (najczęściej chodzi o wspólnotę obywateli państwa) nie mogą uczestniczyć w pełni w ważnych dziedzinach życia tejże wspólnoty." ... "Wykluczenie dotyczyć może pracy, konsumpcji, uczestnictwa w kulturze, życiu społeczności lokalnych i w polityce" [PAN13]. Wykluczenie społeczne związane jest nie tylko z ubóstwem, bezrobociem, dyskryminacją społeczną ale również z brakiem możliwości i umiejętności wykorzystania TIK, wtedy określane jest terminem wykluczenia cyfrowego. W warunkach rosnącego znaczenia TIK w różnych sferach życia oraz konieczności załatwiania wielu spraw za pośrednictwem Internetu (praca, edukacja, dostęp do informacji, uczestnictwo w życiu społecznym i kulturalnym) wykluczenie cyfrowe stale rośnie.

W ramach przeciwdziałania wykluczeniu cyfrowemu podejmowanych jest szereg programów, inicjatyw na poziomie krajowym czy lokalnym, które mobilizują zagrożone grupy do pozyskania odpowiedniej wiedzy i praktycznych umiejętności z zakresu TIK warunkujących dostęp do pełnego uczestnictwa w życiu e-obywatela.

W Polsce zbudowany został nie tylko system edukacji informatycznej, ale również powstały systemy certyfikacji posiadanych umiejętności informatycznych takie jak: ***ECDL*** (*European Computer Driving Licence*) – Europejski Certyfikat Umiejętności Komputerowych wdrożony przez Polskie Towarzystwo Informatyczne, ***ECCC*** (*European Computer Competence Certificat*) – Europejski Certyfikat Kompetencji Informatycznych wdrożony przez Fundację ECCC Polska, certyfikaty ***CISCO: CCNA*** (*Cisco Certified Networking Associate*), ***CCNP*** (*Cisco Certified Networking Professional*), certyfikaty ***MCP*** (*Microsoft Certified Professional*) i inne. Certyfikaty dotyczą różnych obszarów zastosowań i poziomów. Wydaje się, że najodpowiedniejszym certyfikatem potwierdzającym minimalnie umiejętności e-obywatela są: certyfikat ECDL ***e-Citizen*** oraz certyfikaty ECCC: ***IT M1 Sprzęt i oprogramowanie komputerowe, IT M6 Technologie informacyjno-komunikacyjne.***

1.4. ŚWIADOMOŚĆ ZAGROŻEŃ W ŚWIECIE CYFROWYM

Korzystanie z TIK przez e-obywatela związane jest z wieloma korzyściami ale i z zagrożeniami.

Do korzyści jakie e-obywatel uzyskuje za pomocą TIK należą:

- dostęp do odpowiedniej informacji w dowolnym miejscu i czasie,
- otrzymywanie informacji spersonalizowanej,
- aktywna partycypacja publiczna i społeczna (bezpośrednie uczestnictwo w życiu publicznym i społecznym),
- zdalna realizacja wybranych usług drogą elektroniczną – oszczędność czasu i pieniędzy.

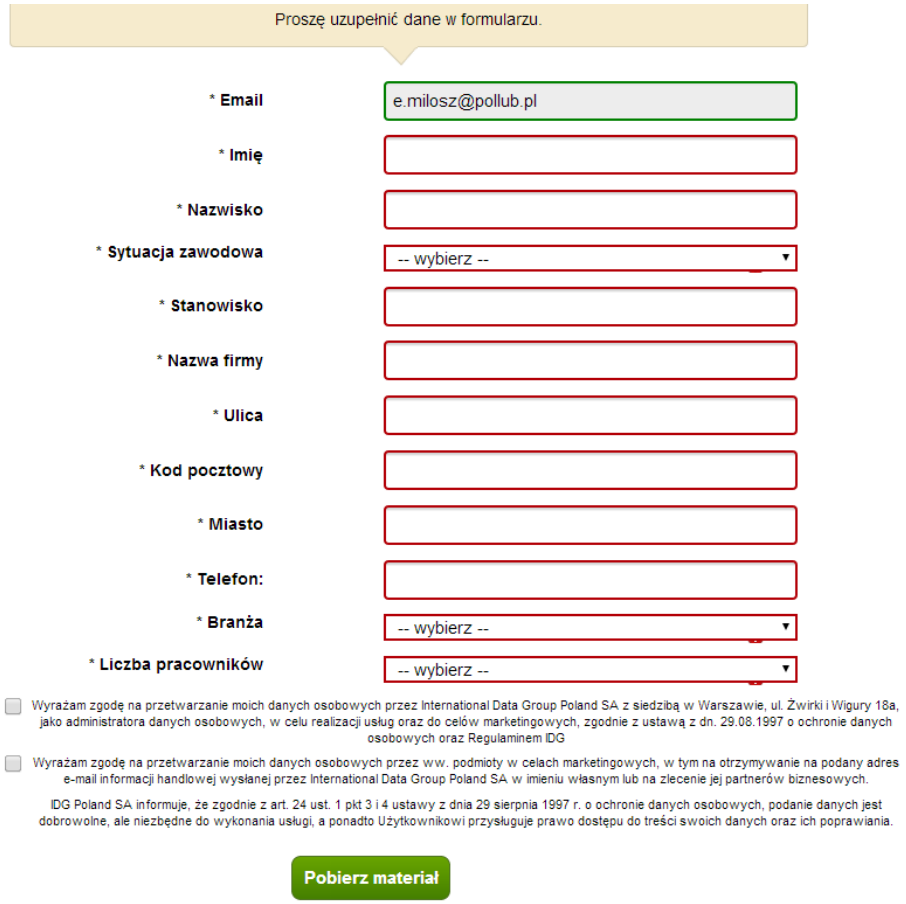
Do zagrożeń związanych w wykorzystaniem TIK można zaliczyć:

- utratę prywatności, intymności, wolności osobistej, danych osobowych,
- uzależnienie od komputera, sieci i mediów społecznościowych,

- kradzież tożsamości cyfrowej, wykorzystanie tożsamości w celu oszustwa, kradzieży, utraty dobrego imienia,
- utrata danych – własnych zasobów na komputerze.

Ochrona prywatność gwarantowana w międzynarodowych i polskich regulacjach prawnych nie zawsze respektowana jest w Internecie. Naruszeniem prywatności, rozumianej jako "osobistej przestrzeni wolnej od ingerencji innych osób oraz organizacji" [SWI13] są np. sytuacje, w których dochodzi do niechcianej ingerencji w życie prywatne, rodzinne, naruszenie integralności psychicznej jednostki, jej przekonań, honoru, wyznania, światopoglądu, naruszenie tajemnicy korespondencji, publikowanie informacji poufnych, podsłuchiwanie, śledzenie, podszywanie się pod cudzą tożsamość i działanie w złej wierze [SWI13]. Zgodnie z polską Ustawą o ochronie danych osobowych naruszeniem prywatności jest również publikowanie danych wrażliwych takich jak: pochodzenie rasowe lub etniczne, przekonania religijne, wyznanie, dane o stanie zdrowia, nałogach, życiu seksualnym, dane o skazaniach, mandatach, orzeczeniach postępowania sądowego lub administracyjnego [UOD97].

Sytuacje naruszające prywatność e-obywatela mogą mieć miejsce podczas korzystania z przeglądarek internetowych wykorzystujących mechanizmy Cookies, ActiveX bez wiedzy na temat konfiguracji przeglądarek i zabezpieczeń ciasteczek, uruchamiania niechcianych programów (spyware) szpiegujących aktywność użytkownika Internetu i wykradających poufne dane, udostępniania danych osobowych jako warunku darmowego korzystania z niektórych usług internetowych, serwisów społecznościowych (rys.3), działania złośliwego oprogramowanie wykradającego poufne dane podczas transmisji danych w sieci, korzystania z technologi GPS lokalizujących miejsce przebywania użytkownika, upubliczniania baz danych tworzonych na potrzeby określonego przedsięwzięcia oraz w innych sytuacjach.



Rys.3. Udostępnienie danych osobowych jako warunek korzystania z usługi dostępu do artykułu
Źródło: http://www.computerworld.pl/whitepaper/2521-Bezpieczenstwo.w.IT.najlepsze.metody.zapobiegania.atakom.i.reagowania.html

Sytuacje naruszające bezpieczeństwo użytkownika TIK – e-obywatela mogą mieć miejsce podczas ataków socjotechnicznych cyberprzestępców (wywieranie wpływu na użytkowniku w celu wykonania określonej czynności – link, pobranie pliku, wypełnienie formularza, podanie danych, ...), korzystania z poczty elektronicznej (otwieranie niebezpiecznych załączników), korzystania z komunikatorów, stron WWW, aplikacji internetowych, wykorzystywanie technologii chmury i w innych sytuacjach.

W Raporcie Bezpieczeństwo w Internecie (styczeń 2013) wskazano 10 głównych zagrożeń dotykających internautów (rys. 4).

Dziesięć zagrożeń, które internautów w Polsce dotykają najczęściej	
niechciane treści w serwisach społecznościowych	63 proc.
utrata danych z komputera (z różnych przyczyn)	41 proc.
otrzymanie złośliwej aplikacji w serwisie społecznościowym	32 proc.
oszukańcze maile, wyłudzające informacje	31 proc.
podszywanie się, kradzież tożsamości	9 proc.
włamanie do komputera bez kradzieży danych	9 proc.
ujawnienie hasła do konta e-mail	8 proc.
włamanie do komputera i kradzież danych	4 proc.
próba włamania do konta bankowego	4 proc.
włamanie do konta bankowego i kradzież pieniędzy	3 proc.
źródło: Fundacja BezpieczniejwSieci.org, styczeń 2013	

Rys. 4. Najczęściej spotykane zagrożenia korzystania z Internetu wg badań Fundacji Bezpieczniejwsieci.org [RAI]

Źródło: Bezpieczeństwo w Internecie Raport, [http://www.interaktywnie.com/biznes/raporty]

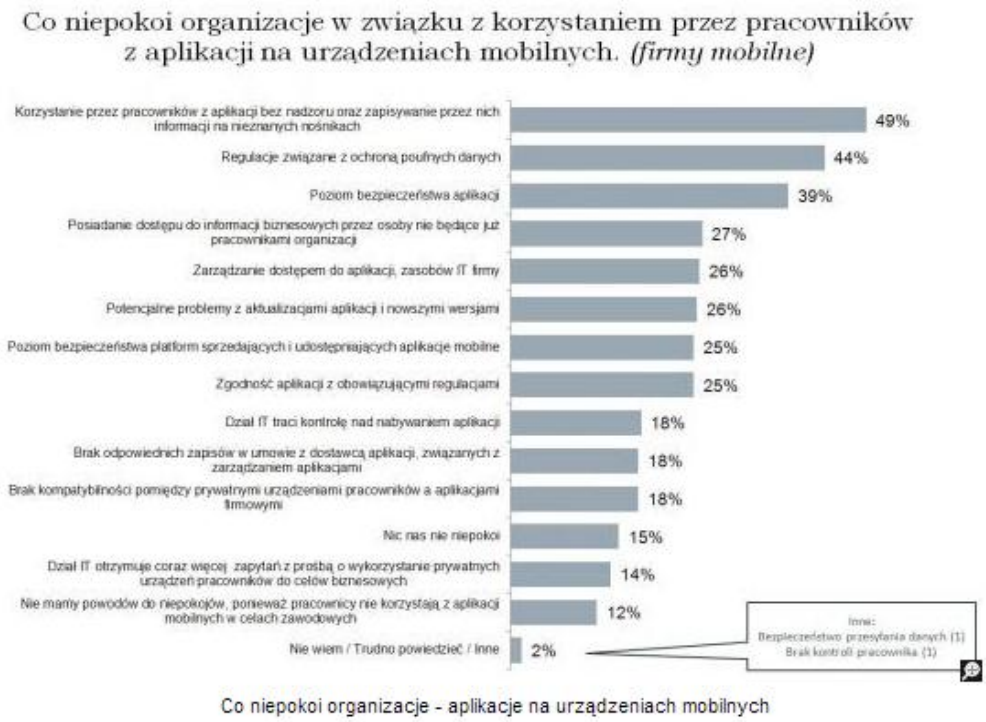
Na rynku dostępne jest oprogramowanie zaawansowanej ochrony przed złośliwym oprogramowaniem jak np. Web Security Appliance, Email Security Appliance, Cloud Web Security firmy Cisco.

W Polsce o bezpieczeństwo w Internecie dbają instytucje takie jak: Rządowy Zespół Reagowania na Incydenty Komputerowe (w zakresie bezpieczeństwa systemów i serwisów administracji publicznej http://www.cert.gov.pl), Urząd

Komunikacji Elektronicznej (w zakresie telekomunikacji http://www.uke.gov.pl) oraz Generalny Inspektor Ochrony Danych Osobowych (w zakresie prawa do ochrony danych: www.giodo.gov.pl).

Zagrożenia bezpieczeństwa nie dotyczą tylko danych osobowych e-obywatela. Jeżeli jest on osobą pracującą i wykorzystuje w pracy TIK może nieświadomie narazić firmę na utratę danych. Problem jest szczególnie istotny w sytuacjach elastycznych form zatrudnienia, pracy zdalnej oraz wykorzystywania prywatnego sprzętu mobilnego (laptop, telefon, smartfon, tablet, ...) do celów służbowych. Przenikanie się życia zawodowego z prywatnym jako trend ostatnich lat związane jest z tzw. zjawiskiem BYOD (*Bring Your Own Device*) polegającym na używaniu przez pracowników w miejscu pracy swoich prywatnych smartfonów i tabletów. Łącząc się przez firmową sieć WIFI z prywatnych urządzeń nie objętych politykami bezpieczeństwa istnieje ryzyko infekcji i wycieku danych firmowych. Z drugiej strony wykorzystywanie służbowych laptopów i smartfonów w celach prywatnych poza firmą związane jest z możliwością kradzieży, zgubienia, czy wycieku danych ze służbowego sprzętu.

Badania zjawiska BYOD przez Computerworld w 2013 r. wykazały, że największym problemem pracodawców jest korzystanie przez pracowników z aplikacji bez nadzoru oraz zapisywanie przez nich informacji na nieznanych nośnikach (rys. 5). Tylko 38% zagranicznych firm (a 13 % polskich firm) pozwala na korzystanie z prywatnych urządzeń pracowników do wykonywania obowiązków zawodowych, a tylko 20% zagranicznych firm (a 4 % polskich firm) zamierza wdrożyć politykę BYOD w najbliższym roku [COM].



Rys. 5. Problemy wykorzystywania urządzeń mobilnych w pracy zawodowej wg badań Computerworld [COM]
Źródło: http://www.computerworld.pl/news/393282/BYOD.w.polskich.i.zagranicznych.firmach.html

1.5. PODSUMOWANIE

Technologie informacyjno-komunikacyjne zrewolucjonizowały codzienne życie e-obywateli dając wiele możliwości aktywnego życia publicznego, zawodowego, społecznego i osobistego. Nabycie i ciągłe doskonalenia kompetencji e-obywatela warunkują świadome i bezpieczne korzystanie z dobrodziejstw komputera i Internetu. Problemy wykorzystania TIK w życiu publicznym, zawodowym, społecznym i osobistym wymagają kompleksowych rozwiązań.

2

Wybrane problemy zarządzania ochroną informacji w przedsiębiorstwie

„Na przestrzeni kilku najbliższych lat w większości przedsiębiorstw i instytucji publicznych świadomość bezpieczeństwa i wartości informacji znacząco wzrośnie. […] Do całkowitego zabezpieczenia się przed stratami spowodowanymi utratą informacji niezbędne jest także systematyczne podnoszenie kwalifikacji administratorów IT, jak i szeregowych pracowników”[2]

2.1. WSTĘP

Ochrona informacji w firmie, staje się obecnie kluczowym zadaniem wszystkich pracowników, w tym przede wszystkim menedżerów. Od odpowiedniego zabezpieczenia danych, bardzo często zależy bowiem kondycja ekonomiczno-społeczna danego przedsiębiorstwa. Z przeprowadzonych w lipcu 2013 r. przez firmę Intel badań[3] wynika, że dane przechowywane w ponad połowie firmowych laptopów, które trafiły w niepowołane ręce, nie były w żaden sposób zabezpieczone. Największy odsetek zanotowano na Węgrzech (58,6%) i Słowacji (55,3%), niższy w Czechach (52%) i Polsce (45%).

---

[2] Marcin Sobaniec, ekspert HSM Polska – http://www.callcenternews.pl/2014/09/26/co-trzecia-firma-zwiekszy-budzet-na-ochrone-informacji [17.10.2014].

[3] Na zlecenie firmy Intel w lipcu 2013, przebadano 726 firm zatrudniających ponad 100 pracowników, w tym 144 firmy czeskie, 329 firm węgierskich, 139 firm polskich i 114 firm *słowackich*. http://www.biznes.newseria.pl/komunikaty/firma/intel_polacy_najwiecej,b1390747873 [05.11.2014].

Co więcej, firmy zdają sobie sprawę z zagrożeń związanych z utratą danych, a mimo to nie podejmują wystarczających kroków, aby je zabezpieczyć. Prawie wszystkie firmy przyznały również, że utrata danych była dla nich bardziej dotkliwa niż utrata sprzętu. Koszt utraconego sprzętu wynosił przeciętnie ok. 1 200 euro, natomiast poziom strat związanych z utratą danych to średnio 7 082 euro. Spośród badanych państw, szacowana wysokość strat jest najwyższa w Polsce (7 739 euro), następnie w Czechach (7 333 euro), na Węgrzech (7 259 euro), a najniższa na Słowacji (6 000 euro). W podanych kwotach uwzględniono, poza utraconymi danymi, również koszty związane z prawami do własności intelektualnej oraz utratę efektów pracy, a także czas poświęcony przez pracowników firmy lub zewnętrznych specjalistów na zaradzenie sytuacji. Badania wskazują również, że średnie łączne straty (poza Słowacją) spowodowane pojedynczą kradzieżą przekroczyły sumę 8000 euro. Należy zatem przyjrzeć się najważniejszym problemom związanym z zarządzaniem bezpieczeństwem informacji w przedsiębiorstwach.

2.2. OCHRONA BEZPIECZEŃSTWO INFORMACJI W FIRMIE

Informacja to termin interdyscyplinarny, który z łaciny oznacza *„informatio" – przedstawienie, wizerunek lub „informare" – kształtować, przedstawiać*. Jest on definiowany bardzo szeroko w zależności od dziedziny naukowej. Najogólniej oznacza on właściwość pewnych obiektów, relację między elementami zbiorów pewnych obiektów, której istotą jest zmniejszanie niepewności.[4] Inaczej mówiąc, informacja to dane przetworzone w taki sposób, że na ich podstawie można wyciągać wnioski lub podejmować decyzje biznesowe.

Informacja jest istotnym składnikiem aktywów o charakterze niematerialnym i ma kluczowe znaczenie dla przedsiębiorstwa, stąd szczególna dbałość o jej ochronę. Podobnie, jak inne wartości, informacja podlega działaniom rynkowym (można ją kupić, sprzedać, wymienić) dzięki którym firmy prowadzą określone interesy i osiągają różne korzyści.

---

[4] Lissowski G., hasło Informacja, [w:] Wielka Encyklopedia Powszechna, 2002, s.126.

Brak należytego zabezpieczenia przed niezamierzonym udostępnieniem może spowodować:[5]

- utratę korzyści finansowych,
- utratę konkurencyjności,
- nieprofesjonalny, a więc negatywny wizerunek firmy.

Tak więc, podejmowanie przez przedsiębiorstwo zabiegów, których celem jest zabezpieczenie danych, należy obecnie do jednych z ważniejszych zadań. Nie wolno jednak zapominać, że jest to proces ciągły i dynamiczny. A to z kolei, oznacza stałe monitorowanie polityki ochrony i udostępniania danych.

R. Borowiecki i M. Kwieciński twierdzą, że bezpieczeństwo informacji to „*obrona informacyjna, która polega na uniemożliwieniu i utrudnieniu zdobywania danych o fizycznej naturze aktualnego i planowanego stanu rzeczy i zjawisk we własnej przestrzeni funkcjonowania oraz utrudnianiu wnoszenia entropii informacyjnej do komunikatów i destrukcji fizycznej do nośników danych*”.[6]

Można je również tłumaczyć jako działania zmierzające do unikania niepewności i ryzyk biznesowych. Jest to ponadto wypadkowa bezpieczeństwa fizycznego, prawnego, organizacyjnego oraz teleinformatycznego przedsiębiorstwa.[7]

W szerokim rozumieniu bezpieczeństwo informacyjne oznacza stan wolny od zagrożeń, którymi mogą być:

- przekazywanie informacji nieuprawnionym podmiotom,
- szpiegostwo,
- działalność dywersyjna lub sabotażowa.[8]

---

[5] http://www.ksoin.pl/bezpieczenstwo_informacji_w_firmie-strony,11,381.html#.VEoNRxb3WM8.

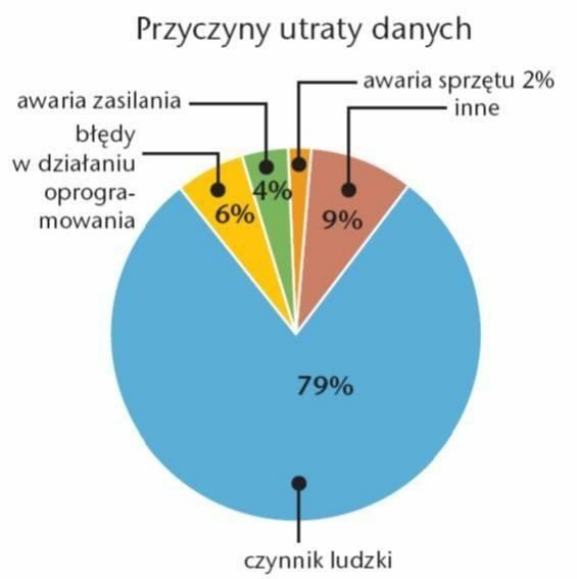
[6] Borowiecki R., Kwieciński M., Monitorowanie otoczenia, przepływ i bezpieczeństwo informacji. W stronę integralności przedsiębiorstwa, Zakamycze 2003.

[7] Łuczak J. (red.), Zarządzanie bezpieczeństwem informacji, Oficyna Współczesna, Poznań 2004, s. 80.

[8] Jabłoński M., Mielus M., Zagrożenia bezpieczeństwa informacji w przedsiębiorstwie. Część 1, Zabezpieczenia 1/2009. http://www.zabezpieczenia.com.pl/ochrona-informacji/zagrozenia-bezpieczenstwa-informacji-w-przedsiebiorstwie-czesc-1, [12.12.2014].

Główne zagrożenia związane z ochroną informacji

Liczba nagannych zachowań związanych z ujawnianiem informacji w przedsiębiorstwach stale rośnie, ale też zmienia się ich rodzaj i sposób postępowania.[9] Można wskazać kilka głównych przyczyn utraty danych (wykres 1).



Wykres 1. Główne przyczyny utraty danych w przedsiębiorstwach
Źródło: http://www.ksoin.pl/bezpieczenstwo_informacji_w_firmie-strony,11,381.html#.VEoNRxb3WM8

Wśród nich największy odsetek (ponad ¾) stanowi tzw. czynnik ludzki. Pozostałe przyczyny to np. awaria sprzętu, awaria w zasilaniu czy błędy w oprogramowaniu. Tak więc, jednym z największych zagrożeń występujących w ochronie informacji przedsiębiorstwa są sami ludzie, czyli pracownicy, współpracownicy i klienci. To oni bowiem mają najszerszy dostęp do informacji i to ich działania mogą przynieść najwięcej strat.

[9] Tamże.

Według CERT Polska, liczba ataków zewnętrznych i wewnętrznych w firmach, systematycznie wzrasta. Do zewnętrznych można zaliczyć np. powstawanie nowych, nieznanych firm komercyjnych, które próbują nielegalnie pozyskać informacje oraz takich, które przechowują i udostępniają nielegalne materiały, chroniąc tożsamość swoich użytkowników.[10] Z kolei do wewnętrznych można zaliczyć dosyć starą, ale skuteczną metodę – przeszukiwanie śmieci.[11]

Sporo niebezpieczeństw niesie rozwój systemów teleinformatycznych, które same w sobie ułatwiają i przyśpieszają pracę oraz komunikację. Ale też mogą podlegać niepożądanym działaniom ze strony każdego, kto posiada dostateczny zasób wiedzy i umiejętności. Wśród nich wskazać można:[12]

- niszczenie informacji,
- fałszerstwa danych,
- podsłuch,
- sabotaż,
- piractwo,
- wandalizm,
- *hacking,*
- *cracking*,
- kradzież tożsamości,
- szpiegowanie,
- wirusowanie.

W celu zapewnienia odpowiedniej ochrony systemów informatycznych stosuje się różne poziomy ich zabezpieczenia (tabela 1).

[10] http://www.cert.pl/PDF/Raport_CP_2007.pdf [za:] Jabłoński M., Mielus M., Zagrożenia bezpieczeństwa…, op. cit.

[11] Łuczak J. (red.), Zarządzanie bezpieczeństwem informacji, Oficyna Współczesna, Poznań 2004, s. 45.

[12] Bączek P., *Zagrożenia informacyjne a bezpieczeństwo państwa polskiego,* Wydawnictwo Adam Marszałek, Toruń 2006, s. 30.

Tabela 1. Odpowiednia hierarchia ochrony systemów informatycznych

ICT Przedmioty ochrony	Poufność danych Kontrola dostępu Uwierzytelnianie Niezaprzeczalność Integralność danych
ICT Mechanizmy ochronne	Szyfrowanie Ochrona ruchu Wymiana uwierzytelnień Sterowanie rutingiem Uwierzytelnienie Mechanizmy sterowania dostępem Podpisy cyfrowe Mechanizmy integralności danych
ICT Rozwiązania ochrony	Zapory ogniowe Filtrowanie zawartości Systemy antywirusowe Wykrywanie włamań Zarządzanie prawami do zawartości cyfrowej Kontrola dostępu Ocena podatności na ataki Zarządzanie zagrożeniami Rozwiązania identyfikacyjne Infrastruktura klucza publicznego Rozwiązania szyfrujące

Źródło: http://itpedia.pl/index.php/Ochrona_informacji_w_sieci_przedsi%C4%99biorstwa [10.12.2014]

Ważnym zadaniem dla firm jest zapewnienie tajności, spójności i niezawodności działań związanych z posiadaniem i przekazywaniem danych wyłącznie uprawnionym osobom. Wymienia się pięć obszarów zagrożeń dla systemów komputerowych:

- kwalifikacje i wiarygodność personelu,
- centra administracyjne systemu i sieci,
- infrastruktura telekomunikacyjna,
- produkcja sprzętu i oprogramowania,
- procedury korzystania z systemów i sieci informatycznych,
- nośniki danych.[13]

Prowadzenie polityki bezpieczeństwa informacyjnego powinno być zatem powiązane z innymi procesami zarządzania firmą, tak by nie utrudniać lub całkowicie paraliżować funkcjonowania w innych obszarach.

[13] Żebrowski A., Kwiatkowski M., *Bezpieczeństwo informacji III Rzeczypospolitej*, Oficyna Wydawnicza Abrys, Kraków 2000, s. 64.

2.3. WYBRANE NARZĘDZIA DO ZARZĄDZANIA OCHRONĄ INFORMACJI W PRZEDSIĘBIORSTWIE

Ochrona informacji w przedsiębiorstwie często napotyka na szereg trudności, wśród których można wskazać:[14]

- wysoki koszt stosowania wielu rozwiązań ochronnych,
- brak świadomości kadry pracowniczej i menedżerskiej,
- brak zasobów wewnętrznych monitorujących i informujących o naruszeniach i przekroczeniach bezpieczeństwa,
- znacznie większa złożoność systemu informatycznego posiadającego rozwiązania ochronne.

Poprawie bezpieczeństwa informacyjnego firmy mogą służyć odpowiednie narzędzia, takie jak:

- ISO 27001,
- oraz DIN 66399.

2.3.1. SYSTEM ISO 27001 JAKO ISTOTNY ELEMENT POLITYKI OCHRONY DANYCH

System zarządzania bezpieczeństwem informacji (SZBI) według ISO/IEC 27001 to norma międzynarodowa, która określa wymagania dotyczącego tego systemu, cele stosowania zabezpieczeń oraz zabezpieczenia, które powinny być zastosowane jako część SZBI. System ten konstytuuje politykę ochrony informacji w firmie na trzech głównych filarach:[15]

- poufności, czyli zapewnieniu, dostępu tylko dla osób uprawnionych,
- integralności, czyli zagwarantowaniu dokładności i kompletności informacji oraz metod ich przetwarzania,
- dostępności, czyli zapewnieniu upoważnionym użytkownikom dostępu do informacji i związanych z nimi zasobów, zgodnie z określonymi potrzebami.

[14] http://itpedia.pl/index.php/Ochrona_informacji_w_sieci_przedsi%C4%99biorstwa [14.11.2014].

[15] http://www.iso.org.pl/iso-27001 [12.12.2014].

Norma ISO 27001 składa się z części podstawowej oraz załączników. Część podstawowa normy określa definiuje wymagania związane z:

- ustanowieniem i zarządzaniem SZBI,
- wymaganą dokumentacją,
- odpowiedzialnością kierownictwa,
- wewnętrznymi audytami i przeglądami SZBI,
- oraz ciągłym doskonaleniem SZBI.

Wszystkie wymagania zdefiniowane w części podstawowej powinny być spełnione. Podstawą ustanowienia oraz utrzymania SZBI jest określenie metody oraz przeprowadzenie analizy ryzyka.

Z kolei załącznik A do normy definiuje wymagania w obszarach:

- polityka bezpieczeństwa informacji,
- organizacja bezpieczeństwa informacji,
- zarządzanie aktywami,
- bezpieczeństwo osobowego,
- bezpieczeństwo fizyczne i środowiskowe,
- zarządzanie systemami i sieciami,
- kontrola dostępu,
- uzyskiwanie, rozwój i utrzymanie systemów informacyjnych,
- zarządzanie incydentami związanymi z bezpieczeństwem informacji,
- zarządzanie ciągłością działania,
- zgodność z wymaganiami prawnymi i własnymi standardami.

Zrealizowanie wszystkich wymienionych wyżej wymagań oznacza wdrożenie systemu ISO 27001.Istotną rolę w procesie kształtowania polityki bezpieczeństwa informacyjnego przedsiębiorstwa na podstawie normy ISO 27001 odgrywa kierownictwo firmy, które przez swoją świadomość i wyrażoną postawę daje jasny sygnał pozostałym pracownikom. Przejawia się to przez:[16]

- wskazanie aktualnych luk bezpieczeństwa,
- wskazanie zagrożeń dla bezpieczeństwa informacji,

[16] http://manager.nf.pl/czyli-bezpieczenstwo-informacji-w-firmie-iso-iec-27001,3,43303,55, [12.12,2014].

- wskazanie praktycznych zabezpieczeń,
- uświadomienie ewentualnych zysków i strat,
- pokazanie, że odpowiedzialnie są chronione informacje należące do klientów.

Wśród korzyści wynikających z wdrożenia systemu zarządzania bezpieczeństwem informacji wg ISO 27001:2013 wskazuje się na:

- obniżenie ryzyka utraty bezpieczeństwa, co w konsekwencji powoduje zmniejszenie ryzyka biznesowego,
- podniesienie wiarygodności organizacji i zaufania do jej działań,
- poprawę reputacji firmy, jako profesjonalnej i odpowiedzialnej,
- pozyskanie nowych rynków i klientów,
- zapewnienie, że spełnione są wymogi prawne, do których przestrzegania zobowiązana jest organizacja,
- sformalizowany i przewidywalny sposób zarządzania bezpieczeństwem informacji,
- możliwość obiektywnej oceny przeprowadzanych procesów,
- stały nadzór – który daje gwarancję, że system zarządzania bezpieczeństwem informacji jest właściwie utrzymywany i zgodny z wymaganiami.[17]

2.3.2. NORMA DIN 66399 JAKO SKUTECZNE NARZĘDZIE DO UTYLIZACJI NOŚNIKÓW INFORMACJI[18]

Innym ciekawym rozwiązaniem stosowanym w celu ochrony informacji przedsiębiorstw jest obowiązująca od października 2012 norma DIN 66399. Stale jednak brakuje pełnej wiedzy firmach, na temat zastosowania elementarnych zasad bezpieczeństwa informacji w codziennym życiu. Norma DIN 66399[19] skierowana do osób odpowiedzialnych za ochronę danych oraz osób zaangażowanych w proces niszczenia danych. Określa ona wymagania dla procesów niszczenia oraz poszcze-

[17] Tamże.

[18] http://www.callcenternews.pl/2014/09/26/co-trzecia-firma-zwiekszy-budzet-na-ochrone-informacji, [12.12.2014].

[19] www.din66399.pl [12.12.2014].

gólnych jego etapów. Norma definiuje trzy różne metody w zakresie niszczenia nośników danych. Każda z nich wymaga zdefiniowania i udokumentowania organizacji, personelu oraz poszczególnych etapów procesów. Często wyciek poufnych informacji to efekt niewiedzy lub zwykłego niedbalstwa osób, które mają z nimi do czynienia. Dlatego warto edukować pracowników w kwestii bezpieczeństwa danych. Poufne i tajne dokumenty zapisane na nośnikach optycznych, magnetycznych czy elektronicznych podlegają takiej samej ochronie, jak informacje zapisane na papierze. Z racji ilości zapisanych na nich danych, winny podlegać szczególnej ochronie. Po ich zdezaktualizowaniu należy je zniszczyć za pomocą odpowiedniej, gwarantującej pewność i bezpieczeństwo technologii. Należy także ograniczyć możliwość wypływu tego typu nośników poza struktury firmy. Niszczenie elektronicznie przechowywanych danych bezpośrednio w miejscu ich powstawania jest najlepszym sposobem zapewnienia bezpieczeństwa. Dzięki temu mamy większą pewność, że wrażliwe informacje nie wycieką. Trzeba pamiętać o tym, że zlecanie tego zadania podmiotom zewnętrznym zawsze wiąże się z ryzykiem ingerencji osób trzecich.

2.4. TWORZENIE TAJEMNICY PRZEDSIĘBIORSTWA

Polityka ochrony informacji w przedsiębiorstwie oparta jest na tworzeniu tajemnicy.

Nie jest to proces skomplikowany, ale wymaga określenia zasad i sposobów ich stosowania. Największy problem stanowi jednak przestrzeganie procedury ochrony informacji przez wszystkich pracowników. Według praktyka R. Solgi, utworzenie tajemnicy przedsiębiorstwa można rozbić na następujące etapy:[20]

Etap I. Identyfikacja – ma ona celu zweryfikowanie posiadanych danych i określenie ich znaczenia gospodarczego. Umożliwi to tym samym, wskazanie przewagi konkurencyjnej przedsiębiorstwa. Etap ten zakłada:

1. Ochronę informacji będącej w dyspozycji firmy w dowolnej postaci: zapisanej lub zapamiętanej.

[20] http://tajemnica-przedsiebiorstwa.pl/category/nieuczciwa-konkurencja, [14.12.2014].

2. Określenie wartości gospodarczej i nadanie statusu poufności, danym szczególnie istotnym.
3. Określenie warunków szczegółowych jej dostępności.

Etap II. Komunikacja – czyli określenie liczby osób dopuszczonych do poznania tajemnicy przedsiębiorstwa oraz sposobu jej przekazywania.

Etap III. Zabezpieczenie poufnych informacji – w postaci zastosowanych rozwiązań prawnych i fizycznych. Wśród nich mogą być np.: osobiste hasła do komputerów, hasła do ważnych dokumentów, oznaczanie dokumentów klauzulą „tajemnica przedsiębiorstwa", trzymanie najważniejszych dokumentów odpowiednich skrytkach i sejfach, oświadczenia lub umowy o zachowaniu poufności, umowy o zachowaniu poufności (NDA) i zakazie konkurencji oraz określenie procedur dodatkowych, które będzie można zastosować w niezamierzonych sytuacjach, jak np. nagłe zwolnienie się pracownika.

Etap IV. Cykliczne szkolenie pracowników – które ma na celu uświadomienie celu oraz istoty ochrony tajemnicy przedsiębiorstwa. Ponadto, informowanie o możliwych negatywnych skutkach (bezpośrednich i pośrednich) wynikających z wykorzystania przez konkurencję poufnych informacji. Świadomość, wiedza oraz odpowiednia postawa pracowników stanowią kluczowe elementy polityki bezpieczeństwa informacyjnego firmy.

W oparciu o powyższe wskazówki, menedżerowie oraz odpowiednie komórki mogą samodzielnie określić politykę ochrony danych w przedsiębiorstwie.

2.5. SAMODZIELNE KSZTAŁTOWANIE PRAWIDŁOWEJ POLITYKI BEZPIECZEŃSTWA INFORMACYJNEGO

Chcąc prawidłowo sprecyzować politykę ochrony danych trzeba najpierw określić czy chodzi o całościową politykę bezpieczeństwa przedsiębiorstwa, politykę w rozumieniu Ustawy o Ochronie Danych Osobowych, czy też może politykę dotyczącą stosowanych systemów i rozwiązań informatycznych. Ustalenie tego będzie miało wpływ na ostateczny kształt polityki bezpieczeństwa firmy, która znajdzie swoje odzwierciedlenie w formalnym dokumencie.

Poniżej zaprezentowana zostanie przykładowa polityka bezpieczeństwa informacyjnego firmy w obszarze IT przedstawiona w formie dokumentu:

Lp.	Określenie procedury	Opis procedury
Krok 1	Zdefiniowanie bezpieczeństwa informacyjnego firmy	W oparciu o następujące wartości: • Poufności informacji – zakaz dostępu dla osób trzecich. • Integralności informacji – w celu uniknięcia wprowadzania nieautoryzowanych zmian w danych. • Dostępności informacji – w każdym momencie żądanym przez użytkownika. • Sprawdzalności operacji – zachowanie pełnej historii dostępu do danych, wraz z informacją kto taki dostęp uzyskał.
Krok 2	Oznaczanie danych podlegających szczególnej ochronie	Czyli: • informacje o realizowanych kontraktach (planowanych, bieżących i zrealizowanych), • informacje finansowe firmy, • informacje organizacyjne, • dane dostępowe do systemów IT, • dane osobowe, • informacje stanowiące o przewadze konkurencyjnej firmy, • inne informacje oznaczone jako „informacji poufne” lub „dane poufne”.
Krok 3	Zasada minimalnych uprawnień	Przydzielanie pracownikom tylko takich uprawnień, które są konieczne do wykonywania pracy na danym stanowisku.
Krok 4	Zasada wielowarst-wowych zabezpieczeń	Równoległa ochrona systemu IT przedsiębiorstwa na wielu poziomach.
Krok 5	Zasada ograniczania dostępu	Przyznawanie odpowiednich uprawnień przez administratora w uzasadnionych przypadkach.

Krok 6	Dostęp do danych poufnych na stacjach PC	Udostepnienie oddzielnych serwerów do umieszczania danych poufnych. Odnotowywanie dostępu do tych danych. Określenie w oddzielnym dokumencie listy systemów objętych tego typu działaniami. Stosowanie dodatkowych zabezpieczeń np. w postaci szyfrowania dysku twardego w komputerach przenośnych. Stosowanie kanału szyfrowanego w celu dostępu do danych poufnych.
Krok 7	Zabezpieczenie stacji roboczych	Ochrona przed nieautoryzowanym dostępem osób trzecich. Stosowanie minimalnych środków ochrony w postaci: • systemów firewall oraz antywirus, • aktualizacji systemu operacyjnego oraz jego składników, • konieczności podania hasła przed uzyskaniem dostępu do stacji, • niepozostawiania bez nadzoru niezablokowanych stacji PC, • bieżącej pracy z wykorzystaniem konta nieposiadającego uprawnień administracyjnych.
Krok 8	Wykorzystanie haseł	Obowiązkowa, okresowa zmiana haseł. Przechowywanie haseł w formie zaszyfrowanej. Tworzenie skomplikowanych, trudnych do zapamiętania haseł.
Krok 9	Odpowiedzialność pracowników za dane poufne	Obowiązek odpowiadania przez pracowników za utrzymanie w tajemnicy powierzonych, poufnych danych.

Krok 10	Monitoring bezpieczeństwa	Stały monitoring (zgodnie z obowiązującym prawem) infrastruktury informatycznej, obejmujący następujące elementy: • analizę wykorzystywanego oprogramowania, • analizę stacji roboczych pod względem stosowania nielegalnego oprogramowania / plików multimedialnych oraz innych elementów naruszających prawa autorskie, • analizę odwiedzanych stron www, • analizę godzin pracy na stanowiskach komputerowych, • analizę wszelakich dostępów, • analizę ruchu sieciowego pod względem komunikacji, szkodliwej dla bezpieczeństwa danych firmy.
Krok 11	Edukacja pracowników w zakresie bezpieczeństwa	Okresowa edukacja pracowników w zakresie bezpieczeństwa informacji.
Krok 12	Odpowiedzialność pracowników za dane dostępowe do systemów	Nałożenie na pracowników obowiązku ochrony swoich danych dostępowych do systemów informatycznych.
Krok 13	Transport danych poufnych przez pracowników	Zakaz przenoszenia niezabezpieczonych danych poufnych poza teren Firmy.
Krok 14	Korzystanie z firmowej infrastruktury IT w celach prywatnych	Zakaz korzystania z firmowej infrastruktury IT w celach prywatnych
Krok 15	Sieć lokalna (LAN)	Odpowiednia ochrona lokalnej sieci przed nieuprawnionym dostępem przez: • odseparowanie sieci klienckich od ważnych serwerów, • nieaktywne publiczne gniazda sieciowe, • brak dostępu do sieci dla osób trzecich,

Krok 16	Systemy IT / serwery	Odpowiednie zabezpieczenie systemów IT.
Krok 17	Dokumentowanie bezpieczeństwa	Prowadzenie bieżącej dokumentacji w zakresie: • aktualnie wykorzystywanych metod zabezpieczeń, • budowy sieci IT, • ewentualnych naruszeń bezpieczeństwa systemów IT, • dostępów do zbiorów danych / systemów udzielonych pracownikom.
Krok 18	Dane osobowe	Opracowanie, w postaci osobnego dokumentu, szczegółowych wytycznych dotyczące przetwarzania danych osobowych.
Krok 19	Publiczne udostępnianie infrastruktury IT	Szczególne zabezpieczenie infrastruktury udostępnionej publicznie, np. przez: • separację od sieci LAN, • wykonanie hardeningu systemu • wewnętrzną lub zewnętrzną weryfikację bezpieczeństwa systemu (np. poprzez realizację testów penetracyjnych).
Krok 20	Kopie zapasowe	Archiwizowanie wszystkich istotnych danych (zwłaszcza poufnych) na wypadek awarii w firmowej infrastrukturze informatycznej. Odpowiednie przechowywanie nośników z kopiami zapasowymi w miejscu uniemożliwiającym dostęp osobom nieupoważnionym. Okresowo testowanie kopii zapasowych w celu sprawdzenia ich odtwarzalności.
Krok 21	Dostęp do systemów IT po rozwiązaniu umowy o pracę	Pozbawiania wszelkich dostępów w systemach informatycznych odchodzących pracowników.

Krok 22	Naruszenie bezpieczeństwa	Zgłaszanie wszelkich podejrzeń dotyczących naruszenia bezpieczeństwa. Odnotowywanie w odpowiedniej bazie danych takich incydentów i stosowanie przewidzianych kroków zaradczych.
Krok 23	Weryfikacja przestrzegania polityki bezpieczeństwa	Przeprowadzanie przez kierownictwo firmy okresowych audytów wewnętrznych lub zewnętrznych, mających na celu wykrycie ewentualnych uchybień w realizacji założeń polityki bezpieczeństwa.

Źródło: Opracowanie własne na podstawie http://www.securitum.pl/baza-wiedzy/publikacje/przykladowa-polityka-bezpieczenstwa [10.12.2014]

2.6. ZAKOŃCZENIE

Informacja, w każdej postaci ma zasadnicze znaczenie w podejmowaniu działań, a pośrednio decyduje o przetrwaniu organizacji. Tworzone obecnie systemy informatyczne mają za zadanie wspieranie decyzji i działań biznesowych. Przez to dostęp do informacji staje się łatwiejszy i mniej chroniony. Rodzi to również szereg zachowań patologicznych, takich jak kradzieże, zniszczenia czy też celowe usunięcie danych.

Prawidłowe zarządzanie ochroną informacji obejmuje oczywiście zabezpieczenia fizyczne i informatyczne, ale również uwzględnia odpowiednie przygotowanie pracowników do obchodzenia się z dostępnymi danymi.

Podsumowaniem omówionych, wybranych problemów niech będą słowa M. Sobańca, jednego z ekspertów ds. ochrony informacji:

„Polskie firmy, aby sprostać coraz bardziej wyśrubowanym standardom stawianym przez rynek będą musiały zacząć wdrażać nowoczesne normy bezpieczeństwa. Mimo tego, że coraz częściej mówi się o końcu papierologii w biznesie, to nadal, aż 43% całej dokumentacji funkcjonuje w tradycyjnej papierowej formie. Z badań wynika, że co czwarty wyciek danych odbywa się za pośrednictwem nośników papierowych. Przez brak znajomości podstawowych norm bezpieczeństwa i niedbalstwo, potencjalnym źródłem zagrożenia są także sami pracownicy. Blisko 21% pracodawców widzi zagrożenie dla bezpieczeństwa informacji wewnątrz organizacji, a 33% organizacji

deklaruje chęć zwiększenia budżetu związanego z ochroną informacji w przyszłości. Z naszego doświadczenia wynika, że im mniej osób zaangażowanych jest w proces utylizacji poufnych danych, tym mniejsze prawdopodobieństwo wycieku. Ponad 53% badanych uważa, że systemy bezpieczeństwa w ich organizacjach są na średnim poziomie, a 2/3 badanych przedsiębiorców przyznaje, że wyciek informacji może skutkować dużymi stratami finansowymi dla ich organizacji. Outsourcing w przypadku bezpieczeństwa informacji też nie jest dobrym rozwiązaniem, ponieważ wymusza ingerencję osób trzecich. Najlepszym sposobem na zabezpieczenie się przed wyciekami informacji, a tym samym przed ryzykiem poważnych strat jest [odpowiednia – przyp. włas.] utylizacja nośników informacji […].[21]

[21] http://www.callcenternews.pl/2014/09/26/co-trzecia-firma-zwiekszy-budzet-na-ochrone-informacji/, [14.12.2014].

3

Profesjonalizm i odpowiedzialność w zawodzie informatyka

3.1. WSTĘP

Współczesny człowiek żyje niewątpliwie w interesujących i ważnych czasach, gdyż to na jego oczach dokonują się postępowe zmiany nie tylko społeczno-gospodarcze, ale przede wszystkim w technice, technologiach elektronicznych i teleinformacyjnych, o których jeszcze pół wieku temu nie mówiono. Ich błyskawiczny i burzliwy rozwój w bardzo szybkim tempie zmienia świat w kierunku gospodarki elektronicznej i społeczeństwa informacyjnego, wpływając na nasze codzienne życie czy tego chcemy czy nie. Zmiany te, chociaż nie zawsze jesteśmy w stanie dostrzec, dokonują się już nie pokoleniowo czy dekadowo, ale niemalże z roku na rok. Najbardziej dostrzegane są w sprzęcie komputerowym, telefonach komórkowych, Internecie i portalach społecznościowych. Technologie, sprzęt, urządzenia, które jeszcze rok czy dwa lata temu były aktualne, dzisiaj albo już nie obowiązują albo są przestarzałe. I z tą intensywną zmiennością musi sobie radzić informatyk.

Ciągły rozwój branży informatycznej, rodzi potrzebę powstawania coraz to nowych specjalności i zapotrzebowania na pracowników w tej branży. Jak podaje raport Komisji Europejskiej „E-skills for job in Europe" popyt na informatyków przewyższa podaż – roczne tempo wzrostu popytu wynosi około 4%. Urzędnicy

europejscy szacują, że w 2020 roku na rynku pracy zapotrzebowanie pracowników z umiejętnościami cyfrowymi, może sięgać około 1 miliona[22]. Nic też dziwnego, że wraz z popytem profesji informatyka, wzrasta również ich rola i znaczenie w gospodarce.

3.2. KIM JEST INFORMATYK

Nasze społeczeństwo osobę informatyka najczęściej postrzega przez pryzmat „lekarza" od komputerów, który zna się na sprzęcie komputerowym, programach informatycznych oraz systemach operacyjnych, a co najważniejsze swoją ogromną wiedzę potrafi zastosować w praktyce. Przez wielu, jego osoba wyobrażana jest jako mały, przygarbiony człowiek w okularach, w rozciągniętym swetrze, spędzający 24 godziny przed monitorem komputera. Samotnik żyjący w swoim własnym świecie i stroniący od towarzystwa „normalnych" ludzi. Czy ten stereotyp wizerunku informatyka ma wiele wspólnego z rzeczywistością?

Informatyk to osoba posiadająca wiedzę i umiejętności, nabyte podczas kształcenia na specjalistę w dziedzinie nauk komputerowych dotyczących metod tworzenia, przetwarzania i przekazu informacji, znający budowę i zasady działania urządzeń komputerowych, a także potrafiący tworzyć, przekształcać i przekazywać dane za pomocą programów komputerowych, przy wykorzystaniu umieszczonych w nich informacji do określonych zadań[23].

Profesja informatyka jest stosunkowo nowa, tak samo jak jej nomenklatura. Pojęcie *informatyk* powstało, na początku lat 80-tych wraz z pojawieniem się pierwszych na szeroką skalę komputerów. Popularyzacja w latach 90-tych Internetu zapoczątkowała gwałtowny rozwój w branży informatycznej trwający do dzisiaj. To pociągnęło za sobą wzrost zapotrzebowania na specjalistów z tej dziedziny.

Dzisiaj pojęcie *informatyk*, chociaż jest powszechnie używane przez społeczeństwo jako określenie osoby zawodowo zajmującej się komputerami, jest pojęciem

[22] www.biznes.newseria.pl/news/mlodzi_informatycy,p1775501207 [17.09.2014].

[23] www.pl.wikipedia.org/wiki/Informatyk [17.09.2014].

ogólnym, pod którym znajduję się duża ilość specjalności związanych z branżą informatyczną. Klasyfikacja Zawodów i Specjalności wymienia około 20 profesji informatycznych[24], różniących się miedzy sobą wykonywanymi zdaniami lub wymaganiami względem posiadanego wykształcenia do wykonywania określonych zadań. Dlatego pod pojęciem *informatyk* należy rozumieć zawody informatyczne bezpośrednio związane z informatycznymi stanowiskami pracy, którymi są min.: specjaliści ds. sieci komputerowych, baz danych, bezpieczeństwa informacji, oprogramowania oraz systemów teleinformatycznych, projektanci i konstruktorzy sprzętu informatycznego, programiści, testerzy i projektanci oprogramowania, analitycy i integratorzy systemów, administratorzy systemów komputerowych, szkoleniowcy i wdrożeniowcy, producenci sprzętu i oprogramowania, dostawcy produktów informatycznych, administratorzy systemów komputerowych, projektanci gier komputerowych[25]. Wśród wielu zróżnicowanych specjalizacji prof. Krzysztof Diks wyróżnił dwa typy profesji[26]:

- **Artystów** jako pomysłodawców i dostarczycieli nowych rozwiązań informatycznych np. tworzą wydajne i funkcjonalne wyszukiwarki internetowe, doskonalą systemy operacyjne pod kątem ich niezawodności, bezpieczeństwa, jakości i ilości usług, projektują i implementują systemy do inteligentnego analizowania i przetwarzania różnego rodzaju danych – tekstów, obrazów, dźwięków, itp.
- **Rzemieślników** dbających o bieżące funkcjonowanie sprzętu i oprogramowania w przedsiębiorstwach, w gospodarstwach domowych. Dobry rzemieślnik – informatyk – jest na wagę złota.

Na rysunku uszczegółowiono charakter pracy podanych profesji informatyka.

[24] Rozporządzenie Min. Pracy i Pol. Społ. Z 27.04.2010 r Dz.U. 2010 nr. 82 poz. 537.

[25] Cieciura M., Wybrane problemy społeczne i zawodowe informatyki, WSFiZ Warszawa, 2012, s. 187.

[26] www.perspektywy.pl/index.php?option=com_content&task, [17.09.2014].

Rys.1. Typy profesji informatyka

Źródło: Opracowanie własne na podstawie M. Cieciura, Wybrane problemy społeczne i zawodowe informatyki, WSFiZ Warszawa, 2012,s.187; www.perspektywy.pl

O informatykach często się mówi, iż są „specyficzną grupą zawodową". Sami informatycy uważają podobnie. Jest to z pewnością związane z wytworzeniem przez nich swoich specyficznych zwyczajów, które można uznać za rodzaj kultury. Ponadto grupa tworzy własny język slangowy, który trudno zrozumieć osobom spoza środowiska. „Sposób postrzegania siebie i swojej pozycji zawodowej jest wyraźnie inny niż w przypadku większości pozostałych profesji – tutaj te różnice są bardziej wyraźne niż gdzie indziej"[27].

[27] Rosiński J. http://www.computerworld.pl/artykuly/316034/Kompetencje.spoleczne.i.uslugi.IT.html#sthash.TDmzuWwd.dpuf.

J. Rosiński w swojej pracy habilitacyjnej dotyczącej postaw zawodowych informatyków jako pracowników wiedzy, wymienia charakterystyczne cechy wyróżniające tę grupę zawodową[28]:

- Indywidualizm,
- wysoki poziom kompetencji,
- innowacyjność,
- cenienie sobie autonomii zawodowej,
- wykazywanie się niskim poziom chęci do współpracy,
- duży dystans do władzy,
- silna potrzeba wymiany myśli i identyfikacji zawodowej oraz odniesienia sukcesu,
- ciągłe pragnienia doskonalenia i rywalizacji opartej na wiedzy,
- pasjonaci swojego zawodu,
- cenienie profesjonalizmu u siebie i u innych,
- utylitarne traktowanie zatrudniającej organizacji jako nie rozwijającej ich kompetencji,
- utrzymywanie więzi z wybranymi osobami w miejscu pracy. Kryterium wyboru jest ocena kompetencji współpracownika,
- przejawianie tendencji do indywidualnej interpretacji norm obowiązujących w miejscu pracy,
- wykazywanie mniejszego zdyscyplinowania jak pozostali pracownicy organizacji.

Specyfiką zawodów informatycznych jest ich indywidualny i zadaniowy charakter. Informatyk pracując nawet w zespole projektowym określone zadanie realizuje samodzielnie, ale dla sprawdzenia efektu i postępu prac co jakiś czas konsultuje się z zespołem.

Kolejną cechą charakterystyczną dla tej grupy zawodowej jest brak identyfikacji z zatrudniającą organizacją, przy jednoczesnej identyfikacji z grupą zawodową.

---

[28] Rosiński J. Postawy zawodowe informatyków: jednostka, zespół, organizacja, WUJ Kraków 2013, s.147–169.

Informatycy znajdują zatrudnienie we wszystkich branżach i dziedzinach, które wykorzystują technologie teleinformatyczne i informatyczne np. zakładach produkcyjnych, dużych sklepach, instytucjach, urzędach, szpitalach, szkołach, bankach, hurtowniach czy instytucjach naukowych.

3.3. PROFESJONALIZM INFORMATYKA

Usługowy charakter zawodu informatyka, duży kontakt z ludźmi, szybki rozwój technologii i cywilizacji powoduje, że wzrasta znaczenie umiejętności i wiedzy oraz wykorzystanie ich w praktyce, a tym samym wykonywania pracy na najwyższym poziomie profesjonalnym.

W tym miejscu należy zadać pytanie. Kim jest profesjonalista? Czy wywiązującego się dobrze ze swoich zobowiązań informatyka można nazwać profesjonalistą? Czy wykonywana przez niego praca-usługa jest profesjonalna i co ją charakteryzuje?

W odniesieniu do literatury przedmiotu za usługę profesjonalną przyjmuje się – „*świadczenie profesjonalisty, który dzięki jego unikalnym talentom umożliwia – w procesie interakcji z klientem – tworzenie unikalnej więzi korzyści, dającej gwarancję realizacji dzieła zgodnie z oczekiwaniami klienta*”[29]. Usługi informatyczne i komputerowe wpisują się w treść przytoczonej definicji, o czym świadczy również wpis do branżowych usług profesjonalnych.

Profesjonalizm jest istotnym elementem integrującym reprezentantów danej grupy zawodowej. Jego istotę stanowi łącznie mistrzowskie opanowanie sztuki zawodu i odpowiednia postawa moralna, bowiem „*odnosi się do wzorów ról zawodowych powstałych w określonych warunkach społecznych i kulturowych*”[30], obejmujących kompetencje zawodowe bazujące na wysokim poziomie wiedzy, umiejętnościach i wartościach etycznych, odwołujących się do cenionych wartości społecznych. Taki wzorzec pozwala na kreowanie wizerunku danego zawodu

[29] Chłodnicki M., Usługi profesjonalne; Od jakości do lojalności klientów, WAE Poznań, 2004,s. 9.

[30] Kafel T., Cechy profesjonalizmu – analiza pojęciowa oraz oczekiwania stawiane zarządzającym podmiotami ekonomii społecznej *http://*fundacja.e-gap.pl/mowes/wp-content/uploads/2012/11/BES-nr-1-Artyku%C5%82-3.pdf.

w społeczeństwie i kształtowanie określonych wzorców etycznych, kulturowych oraz norm przedstawicieli danej profesji[31], który jest pożądany i ceniony przez pracodawców.

U podstaw profesjonalizmu każdego zawodu leży posiadanie specjalistycznej i ugruntowanej wiedzy wykorzystywanej na rzecz i dla dobra klienta, bowiem dobro klienta jest kluczowym celem działań każdego profesjonalisty. Profesjonalizm to ciągłe dążenie do doskonałości wykonywania pracy na wysokim poziomie przy jednoczesnym pełnym poczuciu satysfakcji jego wykonawcy i klienta, jak również „docenienie tego co się wie i pokora przed tym, czego się (jeszcze) nie wie"[32].

W języku potocznym bardzo często określenie „ekspert" stosuje się znamiennie z profesjonalistą. Jest to błąd, gdyż istnieje zasadnicza różnica między profesjonalistą a ekspertem. Różnicę można dobrze przedstawić na przykładzie podejścia dwóch lekarzy w leczeniu choroby pacjenta. Pierwszy robi wszystko, aby przywrócić pacjenta do zdrowia. Natomiast drugi koncentruje się tylko na zlikwidowaniu jednostki chorobowej. U pierwszego czyli profesjonalisty celem było dobro pacjenta, zaś u eksperta usunięcie tylko problemu[33].

Profesjonalny informatyk wykorzystuje specjalistyczną wiedzę w rozwiązywaniu problemów klienta, która jest jednym z wielu elementów budowania autorytetu. Autorytet ten przesądza o jego relacjach z klientem. Podstawą tej relacji jest wzajemne zaufanie – klient obdarza informatyka zaufaniem, w zamian oczekuje od niego prawdziwego zaangażowania i wysokich standardów. Przez wysokie standardy należy rozumieć standardy zachowania i praktyki zawodowej, gwarantujące klientowi wykonanie zadania z należytą starannością i znacznie wyżej od przeciętnego poziomu.

Profesjonalny informatyk to człowiek, o którym z pewnością nie można powiedzieć, że *„chętniej zmienia i ulepsza okoliczności, niż siebie samego. Dlatego pozostaje uwiązany"*[34] , ale jest to osoba wychodząca poza własną strefę komfortu,

---

[31] Tamże.

[32] www.goldenline.pl/grupy/Pozostałe/profesjonalisci//na-czym-wlasciwie-polega-ten-nasz-prtofesjonalizm, 941200 (17.09.2014).

[33] Chłodnicki M., Usługi profesjonalne. Od jakości do lojalności klientów, WAE Poznań 2004, s. 7.

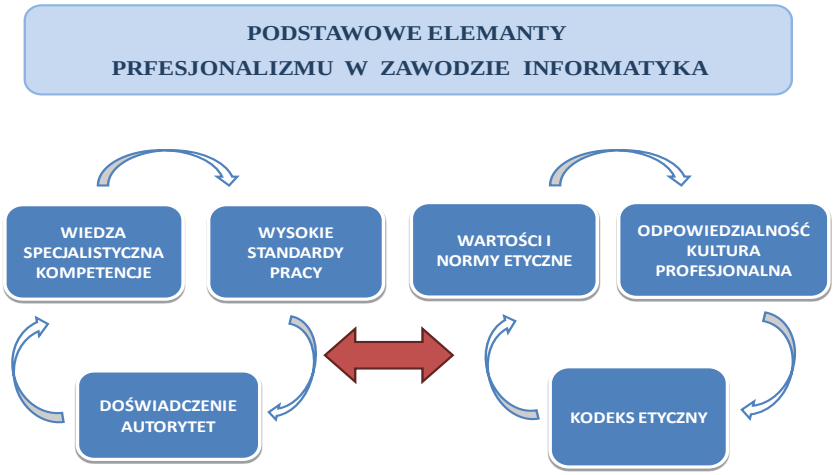
[34] www.dyrektorzy-handlowi.menedzersprzedazy.pl/a/charakterystyka-profesjonalisty-czy-myslisz-powaznie-o-swojej-pracy/511.html (17.09.2014).

zdająca sobie sprawę, że tylko tak może się rozwijać. Nie tylko wiedza specjalistyczna, umiejętności jej zastosowania czy przetwarzania będą świadczyć o profesjonalizmie zawodowym informatyka.

Istotnym czynnikiem profesjonalizmu jest także posiadanie podstaw wiedzy z innych dziedzin związanych z informatyką, zdolność i chęć do ciągłego samodokształcania się w zakresie wiedzy teoretycznej i praktycznej oraz kompetencje np. takie jak: kreatywność, umiejętności abstrakcyjnego i logicznego myślenia, samodzielność pracy, innowacyjność, współpraca, podejmowanie ryzyka, zaangażowanie, zdalności interpersonalne.

Nieodzownym atutem jest posiadanie otwartego umysłu, zdolności dostrzegania kontekstu i specyfiki branży, organizacji oraz odpowiednio wczesne wychwytywanie ryzyka w firmie, projektach czy systemach, a także posiadanie umiejętności identyfikowania i zapobiegania z wyprzedzeniem pojawiających się problemów.

Na rysunku przedstawiono schemat wzajemnych oddziaływań istotnych elementów, mających wpływ na profesjonalizm zawodu informatyka.



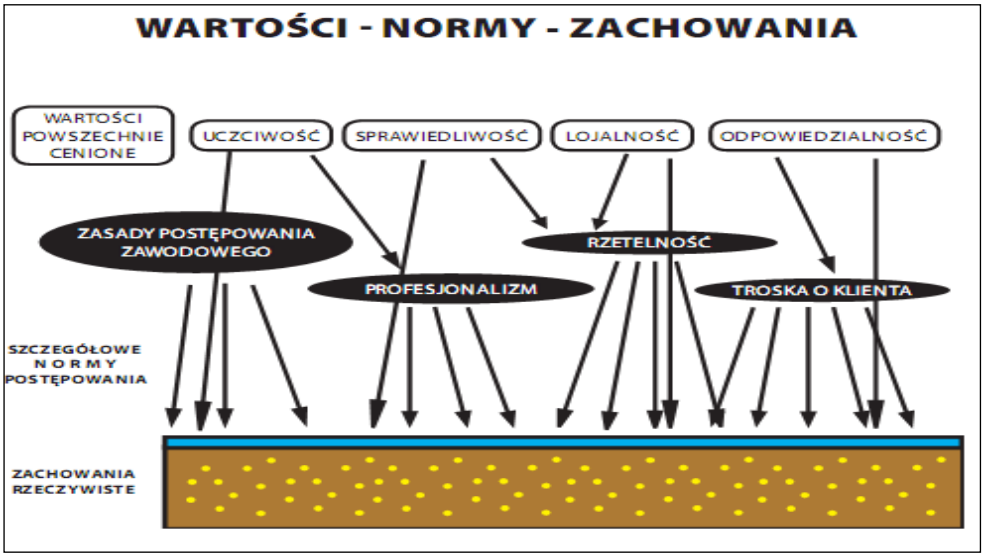
Rys 2. Schemat oddziaływań na profesjonalizm informatyka

Źródło: Opracowanie własne na podstawie M. Chłodnicki, Usługi profesjonalne. Od jakości do lojalności klientów, WAE Poznań 2004, s.7; T. Kafel, Cechy profesjonalizmu – analiza pojęciowa oraz oczekiwania stawiane zarządzającym podmiotami ekonomii społecznej http://fundacja.e-gap.pl/mowes/wp-content/uploads/2012/11/BES-nr-1- Artyku%C5%82-3.pdf

Na poziomie indywidualnym poprzez stosowanie i przestrzeganie określonych wzorców postaw zawartych w kodeksie etycznym, informatyk kształtuje i doskonali swoje normy moralne, a to oddziaływuje na coraz wyższy jego stopień odpowiedzialności i kultury zawodowej. Na poziomie zawodowym, doświadczenie wraz z wiedzą specjalistyczną i kompetencjami zawodowymi wykorzystywane jest do rozwiązywania problemów klienta, które przesądzają o relacjach między nimi i efekcie skutkują wysokim standardem wykonanej pracy. Wymienione elementy zarówno na poziomie indywidualnym jak i zawodowym stosowane łącznie w praktyce, wpływają na profesjonalizm zawodu informatyka.

3.4. ODPOWIEDZIALNOŚĆ

Podstawą każdego ludzkiego działania są wartości. Wartości moralne dotyczą konkretnych zachowań ludzkich. To drogowskazy na drodze życia stanowiące budulec dla „mostów" pomiędzy jego relacjami z jednostką, grupą czy organizacją, ułatwiając podejmowanie słusznych decyzji. Stanowią dla człowieka „płaszcz ochronny" przed demoralizującymi czynnikami zewnętrznymi i wewnętrzny hamulec dla zachowań nie etycznych. W normach moralnych, inaczej etycznych odnajdziemy ogólne wzorce właściwego postępowania i zachowania, bowiem to one kształtują obyczajowość człowieka, styl i jakość życia, jednocześnie mobilizują do postępowania zgodnie z przyjętymi wzorcami. Wskazują jakie zachowania są właściwe, a jakie należy potępiać oraz systematyzują czyny na dobre i złe. Na rysunku zaprezentowano podstawowe wartości powszechnie cenione w zachowaniach.



Rys. 3. Wpływ wartości powszechnie cenionych na zachowania

Źródło: Kosewski M. „*Wartości- Godność, Władza. Dlaczego porządni ludzie czasem kradną, a złodzieje ujmują się honorem”*, VIZJA PRESS & IT, Warszawa 2008, s 16.

Mówiąc o profesjonalizmie zawodu informatyka, nie można pominąć istotnego zagadnienia jakim jest jego postawa moralna, będąca odzwierciedleniem posiadanych wartości i norm moralnych. Profesjonalny informatyk wykonując swój zawód bezwzględnie powinien się kierować takimi wartościami etycznymi i normami moralnymi, które wpisują się w główną zasadę przysięgi Hipokratesa: „*po pierwsze nie szkodzić”* przede wszystkim klientowi, ale też sobie i społeczeństwu. W tym kontekście najbardziej pożądane wartości w pracy profesjonalnego informatyka to:

- **Rzetelność** pracy – skutkuje terminowym i należytym wywiązywaniem z postanowień zawartych w umowach z kontrahentami.
- **Zaufanie** – w relacjach z klientem, pracodawcą i współpracownikami, gdyż zaufanie jako wartość i zasób organizacji niewątpliwie znacząco wpływa na jej reputację, siłę przetargową, rachunek ekonomiczny.
- **Uczciwość** – w różnych zawodach uczciwość wyraża się inaczej, chociaż w warstwie wartości ma to samo imię. Uczciwość informatyka różni się od uczciwości sprzedawcy czy historyka. Uczciwy sprzedawca nie oszukuje na

wadze czy wydawaniu reszty, a historyk nie przekłamuje źródeł i nie nagina faktów historycznych. Natomiast uczciwy informatyk przewiduje skutki swoich działań dla siebie, klienta i społeczeństwa. Jest świadomy tego, co jest prawe i właściwe zarówno w zachowaniu i działaniu własnym jak i innych. Nie poprzestaje na zadawaniu sobie pytania czy to co robi koresponduje z jego wartościami i normami, czy służy dobru i szczęściu ludzi.

- **Odpowiedzialność** – to świadome rozumne kierowania swoim postępowaniem[35]**.**

Obok zaufania i uczciwości jest to istotna wartość w zawodzie informatyka, bowiem w dzisiejszym świecie technologie informatyczne wykorzystywane są na szeroką skalę. Dysponowanie specjalistyczną wiedzą zawodową, a przy tym posiadany prestiż i autorytet zawodowy daje możliwości łatwego wpływania na świat, ludzi, ich zachowania i cenione przez nich wartości**.** Stąd też ciąży na nim ciężar odpowiedzialnego jej używania. Odpowiedzialny informatyk–profesjonalista powinien wykazywać się pełną świadomością prowadzonych działań informatycznych i wynikających z nich konsekwencji własnego zachowania. Odpowiedzialność informatyków obejmuje zakres wykonywanego zawodu łącznie z obszarem dotyczącym relacji z klientami, bowiem charakter wykonywanej pracy wymaga od niego szeregu powiązań z innymi zawodami i ludźmi, włączają w to relacje i stosunki na linii[36]:

- pracodawca – pracobiorca,
- pracobiorca – pracodawca,
- klient – profesjonalista komputerowy,
- profesjonalista komputerowy – profesjonalista komputerowy,
- społeczeństwo – profesjonalista komputerowy.

Odpowiedzialność jest podstawowym filarem więzi międzyludzkich, z tej racji, iż profesjonalny i odpowiedzialny informatyk nawiązując relacje w różnymi obszarami

[35] http://www.ie-ries.com.pl/archiwum/artykuly/RIES_201110241034_Etyka.pdf.

[36] Cieciura M. Wybrane problemy społeczne i zawodowe informatyki, WSFiZ Warszawa, 2012, s. 211.

prowadzonych interesów, niekiedy sprzecznych, będzie się starał unikać sytuacji mogącej doprowadzać do ich konfliktów.

Informatycy tak jak inne grupy zawodowe funkcjonujące w społeczeństwie na zasadzie powszechności, podlegają regułom prawnym i moralnym. W zakresie swojej działalności wg kryterium przewinienia ponoszą odpowiedzialność, służbową, materialną, cywilną i karną oraz zawodową.

- **Odpowiedzialność służbowa** obejmuje powinności informatyka odnośnie wypełniania zadań określonych przez pracodawcę i ponoszenia konsekwencji za działania w tym zakresie.
- **Odpowiedzialność materialna** – informatyk odpowiada materialnie za powierzony mu sprzęt do realizacji prac wynikających z zakresu obowiązku zadań i regulaminu pracy jak również ciąży na ponoszenie skutków za wyrządzane szkody pracodawcy.
- **Odpowiedzialność cywilna** – ma charakter majątkowy. Informatyk ma obowiązek wynagrodzenia wyrządzanej szkody lub straty przez sprawcę – informatyka. W tym zakresie orzecznictwo odpowiedzialności należy do sądów powszechnych.
- **Odpowiedzialność karna** – dotyczy czynu zabronionego m.in. odpowiedzialności za utrzymanie zabezpieczeń, kradzież danych czy stosowanie nielegalnego oprogramowania w firmach. Konsekwencje tych naruszeń określa Kodeks Karny.
- **Odpowiedzialność zawodowa** – wynika z przynależności do określonej grupy zawodowej w środowisku informatycznym. Uregulowana jest przyjętymi przez daną grupę zawodową przepisami prawnymi i zasadami etycznymi, określonymi w kodeksach deontologicznych.

Odpowiedzialność zawodowa informatyka wiąże się z obowiązkiem moralnym lub prawnym ponoszenia skutków za postępowanie osobiste lub polecone innej osobie, niezgodne z zasadami kodeksu etyki zawodowej, uchybiającej godności zawodu i narażającej na szwank dobre imię zawodu informatyka.

Podsumowując tematykę odpowiedzialności podano przykład, jak nieodpowiedzialność zawodowa może drogo kosztować nie tylko osobę informatyka, ale również pracodawcę i klienta. Przekonał się o tym jeden z informatyków zatrudniony w małym

przedsiębiorstwie, który nie zabezpieczył jego bazy danych. Fakt ten spowodował użycie danych przedsiębiorstwa przez osoby nieuprawnione, a w następstwie ich utratę. Dodatkowo została wykorzystania infrastruktura informatyczna przedsiębiorstwa do popełnienia czynu zabronionego. Konsekwencją niezabezpieczenia danych informatycznych była odpowiedzialność w zakresie:

- Kodeksu Pracy – art.100 §4, – art.114 i art120,
- Kodeksu Cywilnego – art. 23–24 i art.45,
- Ustawy o ochronie baz danych art.11–12a,
- przepisów branżowych – dane dotyczące tajemnicy zawodowej, tajemnicy przedsiębiorstwa, etc.,
- Kodeksu Karnego – (ustawy o ochranie danych osobowych art.36, art.39a i art.52).

Reasumując, informatyk najwyraźniej zapomniał, że miarą odpowiedzialności pracownika staje się stosunek do jego właściwych obowiązków służbowych i reguł postępowania.

3.5. ETYKA ZAWODU INFORMATYKA

Każdy, kto zetknął się z czynem nieetycznym dokonywanym w ramach wykonywania pracy, w sposób niewłaściwy przez tzw. „fachowca" – partacza w zawodzie często myśli sobie: czy istnieje etyka zawodowa czy branżowa? Czy można w sposób rozsądny wewnętrznie i wzajemnie nie sprzecznie z obowiązującym prawem spisać osobno zasady etyczne, których powinien przestrzegać każdy np. lekarz, naukowiec, prawnik, kolejarz, elektryk, rolnik czy wreszcie informatyk[37]?

W jakimkolwiek zawodzie – podejście do szeroko rozumianej etyki uwypukla jej służebny charakter. Etyka zawodowa, jeśli nie jest uprawiana w poczuciu służby człowiekowi, łatwo może stać się elementem niezdrowej rywalizacji, nieuczciwości, zatajania prawdy czy ekonomicznych przetargów z pominięciem dobra wspólnego. To etyka wyznacza granice rozróżnienia dobra od zła, a rozróżnienie dokonuje się

[37] http://www.mragowo.pti.org.pl [22.09.2014].

w sumieniu człowieka. Dlatego ważne jest, aby wszystkie środowiska zawodowe w tym informatyczne nie ograniczały się tylko do zagadnień ściśle związanych ze specyfiką pracy specjalisty, ale działań zgodnie z określoną doktryną moralną i określonym systemem wartościowań.

Wszelkie działania związane z próbą tworzenia standardów etycznych regulujących sprofesjonalizowane zachowania zawodowe, których podstawą będą wiodące wartości etyczne takie jak: odpowiedzialność, obiektywizm, rzetelność, uczciwość, zaufanie, unikanie pełnienia konfliktowych ról, poszanowanie prawa własności czy praw człowieka i jego naturalnego środowiska zasługują na duże uznanie.

Dziś bardzo wiele mówi się o globalizacji. Jednym z zagrożeń jest niezdrowa rywalizacja skutkiem, której mogą być mniej lub bardziej nieudane projekty informatyczne finansowane za pieniądze podatników. Trudno wtedy o zachowanie nawet podstawowych reguł etyki. Jeżeli zatem słuszna i pożądana jest rywalizacja centrów informatycznych, to nie może ona dokonywać się kosztem prawdy, dobra, odpowiedzialności, kosztem takich wartości jak: unikanie szkodzenia innym ludziom, respektowanie własności intelektualnej i prywatnej innych, czy też kosztem bogactwa środowiska naturalnego.

Problem etyki jest jednym z kluczowych dylematów w środowisku informatycznym, dlatego sporo uwagi poświęcono temu zagadnieniu. Przyznano, że nie jest ono wolne od grzechów. Jedną z pierwszych prób tworzenia standardów etycznych i moralnych informatyka jest dekalog – Dziesięciu Przykazań Etyki komputerowej[38]:

1. Nie będziesz używał komputera, by szkodzić bliźnim.
2. Nie będziesz przeszkadzał bliźnim w pracy z komputerem.
3. Nie będziesz grzebał w plikach bliźniego.
4. Nie będziesz używał komputera do kradzieży.
5. Nie będziesz używał komputera do składania fałszywych świadectw.
6. Nie będziesz używał lub kopiował programów, za które nie zapłaciłeś.

[38] Cieciura M., Wybrane problemy społeczne i zawodowe informatyki, WSFiZ, W-wa 2012, str. 220.

7. Nie będziesz używał zasobów komputerowych bliźnich bez zezwolenia.
8. Nie będziesz przywłaszczał sobie własności intelektualnej bliźnich.
9. Będziesz rozważał społeczne konsekwencje programów, które napiszesz.
10. Będziesz używał komputera z rozwagą i szacunkiem.

Dziesięć przykazań etyki komputerowej skierowanych do informatyków i do użytkowników komputerów, opracowano przez Amerykański The Computer Ethics Institute (założony w roku 1985).

W ostatnich latach także w Polsce podjęto działania związane z próbą tworzenia kompleksowych i usystematyzowanych standardów etycznych regulujących zachowania zawodowe w środowisku informatycznym, dostosowanych do jego grup i kategorii zawodowych. Współcześnie do najbardziej znanych w kraju kodeksów środowiska informatycznego można zaliczyć m.in.:

1. Kodeks Etyczny Stowarzyszenia Sprzętu Komputerowego,
2. Kartę Praw i Obowiązków Dydaktyki Elektronicznej,
3. Dziesięć Przykazań Etyki Komputerowej,
4. Kodeks Zawodowy Informatyków (PTI).

Kodeks Zawodowy Informatyków Polskiego Towarzystwa Informatycznego uchwalony na X Zjeździe Delegatów PTI dnia 29 maja 2011 roku, zasługuję na większą uwagę, gdyż adresowany jest do szerokiego grona osób o zróżnicowanych formach aktywności informatycznej. Skierowany jest również do osób o dowolnym profilu zawodowym: naukowym, dydaktycznym, gospodarczym oraz społecznym.

W dwunastopunktowym zestawie zaleceń odwołuje się zarówno do zagadnień ściśle związanych ze specyfiką pracy profesjonalistów należących do PTI jak i „sympatyzujących z wyznawanymi wartościami przez nie wartościami etycznymi", również w innych, sprofesjonalizowanych zawodach. Zalecenia właściwych zachowań w informatyce zawarte w Kodeksie Zawodowym Informatyków to[39]:

1. Informatycy stosując informatykę, będącą wiedzą służebną wobec dziedzin jej
2. różnorodnych zastosowań, wspierają rozwój tych dziedzin nie przeszkadzając mu.

[39] www.pti.org.pl [17.09.2014].

3. Zastosowania narzędzi i algorytmów informatyki nie stanowią dla informatyków celu, lecz są środkiem mającym przede wszystkim rozwiązywać z poszanowaniem zasad logiki, praw człowieka, jego środowiska naturalnego, ergonomii, ekonomii, poprawności językowej, norm jakości oraz specyfiki dziedzin szczegółowych przedstawiane problemy informatyczne.
4. Informatycy stale doskonalą swoją wiedzę, a jednocześnie zawsze przedstawiają swoje kompetencje i doświadczenie zawodowe zgodnie ze stanem faktycznym.
5. Informatycy wzorowo szanują własność intelektualną i prawa jej ochrony.
6. Informatycy przestrzegają praw majątkowych do informacji i wiedzy zawartych w systemach informatycznych swojego pracodawcy i klienta.
7. Informatycy nie podejmują się nieuprawnionego naruszania integralności systemów informatycznych jakichkolwiek podmiotów.
8. Informatycy prowadzący wolną działalność dydaktyczną prezentując konkretne rozwiązania zawsze starają się przedstawić możliwie szerokie spektrum rozwiązań o analogicznej funkcjonalności oraz przeznaczeniu, jeśli takie istnieją. Analogicznie starają się w tego rodzaju działalności oddzielać własne poglądy w konkretnej sprawie od innych istniejących poglądów.
9. Informatycy prowadzący działalność naukową lub badawczo-rozwojową zawsze wyraźnie oddzielają wiedzę pewną i już udowodnioną od przyjmowanych przez siebie założeń.
10. Informatycy zawsze przedstawiają swojemu klientowi pełne i rzetelne informacje o przewidywaniach kosztów oraz przypuszczalnym czasie trwania analizowanego przez siebie projektu lub przedsięwzięcia znajdującego się już w fazie realizacji.
11. Informatycy podają pełne i rzetelne informacje o przyszłych konsekwencjach technicznych i finansowych wynikających z realizacji projektu.
12. Informatycy nie podejmują się równocześnie prac u kilku zleceniodawców, jeśli ich interesy mogłyby być ze sobą sprzeczne.

13. Informatycy unikają jednoczesnego pełnienia w przedsięwzięciach ról wzajemnie opozycyjnych, jak w szczególności zleceniodawcy i zleceniobiorcy, podwykonawcy i kontrolera, programisty i testera.

Głównym celem statutowym Polskiego Towarzystwa Informatycznego jest dbanie o wysoki poziom etyczny i zawodowy jego członków oraz tworzenie warunków do jego podnoszenia. Kodeks ma „*za zadnie (…) wspierać (…) osoby w rozstrzyganiu w swoim sumieniu, czy dane postępowanie na polu zawodowym jest, czy nie jest właściwe, a w razie potrzeby też wspierać w uzasadnianiu działań. Rolę tę kodeks ma do spełnienia nie tylko w odniesieniu do osób fizycznych, ale również w relacjach informatyków z klientami, partnerami gospodarczymi, współpracownikami, kolegami, przełożonymi, pracodawcami oraz władzami*" (Kodeks Zawodowy Informatyków 2011).

Z pewnością zróżnicowanie zawodów informatycznych będzie wciąż postępować, tak jak wciąż będą się pojawiać nowe dylematy i problemy etyczne w tych sprofesjonalizowanych zawodach. Niektóre z nich na pewno doczekają się rozwiązań prawnych, jednak większość będzie podlegała regulacji na poziomie tworzenia nowych programów etycznych czy też nowych kodeksów etycznych[40].

[40] Art. Danuta Walczak-Duraj „Kontekst etyczny zawodów informatycznych".

4

Internet rzeczy w e-gospodarce – wyzwania i perspektywy

4.1. WPROWADZENIE

W artykule przedstawiono koncepcję Internetu, w której zwykłe przedmioty i urządzenia codziennego użytku połączone za pomocą sieci teleinformatycznych komunikują się między sobą, oddziałują na siebie oraz współpracują ze sobą. Systemy realizacji Internetu rzeczy (ang. Internet of Things, IoT) są praktycznie nieograniczone i obejmują inteligentne miasta, domy, sieci energetyczne, przemysł, etc. Według opracowań Gartner Inc. dotyczących cyklu życia technologii, prezentowana technologia znajduje się obecnie w fazie, w której oczekiwania rynku z nią związane, przechodzą przez etap wzrostu. Taka sytuacja sprzyja powstawaniu wielu nowych rozwiązań, przyczynia się do zwiększenia liczby wdrożeń i w rezultacie napędza gospodarkę. Jednak wprowadzenie każdej nowej technologii wiąże się także z koniecznością przezwyciężania wielu wyzwań. W przypadku Internetu rzeczy są to przede wszystkim problemy związane z bezpieczeństwem użytkowników, ich prywatnością i poufnością danych.

Pojawianie się nowych idei, koncepcji oraz technologii w obszarze IT, poszukiwanie i znajdowanie dla nich innowacyjnych zastosowań sprawia, że branża

ta, charakteryzująca się bardzo szybkim tempem rozwoju, ma istotny wpływ na sprawność działania wielu sektorów zarówno w elektronicznej jak i w tradycyjnej gospodarce światowej oraz w gospodarkach na poziomie poszczególnych krajów. Rozwój Internetu w latach dziewięćdziesiątych stworzył dla biznesu nieograniczone możliwości. Dzięki globalnej sieci komunikacja stała się natychmiastowa, transakcyjna, szyfrowana i stale dostępna. Duża część firm przeszła transformację, odchodząc od tradycyjnych wzorców funkcjonowania i przechodząc do systemu opartego na działaniach wielokanałowych, wykorzystujących podstawowe usługi Internetowe i ich pochodne, rozpoczynając tym samym e-biznesową rewolucję. Równolegle można zaobserwować na świecie intensywny rozwój gospodarki elektronicznej (e-gospodarki) – określanej jako globalna, wirtualna przestrzeń, w której prowadzona jest działalność gospodarcza. W sferze tej realizowane są procesy gospodarcze (produkcja, sprzedaż, dystrybucja) za pomocą środków elektronicznej wymiany danych. Postęp w technologii informacyjno-komunikacyjnej (TIK) przyczynił się do zmiany procesów zachodzących wewnątrz przedsiębiorstw, pomiędzy nimi (tzw. B2B), w kontakcie z klientami indywidualnymi (B2C), a między samymi klientami (C2C) [WAW03]. Rozwój gospodarki elektronicznej doprowadził do powstania nowych modeli biznesowych, nowych usług, metod i miejsc pracy oraz nowych sposobów pozyskiwania informacji i wiedzy.

Każdego roku na świecie publikowanych jest wiele raportów przedstawiających prognozy dotyczące kierunków rozwoju najbardziej perspektywicznych technologii informatycznych. Z doniesień, które ukazały się w ostatnim okresie wynika, że kolejnym kluczowym etapem w rozwoju globalnej sieci zaraz po WWW i Internecie mobilnym stanie się Internet rzeczy (McKinsey Global Institute [MCK13], Gartner Inc. [GAR14], Pew Research Center [AND14], Cisco [EVA11]). Zdaniem wielu analityków, w najbliższych latach liczba urządzeń i przedmiotów codziennego użytku podłączanych do Internetu będzie rosła w coraz szybszym tempie, a przebieg czasowy wzrastającego zainteresowania tą tematyką pokazuje wykres prezentowany w serwisie Google Trends [GOO14].

Celem artykułu jest przedstawienie Internetu rzeczy w wymiarze e-gospodarki ze szczególnym uwzględnieniem perspektyw oraz wyzwań, jakie ta koncepcja

stworzyła dla sfery biznesu, na etapie poprzedzającym fazę dojrzałości i nasycenia rynku w cyklu życia tej technologii jako produktu.

Znaczenie tej technologii odkryły już największe ekonomicznie gospodarki takie jak Chiny, USA, Japonia czy Unia Europejska, które inwestują ogromne środki finansowe w badania z zakresu IoT, wspierając tym samym swoje gospodarki w dążeniu do osiągnięcia przewagi konkurencyjnej na globalnym rynku.

Według cyklu życia nowych technologii (ang. hype cycle) opracowanego i każdego roku aktualizowanego przez firmę analityczno-doradczą Gartner Inc., Internet rzeczy znajduje się obecnie w fazie nadmiernie rozbudzonych oczekiwań (ang. Peak of Inflated Expectations) etapie uzasadniającym obecne rosnące zainteresowanie tą technologią [GAR13]. W dalszej części cyklu prowadzącego do fazy dojrzałości technologia IoT będzie wymagała rozwiązania wielu problemów m. in. natury technicznej, społecznej czy prawnej. Kwestią fundamentalną dla spopularyzowania Internetu rzeczy będzie zdobycie zaufania wśród indywidualnych użytkowników i przedsiębiorstw. Osiągnięcie tego celu będzie możliwe gdy konsumenci będą mieć pewność, że informacje pozyskiwane i przetwarzane przez IoT, nie będą miały negatywnego wpływu na nich samych i na resztę społeczeństwa. Potencjał, jaki niesie z sobą Internet rzeczy w zakresie dostarczenia użytkownikom nowych możliwości i korzyści, będzie w pełni wykorzystany, kiedy zostaną wyeliminowane zagrożenia dotyczące polityki bezpieczeństwa i prywatności.

Kolejnym ważnym zagadnieniem jest standaryzacja, prowadząca do interoperacyjności, czyli zdolności do współdziałania i komunikowania się. Obecna sytuacja jest skomplikowana z powodu braku holistycznego podejścia do idei Internetu rzeczy, braku spójnych koncepcji jednoczących się wokół tej technologii oraz braku jednolitej wizji architektury dla IoT. W związku z tym indywidualni producenci tworzą własne rozwiązania z obszaru IoT, wykorzystując tym samym tylko swoje, niedostępne szerzej technologie [COE11].

4.2. INTERNET RZECZY – PREZENTACJA KONCEPCJI

Internet rzeczy to młoda, obecnie szybko rozwijająca się i dojrzewająca koncepcja, mająca swoje korzenie w różnego rodzaju sieciach, percepcji zjawisk fizycznych przez sensory i różnorodnych podejściach do przetwarzania informacji [IER12]. Sama idea IoT polega na podłączaniu do Internetu fizycznych obiektów, przedmiotów codziennego użytku, różnej wielkości sensorów i urządzeń wykonawczych, komputerów, smartfonów, urządzeń medycznych oraz systemów przemysłowych. W ten sposób rzeczy stają się częścią globalnej sieci i mogą się komunikować zarówno ze sobą jak i z ludźmi. Jak dotąd nie uzgodniono jednej wspólnej definicji Internetu rzeczy. Według CASAGRAS Internet rzeczy definiowany jest jako „globalna infrastruktura sieciowa, łącząca fizyczne i wirtualne obiekty poprzez wykorzystanie możliwości pozyskiwania danych i komunikacji. Taka infrastruktura obejmuje istniejący i ewoluujący Internet oraz rozwijające się sieci. Oferuje ona jednoznaczną identyfikację obiektów, możliwości podłączenia sensorów i łączność, które będą stanowić podstawy do rozwoju niezależnych, współpracujących usług i aplikacji. Ponadto infrastrukturę tą cechuje wysoki poziom autonomicznego zbierania danych, transferu informacji o występujących zdarzeniach, łączność sieciowa oraz interoperacyjność" [CAS11].

Architektura IoT oparta jest zasadniczo na modelu zbudowanym z 3 warstw i charakteryzującym się wszechstronną percepcją i identyfikacją (warstwa percepcyjna), wiarygodną transmisją (warstwa sieciowa) i inteligentnym przetwarzaniem (warstwa aplikacji). Internet rzeczy obejmuje szeroki wachlarz różnych technologii, wchodzących w skład poszczególnych warstw. Do urządzeń realizujących zadania pierwszej warstwy należą: czujniki, tagi RFID, kamery oraz terminale GPS. Druga warstwa obejmuje różnego typu sieci: szkieletowe, mobilne, WLAN, satelitarne itd. W skład trzeciej warstwy wchodzą technologie przetwarzania rozproszonego (P2P – Peer to Peer, cloud computing, big data, data mining). Niektórzy badacze rozszerzają ten ogólny model jeszcze o 2 warstwy i w ten sposób na architekturę IoT składają się warstwy: biznesowa, aplikacji, przetwarzania, transportu i percepcji [ZHE11]. Architektura IoT jest otwarta, ponieważ wykorzystuje otwarte protokoły wspierające istniejące protokoły sieciowe.

4.3. POTENCJAŁ I PERSPEKTYWY INTERNETU RZECZY W OBSZARZE E-BIZNESU

Możliwości zastosowań Internetu rzeczy są praktycznie nieograniczone i obejmują inteligentne otoczenie (miasta, drogi, ulice, domy), energooszczędną i niskoemisyjną gospodarkę, eko-gospodarkę, rolnictwo, zdrowie, przemysł i wiele form działalności gospodarczej. Pojawienie się IoT, z punktu widzenia elektronicznej gospodarki i e-biznesu, przyczyniło się do wykształcenia się nowych modeli usług biznesowych. Niektóre firmy stworzyły i uruchomiły usługi działające w oparciu o IoT. Jedną z takich firm jest Rolls-Royce, który umieszcza w produkowanych przez siebie silnikach lotniczych specjalne układy elektroniczne. Układy te transmitują informacje dotyczące stanu urządzenia, komunikaty o ewentualnej potrzebie przeprowadzenia przeglądu, konserwacji czy naprawy. W ten sposób firma może szybko zareagować na bieżące problemy, zapewnić i dostarczyć odpowiednią część do właściwego portu, do którego przyleci dany samolot [MCA12]. W podobny sposób działa już także wielu producentów i handlowców. Za pośrednictwem Internetu otrzymują oni od różnych urządzeń, informacje o kończących się zapasach określonych produktów i automatycznie mogą uzupełniać braki, a następnie realizować zamówienia. Na tej zasadzie w niektórych krajach działają już automaty sprzedające napoje i przekąski. Dzięki zainstalowanym kamerom najpierw oceniają swojego klienta i wykorzystując dostępną wiedzę ze swojej bazy danych, dobierają dla niego odpowiedni produkt. W ten sposób w przyszłości w gospodarstwie domowym pralka sama zapewniałaby sobie środki piorące, lodówka dbałaby o swoją zawartość, natomiast drukarka sama zarządzałaby dostawami materiałów eksploatacyjnych w celu zapewnienia ciągłości swojego działania.

Internet rzeczy i technologie mobilne będące łącznikiem między światem rzeczywistym i cyfrowym stwarzają nowe możliwości między innymi w obszarze marketingu. Technologie te przyczyniają się do poprawy atrakcyjności opracowywania reklamy oraz nadawania jej bardziej interaktywnej formy. Skutkują również trafniejszym kierowaniem reklamy do potencjalnych odbiorców. Specjalnym przypadkiem marketingu mobilnego jest tzw. wszechobecna reklama (ang. pervasive advertising), rozszerzająca zasięg urządzeń mobilnych na fizyczne przedmioty lub obiekty obliczeniowe. Jednym z przykładów zastosowania tych technologii mogą być inteligentne bilbordy, prezentujące w interesujący i zachęcający sposób reklamy

cyfrowe. Z jednej strony mogą one emitować filmy promocyjne, z drugiej mogą także proponować cyfrowe kupony z informacją o lokalizacji (w postaci współrzędnych GPS) do wszystkich sklepów, które oferują określoną promocję. Zainteresowany klient znajdujący się w pobliżu takiego źródła reklamy, może w prosty sposób za pomocą metody „drag and drop" przenieść oferowany kupon na swoje urządzenie mobilne. Zaletą tej formy reklamy jest możliwość monitorowania preferencji przechodniów, których wszystkie interakcje z elektroniczną tablicą mogą być wykorzystane w celu stworzenia profilu preferencji dla każdego mobilnego urządzenia znajdującego się w otoczeniu określonego bilbordu. Odbywać się to może dzięki informacjom o upodobaniach właściciela danego urządzenia mobilnego, pomimo braku znajomości danych identyfikacyjnych jego użytkownika, ale dzięki informacjom zgromadzonym wyłącznie na podstawie wiedzy uzyskanej z treści, które wcześniej pobrał on jako użytkownik danego sprzętu mobilnego. W ten sposób możliwe jest monitorowanie efektywności każdego bilbordu w czasie rzeczywistym, tylko na podstawie informacji o miejscu, w którym dany kupon został pobrany. Dzięki temu reklamodawca otrzymuje dokładniejszą informację zwrotną, co może mu pomóc w poprawieniu skuteczności swoich działań marketingowych. Na następnym etapie rozwoju, reklamy wyświetlane na inteligentnych bilbordach będą mogły być także świadome swej lokalizacji. Oznacza to, że posiadając profile preferencji klientów, firma reklamująca swe produkty lub usługi na zewnątrz będzie w stanie w bardziej precyzyjny sposób dobierać i wyświetlać prezentowane treści w zależności od obecności użytkowników urządzeń mobilnych znajdujących się w pobliżu danego bilbordu. Kolejnym przykładem zastosowania tzw. świadomych tablic reklamowych w marketingu może być usługa oferująca posiadaczowi mobilnego kuponu pomoc w postaci przewodnika wyświetlającego wskazówki dotyczące drogi prowadzącej do konkretnego sklepu [GER12].

Internet rzeczy jest także wykorzystywany w marketingu mobilnym w formie technologii Estimote opartej na urządzeniach w postaci niewielkich czujników przymocowanych do towarów. Czujniki te emitując sygnał radiowy, przekazują informacje o produkcie do urządzenia mobilnego użytkownika znajdującego się w pobliżu z zainstalowanym odpowiednim oprogramowaniem umożliwiającym wyświetlanie takich danych. Wysyłane komunikaty są spersonalizowane i dostoswane do potencjalnych wymagań konsumentów. Informacje na temat potrzeb klientów mogą

być pozyskiwane z różnych źródeł: z serwisów społecznościowych, wyszukiwarek, listy serwisów odwiedzanych sklepów internetowych oraz innych stron www czy z samych urządzeń mobilnych. Estimote może także pobierać informacje o bieżącej lokalizacji klienta w sklepie, sposobie jego przemieszczania się itd. [EST14]

Zakłada się, że w przyszłości producenci różnych towarów jeszcze skuteczniej niż obecnie, dzięki technologii IoT, będą mogli na bieżąco otrzymywać informację zwrotną od konsumentów, a właściwie od przedmiotów przez nich zakupionych i użytkowanych. Będzie to kolejny sposób na ulepszanie istniejących produktów i usług, dużych oszczędności i inteligentnego korzystania z posiadanych zasobów [CAM11]. W przemyśle stosowanie inteligentnych maszyn przetwarzających dane z aplikacji biznesowych może w efekcie dopasowywać tempo i rodzaj produkcji do rozpoznawanych na bieżąco potrzeb rynkowych. W energetyce dzięki danym z inteligentnych liczników możliwe jest już dostosowanie podaży do popytu energii. W motoryzacji pojazdy podłączone do sieci i urządzeń mobilnych mogą być na bieżąco lokalizowane, a wyposażenie ich w czujniki może umożliwić proaktywne serwisowanie w momencie wykrycia jakiegoś błędu w działaniu poszczególnych zespołów. Kolejnym szerokim obszarem wykorzystania IoT jest logistyka. W tym przypadku możliwe jest kontrolowanie warunków, w jakich przewożone są towary, uwzględniających np. wstrząsy, wibracje, temperaturę, etc. Ponadto Internet rzeczy jest nieoceniony w sytuacji, gdy konieczna jest lokalizacja przedmiotów na dużych powierzchniach magazynowych, śledzenie floty pojazdów np. transportujących specjalne towary, w tym towary delikatne, niebezpieczne, cenne itp. oraz śledzenie przesyłek w przypadku zakupu czy przesyłania towarów [FAB14]. W obszarze handlu elektronicznego już teraz wykorzystuje się IoT w standardzie NFC do dokonywania płatności z bliskich odległości za pomocą kart zbliżeniowych.

4.4. INTERNET RZECZY – WYZWANIA

Internet rzeczy jako pożyteczne narzędzie i źródło wielu potencjalnych rozwiązań w gospodarce, jest równocześnie technologią stojącą w obliczu wyzwań. Pokonanie obserwowanych i przewidywanych problemów to klucz do zwiększenia popularności tej koncepcji w przemyśle i biznesie, wśród użytkowników indywidualnych

i wprowadzenia IoT na kolejne etapy rozwoju w cyklu życia produktu. Ze względu na skalę przedsięwzięcia, dużą liczbę obiektów podłączonych do Internetu duża jest też liczba napływających danych i duża jest również skala trudności całego zadania technologicznego. Potężny napływ danych różnego typu wymaga zawsze dostępu do sprzętu o odpowiednio wysokiej jakości i wydajności, a dodatkowo także bezpiecznego przesyłania, magazynowania, przetwarzania oraz interpretacji gromadzonych informacji.

4.4.1. WSPÓLNA KONCEPCJA ARCHITEKTURY INTERNET RZECZY

W Europie i na świecie realizowanych jest równolegle wiele projektów związanych z IoT, w których szuka się rozwiązań dla zdefiniowanych problemów (CASAGRAS/CASAGRAS2, Smart Santander, IoT@Work, IoT-i, iCore, IoT-A, SENSEI, ASPIRE, AKARI). Jednym z głównych wyzwań stojących przed naukowcami jest opracowanie jednolitej i całościowej koncepcji architektury Internetu rzeczy łączącej w całość różne segmenty IoT oraz zasoby wirtualne.

Zagadnienie to jest bardzo skomplikowane i obejmuje cały szereg kwestii, dotyczących technologii identyfikacji, sieci, aplikacji i bezpieczeństwa, do których m.in. należą [VER11]:

- zdefiniowanie głównych elementów systemu i ich funkcjonalności, interfejsów, łącz komunikacyjnych, narzędzi do zapewnienia bezpieczeństwa i prywatności,
- zapewnienie wysokiego poziomu skalowalności, mobilności i interoperacyjności obiektów, aplikacji i usług wchodzących w skład IoT,
- możliwości współpracy i interakcji różnych urządzeń i usług wykorzystujących protokół IP oraz inne protokoły, integracja protokołów,
- zorientowanie architektury na usługi SOA (ang. Service Oriented Architecture) i wykorzystanie chmury obliczeniowej,
- dostarczenie mechanizmów zarządzania dostępem do zasobów,
- dostarczenie mechanizmów gwarantowanej jakości usług,

- sprostanie ograniczeniom urządzeń w zakresie dostępnej energii, mocy obliczeniowej, pojemności pamięci i możliwości komunikacyjnych,
- połączenie ze sobą różnych typów sieci (WAN, LAN oraz sieci IoT – 6LoWPAN, ZigBee, etc.).

4.4.2. WPROWADZENIE PROTOKOŁU IPV6

Kolejnym istotnym zagadnieniem, oprócz opracowania koncepcji wspólnej architektury dla wszystkich składników IoT, jest wdrażanie protokołu IPv6, następcy IPv4. Każde urządzenie podłączone do Internetu musi posiadać swój własny unikalny identyfikator w postaci adresu IP. Według badań przeprowadzonych przez firmę Cisco prognozuje się, że do roku 2020 liczba urządzeń podłączonych do globalnej sieci sięgnie 50 Systems miliardów. Zaadresowanie takiej liczby fizycznych obiektów wymaga skorzystania z adresacji IPv6, znacznie rozszerzającej pulę adresów. Poza tym IPv6 usprawnia zarządzanie sieciami dzięki możliwościami auto-konfiguracji oraz dostarcza właściwości poprawiających bezpieczeństwo. Rozwiązanie problemu z adresacją pozwala już także na masowe stosowanie IoT w przemyśle i przejście z lokalnych zastosowań do rozwiązań stosowanych na dużą skalę.

4.4.3. SAMOWYSTARCZALNOŚĆ ENERGETYCZNA URZĄDZEŃ IOT

Jednym z głównych elementów warstwy percepcyjnej IoT są różnego typu czujniki często łączone w sieci, komunikujące się ze sobą lub z głównym węzłem (bramą) w sposób bezprzewodowy. Problemem w tym przypadku jest ich zasilanie. Ze względu na trudności z wymianą baterii w ogromnej liczbie tego typu urządzeń rozlokowanych na dużej przestrzeni, dąży się do tego, aby sensory były samowystarczalne, aby same pobierały/wytwarzały energię z otoczenia np. z wibracji, światła, przepływu powietrza itd. Ostatnio nastąpił pewien postęp w tej dziedzinie, za sprawą elastycznego układu nanogeneratora, wykorzystującego ruch ciała (ucisk palca) do wytwarzania energii.

4.4.4. WYPRACOWANIE I UZGODNIENIE STANDARDÓW

Internet rzeczy zacznie rozwijać się bardziej intensywnie, gdy nastąpi znaczący postęp w zakresie opracowania odpowiednich standardów dotyczących m.in. architektury, komunikacji, bezpieczeństwa i poufności. Standardy te powinny być zaprojektowane w taki sposób, aby wspierały szeroki zakres zastosowań i wspólnych wymagań dla rozwiązań z różnych sektorów przemysłu, potrzeb środowiska i społeczeństwa. Głównym celem opracowania standardów jest zapewnienie wysokiego stopnia interoperacyjności, która umożliwi interakcje między różnymi źródłami danych i między wieloma rodzajami urządzeń oraz zminimalizuje niejednoznaczności związane z interpretacją wymienianych informacji [VER11]. W chwili obecnej część standardów już istnieje, a w grupie tej są już standardy dotyczące danych, ich kodowania, protokołów, interfejsów urządzeń, Internetu czy regulacje w zakresie częstotliwości transmisji.

4.4.5. BEZPIECZEŃSTWO

Fundamentalnym zagadnieniem wymagającym dobrych i szybkich rozwiązań jest bezpieczeństwo informacji, sieci i aplikacji. Włączanie elementów IoT (czujników, urządzeń sieciowych oraz urządzeń do przechowywania danych) do globalnej sieci naraża je na szereg zagrożeń. Podatność tych urządzeń na różnego typu ataki, może skutkować zmniejszeniem wiarygodności i niezawodności tej technologii. Zabezpieczenie dużej ilości urządzeń, szczególnie czujników (tagów), posiadających zwykle ograniczoną moc obliczeniową, które nie są w stanie sprostać wymaganiom konwencjonalnych rozwiązań antywirusowych, będzie w najbliższej przyszłości jednym z kluczowych wyzwań. Każda warstwa architektury IoT jest podatna na różnego typu zagrożenia ze strony hakerów. Do głównych zagrożeń dla bezpieczeństwa sieci sensorowych – jednej z najważniejszych technologii wchodzącej w skład warstwy fizycznej IoT należą [WAR11]:

- zniszczenie i kradzież sprzętu,
- zakłócenia środowiskowe lub celowe zagłuszanie,

- ataki na integralność, poufność lub prywatność danych – nieupoważniony dostęp do danych zawartych w czujnikach (tagach) i ewentualne fałszowanie tych danych (podszywanie się pod zaufanego użytkownika),
- modyfikacja lub obejście kodu znajdującego się w pamięci urządzeń – kompromitacja systemu zabezpieczeń, przejęcie węzła,
- ataki typu DoS (ang. Denial of Service) odmowa usługi i brak dostępności – przeciążanie atakowanych węzłów sieci sensorowej,
- ataki typu Sybil oraz typu dziura (ang. sinkhole) – nieautoryzowany dostęp do sieci i transmitowanych przez zaufanego użytkownika danych (podszywanie się),
- podsłuchiwanie transmisji i ewentualna modyfikacja danych.

W celu zabezpieczenia się przed powyższymi zagrożeniami dla sieci sensorowych należy stosować zaawansowane metody i algorytmy ograniczające do minimum ryzyko powodzenia ataku na pojedyncze węzły lub całą sieć. Do ochrony mogą być wykorzystywane takie same techniki jak w przypadku klasycznego Internetu tzn. autentykacja, kontrola dostępu i procedury audytowe. Do zapewnienia bezpieczeństwa stosuje się także różne mechanizmy kryptograficzne. W przypadku bezprzewodowych sieci sensorowych (ang. Wireless Sensor Network – WSN) nie mogą to być tradycyjne metody takie jak AES czy RES, muszą to być „lekkie" algorytmy szyfrujące oraz „lekkie" protokoły komunikacyjne [ZHE11]. Kolejnym sposobem ochrony jest stosowanie zabezpieczeń polegających na przykład na monitorowaniu emisji radiowej czy stosowaniu dedykowanych i bezpiecznych protokołów transmisji danych itd. [WAR11].

Dodatkowym aspektem wymagającym uwzględnienia w trosce o bezpieczeństwo opisywanej technologii są kwestie prawa, uregulowań oraz polityka poszczególnych państw, regionów i sektorów przemysłu w tym zakresie [ZHE11].

4.4.6. PRYWATNOŚĆ I POUFNOŚĆ

Prywatność ludzi i poufność procesów biznesowych to dwa ważne aspekty zarówno w tradycyjnym Internecie jak i w Internecie rzeczy, zapobiegające nieautoryzowanej identyfikacji i śledzeniu. Obie kwestie są trudne do kontrolowania ze względu na skalę wykorzystania, mobilność i stosunkowo małe skomplikowanie elementów Internetu rzeczy. Prywatność i poufność są szczególnie ważne w przypadku IoT, ponieważ gromadzone dane są bliższe prywatnym danym użytkowników (np. dane fizjologiczne). Ze względu na fakt, że istniejąca technologia szyfrowania danych jest złożona, konieczne jest opracowanie szybszych i bardziej energooszczędnych algorytmów szyfrowania, opartych na mechanizmie dystrybucji kluczy.

4.5. PODSUMOWANIE

Internet rzeczy oferuje duży potencjał korzystnych rozwiązań, które mogą być wykorzystane w e-gospodarce. Odpowiednio dostosowane i właściwie przygotowane wprowadzanie tej technologii w firmach może skutecznie wesprzeć działania biznesowe, co wiąże się ze wzrostem zysków, efektywności sprzedaży, jakości produkcji i jest szansą na wdrożenie ułatwień w systemie pracy.

Autorzy raportu McKinseya przewidują, że w najbliższym czasie Internet rzeczy będzie miał znaczący wpływ na stwarzanie nowych możliwości biznesowych dla przedsiębiorców i w związku z tym na powstawanie nowych produktów i usług, które będą pod wieloma względami lepsze, oszczędniejsze oraz które w coraz bardziej skuteczny i świadomy sposób będą wykorzystywały dostępne zasoby [MCK13]. Dlatego też inteligentne i postępowe organizacje obecnie zastanawiają się nad tym, jak usprawnić swoje działania biznesowe, aby wykorzystać postęp w dziedzinie IoT i uczynić go częścią swojej przewagi konkurencyjnej na rynku.

Wachlarz możliwości rozwoju gospodarczego dzięki wykorzystaniu technologii IoT w działaniach organizacji jest szeroki. Internet rzeczy dostarcza firmom nowych modeli biznesowych i umożliwia efektywniejsze zarządzanie swoimi zasobami. W przemyśle IoT przyczynia się m.in. do większej wydajności i optymalizacji produkcji.

W obszarze e-handlu największe zainteresowanie tą technologią widoczne jest w dziedzinach takich jak: logistyka, gospodarka zasobami oraz płatności.

Technologia IoT znajduje się obecnie na początku drogi w cyklu swojego rozwoju. Istniejące bariery i wyzwania z czasem zostaną prawdopodobnie przezwyciężone, a zadecydują o tym wymierne korzyści, które przemysł, biznes i indywidualni użytkownicy będą mogli czerpać z rozwoju tej koncepcji. Współpraca świata przemysłu, biznesu, nauki, rządów i organizacji standaryzujących jest kluczem do rozwiązania istniejących problemów i wykorzystywania tej idei na coraz szerszą skalę zarówno w zakresie ciągłego opracowywania nowych, jak i ulepszania dostępnych rozwiązań technologicznych związanych z IoT.

5

Bezpieczeństwo informacji na przykładzie międzynarodowej organizacji handlowej

W dobie globalizacji, Internetu, smartfonów oraz spektakularnie małych nośników pamięci, przepływ informacji stał się szalenie prosty. Uzyskanie jakichkolwiek danych nie stanowi już żadnego problemu. Problemem stało się zatrzymanie informacji i ograniczenie do niej dostępu. Każdy, kto korzysta z portali społecznościowych wie, jak łatwo jest uzyskać informacje o innych ludziach i jak trudno ograniczyć dostęp do swoich publikacji innym użytkownikom.

Z problemem tym zmagają się nie tylko pojedynczy ludzie, ale również firmy, organizacje, stowarzyszenia czy też rządy każdego kraju. Informatycy prześcigają się w opracowywaniu coraz lepszych zabezpieczeń, tworzą poziomy dostępów, uprawnienia oraz kodyfikację, aby sprawować jak największą kontrolę nad zasobami firmy. Należy sobie jednak zadać pytanie, czy to wystarczy, by zapewnić bezpieczeństwo informacji w organizacji.

Jedna z definicji przedstawia „bezpieczeństwo informacji" jako ochronę ważnych z punktu widzenia prawnego i biznesowego informacji przed nieuprawnionym korzystaniem, zniszczeniem, modyfikacją, zapewniając dostęp dla upoważnionej osoby. Błędne jest zatem przeświadczenie, że ochrona informacji to tylko i wyłącznie

zachowanie jej poufności.[41] W systemie zarządzania organizacją, ochrona informacji to zagadnienie zarządcze i organizacyjne, a nie tylko techniczne. Powinno ono naturalnie wpisywać się w proces zarządzania całościowym bezpieczeństwem organizacji.

- Zagrożenia bezpieczeństwa informacji można podzielić na trzy kategorie[42]:
- zagrożenia zewnętrzne – gdy zachodzi możliwość utraty danych na wskutek działania osób spoza firmy,
- zagrożenia wewnętrzne – spowodowane nieprawidłowym działaniem pracowników firmy, awarią sieci komputerowej czy też złośliwym oprogramowaniem,
- zagrożenia fizyczne – wynikające z fizycznego uszkodzenia sieci komputerowej, zarówno celowego, jak i przypadkowego.

Korzystanie z sieci Internet niesie za sobą największe zagrożenia utraty bezpieczeństwa informacji. Można je podzielić na kilka grup[43]:

- podsłuch transmisji danych w sieci,
- nieuprawnione korzystanie z zasobów systemu komputerowego,
- blokada lub spowolnienie usług systemu poprzez narzucenie dużej liczby zadań,
- utrata danych na wskutek działania złośliwego oprogramowania lub poprzez włamanie do systemu,
- fałszowanie informacji poprzez podszywanie się pod innego użytkownika, np., rozsyłanie poczty z cudzego adresu mailowego,
- fizyczne odcięcie źródła informacji od sieci komputerowej, np., awaria serwera lub kradzież.

Przyjrzyjmy się systemowi działania jednej z dużych organizacji handlowych. Przedsiębiorstwo, o którym mowa jest międzynarodową organizacją handlową, działającą na terenie Europy i Azji. Tylko w Polsce zatrudnia ok. 8 tysięcy pracowników. Placówki firmy rozlokowane są w ponad 40 miastach Polski i zajmują prawie 300 000m^2 powierzchni. Wielkość i skala prowadzonego przedsięwzięcia

[41] www.ksoin.pl/bezpieczenstwo_informacji_jako_wazny_element_bezpieczenstwa_calej_organizacji-strony, 11,278.html#.VDF8n6OFlX5, [05.10.2014].

[42] www.bbn.gov.pl/download/1/1002/bezpieczenstwoinformacji, [05.10.2014].

[43] M. Cieciura, *Wybrane problemy społeczne i zawodowe informatyki*, Warszawa 2012, s. 69.

narzuca również wykorzystanie dużej liczby systemów komputerowych, zarówno do przetwarzania i analizy danych jak i do prowadzenia magazynów i sprzedaży firmy.

Omawiana organizacja bardzo dba o *bezpieczeństwo danych*. Stworzone są mapy dostępów, które regulują możliwości udostępniania informacji. Na podstawie struktury firmy, do każdego stanowiska przypisane są aplikacje czy systemy, z których może pracownik korzystać. Uprawnienia nadawane są na wniosek przełożonego, który to wysyła odpowiednie zgłoszenie do działu IT. Zgłoszenia wysyłane są przez specjalnie do tego przygotowaną aplikację, w innej formie zlecenie nie zostanie przyjęte. Dostęp do aplikacji zgłoszeniowej mają również tylko osoby do tego uprawnione zgodnie z mapą dostępu. Można pracownikowi udzielić niestandardowych uprawnień, ale za pisemnym wnioskiem przełożonego, podpartym konkretnymi argumentami. Wniosek taki trafia do właściciela procesu, który ewentualnie wyraża zgodę na tymczasowe lub stałe uprawnienia dodatkowe.

Dostęp do wszystkich aplikacji i systemów jest uruchamiany na podstawie przyznanego indywidualnego loginu oraz hasła. Hasło posiada wymogi, co do ilości i jakości znaków, tak aby było trudne do rozszyfrowania. W zależności od ważności aplikacji lub finezji obsługującego ją informatyka, stopnie trudności utworzenia hasła mogą być różne. Niejednokrotnie nie może to być wyraz, występujący zarówno w języku polskim jak i angielskim. Sugestią są anagramy zdań, powiedzeń, czy też wierszy, które użytkownik będzie mógł w jakiś sposób zapamiętać, ale utrudni to rozszyfrowanie hasła przez niepowołane osoby. Dodatkowo ważność haseł wygasa najpóźniej po miesiącu czasu, wymuszając na użytkowniku jego zmianę.

Kadra menedżerska tej organizacji korzysta z co najmniej kilkunastu aplikacji czy systemów. Według informatyków, twórców zabezpieczeń, każda z nich powinna być zabezpieczona innym hasłem. Zapamiętanie wszystkich haseł jest zatem niemożliwe do zrealizowania. Pracownicy stosują metodę zapisywania haseł, co jest niedopuszczalne z punktu widzenia informatycznego. Jak zatem poradzić sobie z tak dużą ilości haseł, pamiętając dodatkowo o tym, że każdy prywatnie posiada przynajmniej jedno bankowe konto internetowe, facebooka, dziennik elektroniczny swoich dzieci, konto w sieci telefonicznej, pocztę elektroniczną, program bonusowy, itp.?

Każdy pracownik posiada zapis wszystkich haseł, niejednokrotnie stosując zasadę zmiany tylko jednego znaku w kolejnym haśle. Często takie samo hasło jest stosowane do wszystkich aplikacji, aby nie trudzić się w procesie logowania.

Następną kwestią są *poziomy uprawnień*. Sam dostęp do jakiegoś systemu nie oznacza wcale dostępu całkowitego. W zależności od zajmowanego stanowiska i specyfiki obszaru działalności, każdy pracownik ma inny poziom uprawnień do danych czy też do modyfikacji danych. Jest to szczególnie ważne ze względu na poziomy odpowiedzialności danych ludzi, a także stopnia tajności poszczególnych informacji. Niejednokrotnie jednak, pracownik dostaje zadanie stworzenia raportu, który wykracza poza obszar jego uprawnień. Jest zmuszony zatem, aby prosić o dane pracownika z większymi uprawnieniami. Wielkość obsady czy zakres obowiązków nie zawsze pozwala na takie działania, w konsekwencji czego, dostęp jest przekazywany osobie postronnej.

To samo dzieje się, gdy występuje presja czasu i o sukcesie danego przedsięwzięcia decyduje *szybkość reagowania*. Wówczas to brak osoby uprawnionej do pożądanej wiedzy blokuje cały proces. Wtedy kwestia bezpieczeństwa nie odgrywa już tak istotnej roli i na pierwszy plan wysuwa się osiągnięcie zamierzonego celu. W konsekwencji, dostępy są przekazywane innym osobom z pominięciem wszystkich formalności i zasad bezpieczeństwa.

W omawianym problemie ogromną rolę odgrywa *czynnik ludzki*. W dużych organizacjach procesy są mocno sformalizowane i wymagają niejednokrotnie zachowania zasady „dwóch par oczu". Tak jest w przypadku większości procesów związanych z przepływem pieniężnym. Jest to oczywiście mocno uzasadnione i racjonalne postępowanie, gdyż to w tym obszarze najczęściej dochodzi do różnego rodzaju malwersacji i nadużyć. W opisywanej organizacji procesy przekazywania informacji są tak stworzone, aby na każdym etapie była konieczność kontroli działania. Jednak obecny rynek wymusza na firmach jak największą zyskowność przedsięwzięcia. Tego oczekuje także zarząd firmy a przede wszystkim akcjonariusze czy udziałowcy przedsiębiorstwa. Jednym z najczęściej stosowanych sposobów na osiągnięcie wysokiego zysku jest redukcja kosztów. Wiele firm uważa, że największym kosztem organizacji jest pracownik. Co za tym idzie, organizacja stawia na wysoką produktywność, ograniczając do minimum zatrudnienie. Nie zawsze bierze jednak pod

uwagę warunki bezpieczeństwa procesu. Aby dokonać formalności, pracownicy „obchodzą" system, udostępniając sobie dostępy do aplikacji czy kody weryfikujące.

Organizacje, tworząc mapy dostępów i poziomy uprawnień chcą oprócz zabezpieczenia danych, zapewnić *identyfikowalność działań*. Dlatego też każdy pracownik ma nadany indywidualny login bądź numer identyfikacyjny, który pozwoli na pełną kontrolę operacji danej osoby. Firma wiele zyskuje dzięki takim praktykom, przede wszystkim jest w stanie w dowolnym momencie wskazać autora danego działania, przypisując mu zarówno zasługi dla firmy jak i wykroczenia. Jednak w przypadku, gdy liczba uprawnionych osób jest niewystarczająca do prawidłowego wykonania danego zadania, następuje upublicznienie dostępu. Odpowiedzialność rozmywa się na grupę ludzi, chociaż oczywiście konsekwencje ponosi właściciel uprawnień. I tu dochodzi do sytuacji tzw. zamkniętego koła, gdyż w przypadku otrzymania kary za udostępnienie uprawnień, pracownik natychmiast blokuje dostęp osobom postronnym. To z kolei powoduje opóźnienie w wykonaniu wielu zadań lub też wymusza konieczność ciągłego zaangażowania osoby dysponującej dostępem.

Należy jeszcze poruszyć problem kosztów w firmie. To bowiem z ich powodu większość organizacji wprowadza *centralizację usług IT*, tworząc działy Help Desk-u. Zarządzanie całym systemem informatycznym, bez względu na wielkość i rozproszenie firmy, znajduje się wówczas w jednym miejscu, w jednej komórce. Podobnie rzecz ma się w opisywanej firmie. Porozumiewanie się tutaj z tym działem odbywa się poprzez odpowiednie do tego przygotowane aplikacje. Jest to bardzo wygodne narzędzie, jednak niesie ze sobą pewne konsekwencje. Komunikacja ta bowiem jest raczej jednostronnie czynna. Uniemożliwia to z jednej strony prowadzenie długich dysput na zgłaszane problemy, z drugiej zaś ogranicza się jedynie do zasygnalizowania problemu bez możliwości dodatkowych wyjaśnień. Ten sposób porozumiewania wymusza również zwięzłość wypowiedzi, w postaci konkretnych i rzeczowych komunikatów. Należy zauważyć jednak, że nie wszyscy pracownicy, a nawet ich zdecydowana większość, nie operują językiem specjalistycznym z dziedziny informatyki, co w konsekwencji wpływa na brak jednoznaczności wypowiedzi. Tym samym rodzi to często pomyłki i wywołuje nieporozumienia. Dodatkowo skala wielkości zgłaszanych problemów w stosunku do wielkości danej komórki IT, powoduje wydłużenie w czasie szybkości reagowania.

Kolejnym newralgicznym tematem są *różnice kulturowe i uwarunkowania organizacyjne* występujące w poszczególnych społecznościach. Firmy, które działają na obszarach wielu krajów a tym bardziej kontynentów, muszą uwzględniać odmienność w działalności prowadzonej na terenie tych państw i dostosowywać się do obowiązujących przepisów i zasad. Często jednak występuje niezrozumienie konieczności wprowadzania zmian tylko dla jednego środowiska. Dział IT odrzuca wniosek o zmianę z powodu niezrozumienia istoty i ważkości problemu, powodując wydłużenie jakiegoś procesu.

Bezpieczeństwo informacji jest również mocno powiązane z *powszechnym dostępem do Internetu*. Łatwość przesyłu informacji tą droga jest tak duża, że firmy ograniczają do minimum dostęp do sieci. Wiele firm zakłada blokady do korzystania z prywatnej poczty internetowej, uniemożliwia dostęp do portali społecznościowych typu Facebook czy Twitter. Prowadzi również monitoring odwiedzanych stron, aby śledzić działania pracownika. Komputery są specjalnie przystosowywane, zazwyczaj mają blokadę portów usb oraz brak stacji dysków, aby uniemożliwić zapisywanie danych na przenośne nośniki pamięci. Niejednokrotnie również istnieje blokada wysyłania maili na prywatne konta. Dopuszczalne są tylko operacje pomiędzy firmowymi użytkownikami.

Analizując wszystkie opisane wcześniej działania można wyciągnąć wnioski, że nie zawsze założenia administratorów systemów mogą być zrealizowane. Można odnieść wrażenie, że teoria nie nadąża za praktyką, a praktyka nie do końca uwzględnia założenia teorii. Życie, zwłaszcza organizacyjne, wymusza bowiem wiele sytuacji i obejmuje szereg działań na które trzeba reagować na bieżąco, bez zbędnej zwłoki.

Jest jeszcze drugi, istotny aspekt tej sprawy, a mianowicie *czynnik ludzki i jego poziom świadomości*. Niewiele osób zdaje sobie sprawę, że udostępniając komuś swojego firmowego e-maila, może spowodować wyciek informacji poza organizację. Niewiele też osób próbuje przeciwstawiać się udostępnianiu haseł do aplikacji, stawiając na pierwszym miejscu szybkość reagowania na potrzeby rynku. Należy zadać sobie pytanie, czy jest to wynik małej świadomości pracowników czy może raczej odgórnego przyzwolenia na zaistniałą sytuację. Ponadto, czy zaniechanie takich praktyk przez poszczególnych pracowników, nie wymusiłoby w końcu na organizacji zmiany zasad działania?

6

Sprzętowe rozwiązania informatyczne zapewniające bezpieczeństwo tożsamości cyfrowej

6.1. WPROWADZENIE

Zdając sobie sprawę ze znaczenia informacji przechowywanej w systemach informatycznych oraz chcąc spełnić wymogi prawne związane z bezpieczeństwem danych osobowych [ZEG14], przedsiębiorcy muszą zdecydować jak i czym optymalnie chronić swoje zasoby. Oznacza to, że powinna zostać zabezpieczona poufność (brak dostępu przez osoby nieuprawnione), integralność (oryginalność) oraz dostępność danych dla osób uprawnionych. Te trzy czynniki w skrócie CIA (ang. *Confidentiality, Integrality, Aviability*) [CHI12] muszą zostać wzięte pod uwagę przy wyborze sposobu zabezpieczenia danych tak, by był optymalny dla przedsiębiorstwa i uwzględniał jego specyfikę (wielkość, potrzebę zabezpieczeń, nakłady na zakup i eksploatację urządzeń itp.). Dodatkowo norma ISO[44] [GIO07] rozszerza wymagania, które muszą być spełnione by informacja była traktowana jako bezpieczna o: rozliczalność (jednoznaczne przyporządkowanie działań danemu podmiotowi), autentyczność (pewność, że tożsamość danego zasobu lub użytkownika, który ma do

[44] PN-ISO/IEC-17799:2005.

niego dostęp jest taka sama jak deklarowana), niezaprzeczalność (brak możliwości wyparcia się działań przez ich sprawcę) oraz niezawodność (spójność i powtarzalność wyników przy poszczególnych działaniach)[45].

Zaplanowanie i przemyślenie działań związanych z bezpieczeństwem danych jest wymuszane przez przepisy prawa, działania konkurencji oraz mechanizmy rynkowe. Ustawa o ochronie danych osobowych [UST97] nakłada na przedsiębiorcę konieczność opracowania i wdrożenia polityki bezpieczeństwa, w której skład wchodzi m.in. *Określenie środków technicznych i organizacyjnych niezbędnych dla zapewnienia poufności, integralności i rozliczalności*. Niewłaściwie zabezpieczony dostęp do danych naraża przedsiębiorstwo na ryzyko ich kradzieży lub utraty, co może skutkować utratą przewagi konkurencyjnej, klientów czy danych archiwalnych wymaganych przez organy państwowe (groźba odpowiedzialności karnej czy karno-skarbowej). W takiej sytuacji może zadziałać też mechanizm rynkowy eliminujący z przestrzeni gospodarczej podmioty nieprzystosowane. Eliminacją może skutkować odpływ klientów spowodowany utratą reputacji, powództwa cywilne czy problemy organizacyjne wynikające z utraty bądź kradzieży danych.

Przedsiębiorcy do wyboru mają trzy metody uwierzytelniania, czyli potwierdzenia praw dostępu do danych: opartą o wiedzę, posiadany przedmiot lub cechy fizyczne. I tak, po zadeklarowaniu swojej tożsamości użytkownik dostarcza dowód, którym może być: hasło, hasło jednorazowe wygenerowane przez urządzenie zwane tokenem bądź niepowtarzalny układ żył krwionośnych dłoni zeskanowany przez specjalne urządzenie. Wybór metody zabezpieczającej powinien być starannie przemyślany i poprzedzony analizą wad i zalet dostępnych metod.

6.2. CEL I UZASADNIENIE PRACY

Celem niniejszej pracy jest przegląd oraz porównanie dwóch grup metod uwierzytelnienia: z użyciem przedmiotu i cech biometrycznych. Publikacja w założeniu ma stanowić uzupełnienie wiedzy użytkowników systemów informatycznych oraz

[45] Definicje opracowane na podstawie normy PN-I-13335-1.

może być wykorzystywana jako pomoc dla przedsiębiorców w wyborze metody zabezpieczenia systemów informatycznych.

Hasła, jako metoda uwierzytelnienia, nie zostały ujęte w zestawieniu. Jest to decyzja oparta o fakt, że hasła w obecnych czasach są niejako opcją domyślną. Programy i systemy operacyjne są wyposażone w możliwość zakładania kont różnym użytkownikom, sterowania ich uprawnieniami i przywilejami. Stosowanie haseł nie wymaga zatem podejmowania wyboru, taka opcja jest po prostu dostępna i co ważne zwykle darmowa[46]. W gestii przedsiębiorcy jest ustalenie i przestrzeganie polityki haseł.

Wybór metody z użyciem przedmiotu lub cech biometrycznych natomiast niesie ze sobą konieczność poniesienie inwestycji. Stąd zupełnie inne wydają się potrzeby informacyjne służące do wyboru tokenu, karty czy czytnika niż korzystania z wbudowanej opcji haseł.

6.3. PRZEDMIOTY UWIERZYTELNIAJĄCE

Zasadą działania przedmiotów uwierzytelniających jest generowanie właściwej informacji w oparciu o szyfr rozumiany przez przedmiot uwierzytelniający i oprogramowanie zainstalowane w urządzeniu (stacjonarnym lub mobilnym), które służy do uzyskania dostępu do danych.

Z uwagi na formę odpowiedzi można przedmioty podzielić na:

1. generujące jednorazowe hasła, które użytkownik sam wpisuje do systemu,
2. generujące zaszyfrowany ciąg bitów przekazywany z przedmiotu do systemu.

Co ważne określenie *przedmiot* należy odczytywać w szerokim ujęciu, gdyż oprócz odrębnych urządzeń może to być także aplikacja uwierzytelniająca (tzw. *soft token*) zainstalowana w urządzeniu, którego głównym celem nie jest zapewnienie uwierzytelnienia np. w telefonie komórkowym.

[46] Częstą polityką firm produkujących oprogramowanie dedykowane jest zapewnienie określonej liczby bezpłatnych kont użytkowników. Jednak pewne funkcjonalności np. zwiększenie liczby kont czy dodatkowe narzędzia do zarządzania tożsamościami mogą być dodatkowo płatne.

6.3.1. TOKEN OTP (ANG. ONE TIME PASSWORD TOKEN)

Są to niewielkie urządzenia, które przypominają mały kalkulatorek lub brelok do kluczy (Rys. 1). Zwykle są programowane dla jednego konkretnego użytkownika. Pracują na zasadzie współdzielenia szyfru z serwerem uwierzytelniającym (ang. s*hared secret).* Można je podzielić na:

1. **tokeny działające na zasadzie wezwanie – odpowiedź**

Token zawiera elementy: wyświetlacz, na którym wyświetlane jest hasło jednorazowe, przycisk inicjujący generowanie hasła i klawiatura.
Uwierzytelnienie przebiega wg poniższego schematu:

- użytkownik wykonuje operację wymagającą potwierdzenia z użyciem tokena,
- serwer w celu uwierzytelnienia przesyła wygenerowany ciąg cyfr (ang. *Challenge*),
- token generuje hasło będące odpowiedzią (ang. *Response*),
- użytkownik wprowadza hasło do systemu żądającego uwierzytelnienia z użyciem tokena.

2. **tokeny z synchronizacją czasową**

Zawierają wyświetlacz i przycisk, który powoduje wygenerowanie hasła ważnego przez określony, krótki czas (zwykle 60 sek.). Działają one w synchronizacji czasowej z aplikacją wymagającą uwierzytelnienia.

3. **tokeny oparte o licznik**

Oprócz klucza generowanie hasła wymaga właściwego stanu licznika identycznego ze stanem licznika serwera.

Rysunek 1. Przykładowe tokeny OTP typu „kalkulatorek" i „brelok"
Źródło: [HID14]

6.3.2. TOKEN USB I TOKEN HYBRYDOWY

Token USB (Rys. 2) jest rozwiązaniem równoważnym kartom inteligentnym stykowym. Podstawową różnicą jest zintegrowanie karty i czytnika.

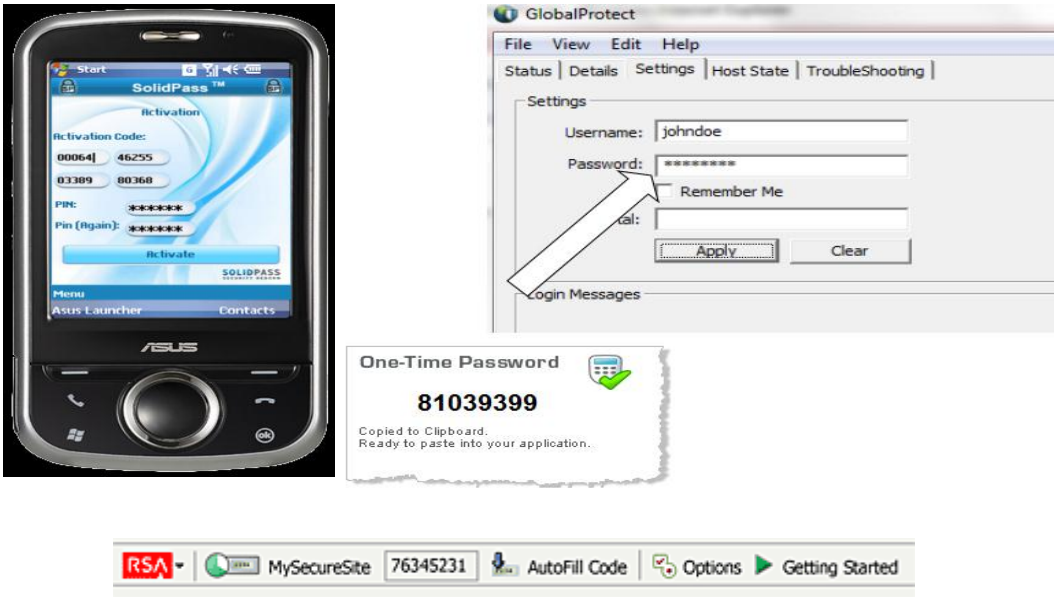
Rysunek 2. Przykładowy token USB
Źródło: [KRY14]

Token hybrydowy (Rys. 3) to rozwiązania łączące token OTP z tokenem USB. Urządzenie posiada wyświetlacz na hasła jednorazowe, przycisk do ich generowania oraz złącze USB. Ten rodzaj tokena może przechowywać certyfikaty i klucze tak jak karta inteligentna.

Rysunek 3. Token hybrydowy
Źródło: [WIK14]

6.3.3. TOKENY PROGRAMOWE

Tokeny programowe (Rys. 4) generujące hasło jednorazowe mają postać aplikacji, która może być zainstalowana na komputerze stacjonarnym (ang. *PC Soft Token*), urządzeniu mobilnym (ang. *Mobile Soft Token*) lub jako pasek narzędziowy w przeglądarce (ang. *Web Soft Token*). Taki token jest w użytkowaniu konkretnego użytkownika, ale może być używany na wielu urządzeniach. Jest szczególnie przydatny w pracy na odległość oraz bankowości elektronicznej.



Rysunek 4. Tokeny programowe
Źródło: [SOL14], [PAL14], [EMC14]

6.3.4. KARTY KRYPTOGRAFICZNE

Karty kryptograficzne (Rys. 5) wykorzystywane w przedsiębiorstwach jako narzędzia uwierzytelnienia to zwykle małe urządzenia przypominające kartę bankomatową[47]. Wymagają użycia dodatkowego sprzętu: czytnika kart. Można je podzielić wg różnych kryteriów na [SZY03]:

1. stykowe i bezstykowe (kryterium: komunikacja z urządzeniami odbiorczymi),
2. karty pamięciowe i mikroprocesorowe czyli karty inteligentne z ang. *SmartCards* (kryterium: obecność wbudowanego procesora).

Karty stykowe (ang. *Contact Cards*) komunikują się z czytnikiem za pomocą pokrytego złotem styku, który służy także do zasilania karty podczas jej użytkowania w czytniku.

[47] Karty bankomatowe są również de facto kartami kryptograficznymi.

Karty bezstykowe (ang. *Contactless Cards*) występujące rzadziej niż stykowe nie wymagają fizycznego połączenia z czytnikiem. Komunikacja odbywa się za pomocą fal radiowych, zasilanie natomiast może być z baterii lub z wykorzystaniem cewek pobudzanych polem elektromagnetycznym. Czytnik może być ukryty np. w ścianie. Karta wykorzystywana jest m.in. tam, gdzie identyfikacja użytkowników odbywa się z dużą częstotliwością.

W porównaniu z tokenami karta inteligentna (zaopatrzona w procesor) ma dużo szerszy zakres zastosowań. Może być ona stosowana do fizycznej kontroli dostępu zarówno do zasobów jak i pomieszczeń, stanowić identyfikator uprawnień osobistych czy potwierdzać oryginalność dokumentów [SZY03].

Karta przechowuje klucze prywatne posiadacza karty. Ich bezpieczeństwo determinuje szereg faktów: klucz prywatny nigdy nie opuszcza karty, operacje szyfrowania czy poświadczania oryginalności dokumentu dokonuje się w karcie, konstrukcja urządzenia wyklucza manipulacje danymi [WIK14].

Rysunek 5. Karta kryptograficzna wraz z czytnikiem
Źródło: [WIK14b]

6.4. UWIERZYTELNIENIE BIOMETRYCZNE

Potwierdzenie praw dostępu do danych zasobów może być potwierdzone za pomocą immanentnych cech użytkownika, zarówno fizycznych jak i behawioralnych.

6.4.1. CHARAKTERYSTYKA METOD UWIERZYTELNIENIA

Cechy, które mogą posłużyć uwierzytelnieniu oraz metody ich wykorzystania to głównie [BAN13]:

- odcisk palca – układ punktów charakterystycznych (minucji),
- tęczówka oka – cechy charakterystyczne tęczówki,
- naczynia krwionośne palca – charakterystyczny wzór naczyń krwionośnych,
- naczynia krwionośne dłoni – charakterystyczny wzór naczyń krwionośnych,
- geometria twarzy – analiza obrazu 2D i 3D,
- geometria dłoni – proporcja i wymiary,
- głos – parametry głosu,
- podpis odręczny – dynamika pióra i analiza obrazu 2D.

Wyżej wymienione metody charakteryzują się różnym stopniem kontaktu z urządzeniem sczytującym, co przekłada się na postrzeganie ich przez użytkownika. Można tu wyróżnić [PLU14]:

- Metody interakcyjne, czyli wymagające fizycznego kontaktu z urządzeniem np. weryfikacja z użyciem odcisku palca lub geometrii dłoni. Postrzegane są jako mniej higieniczne.
- Metody nieinterakcyjne takie jak skanowanie siatkówki czy badanie głosu.

6.4.2. PROCES UWIERZYTELNIENIA Z UŻYCIEM METOD BIOMETRYCZNYCH

Elementy konieczne do potwierdzenia tożsamości użytkownika to urządzenie sczytujące dane, wzorzec referencyjny oraz sam użytkownik.

Urządzenia służące wprowadzaniu danych są dedykowane do każdej z metod. Stąd wyróżniamy: czytniki linii papilarnych (Rys. 6), skanery tęczówki, czytniki układu naczyń krwionośnych oraz rejestrator geometrii twarzy/kamera, czytnik geometrii

dłoni, dowolny rejestrator dźwięku (zapis w postaci cyfrowej) np. telefon, dedykowany tablet z dotykowym ekranem.

Wzorzec referencyjny to wzór w postaci cyfrowej, utworzony na podstawie danych dostarczonych przez użytkownika (np. odcisku palca), który będzie służył jako punkt odniesienia podczas weryfikacji użytkownika. Po utworzeniu wzorca zwykle następuje faza treningowa, podczas której system uczy się rozpoznawać cechy użytkownika przez sensory. Wzorzec referencyjny może być zmieniany (uaktualniany) po każdej udanej weryfikacji (adaptacja). Uwzględniony tym samym staje się proces zmian zachodzących w organizmie człowieka (starzenie się, choroba itp.). Dotyczy to metod bazujących na cechach, które mogą ulec zmianie np. geometria twarzy [DAG14].

Proces autoryzacji polega na wprowadzeniu próbek do systemu (fizyczne sczytanie przez sensory oraz zamiana na sygnał cyfrowy), porównaniu ich ze wzorcem referencyjnym a następnie w zależności od wyniku tego porównania – udzielenie dostępu, bądź odrzucenie żądania.

Wyróżnione są dwa warianty porównania próbek ze wzorcem [DAG14]:

- Za pomocą identyfikacji, czyli ustalenie, kim jest osoba deklarująca chęć dostępu do chronionych zasobów. W tym celu następuje porównanie próbek z każdym wzorcem przechowywanym w bazie, aż do znalezienia właściwego dopasowania.
- Z użyciem prostej weryfikacji, czyli porównania próbki z jednym wzorcem użytkownika, którego tożsamość została zadeklarowana lub który jest użytkownikiem domyślnym.

Stąd można wyróżnić dwa miejsca przechowywania wzorca referencyjnego: w bazie danych przedsiębiorstwa oraz w urządzeniu służącym weryfikacji.

Rysunek 6. Czytnik linii papilarnych
Źródło: [MOR14]

6.4.3. WIARYGODNOŚĆ UWIERZYTELNIENIA

W przeciwieństwie do metod, które działają na sposób zero-jedynkowy, czyli przedmiotów i haseł, stosowanie metod biometrycznych jest obciążone ryzykiem niewłaściwej identyfikacji użytkownika. Ryzyko to możemy podzielić na [BAN13]:

- Akceptację nieuprawnionej osoby (udział w ogólnej liczbie przeprowadzonych weryfikacji to FAR, czyli z ang. *False Acceptance Rate*) – spowodowana znacznym zbliżeniem cech fizycznych lub behawioralnych, zawodnością urządzenia lub poziomem dokładności badania.
- Odrzucenie uprawnionej osoby (udział w ogólnej liczbie przeprowadzonych weryfikacji to FRR, czyli z ang. *False Rejection Rate*) – spowodowane najczęściej zmianą jej cech fizycznych lub behawioralnych niemieszczącą się z zakresie adaptacyjnym (np. chrypa spowodowana przeziębieniem, uszkodzenie opuszki palca itp.) lub innymi zakłóceniami (np. okulary, oświetlenie).

Im większy udział FRR w ogólniej liczbie weryfikacji, tym ta metoda staje się bardziej uciążliwa dla użytkownika. Z kolei im większy FAR, tym mniejsze staje się

bezpieczeństwo systemu. Oba współczynniki są ze sobą powiązane. Obniżenie dokładności pomiaru zmniejsza udział FRR (system bardziej przyjazny użytkownikowi), ale za to zwiększa udział FAR. I analogicznie, zwiększenie dokładności pomiaru skutkuje podwyższeniem bezpieczeństwa systemu kosztem dogodności jego użycia [PLU14].

Konieczny jest kompromis, uwzględniający oba te czynniki (osiągnięcie równowagi między FAR a FRR, czyli EER z ang. *Equal Error Rate*), wybór metody, której udział zarówno FAR jak i FRR są stosunkowo niskie lub zastosowanie rozwiązania, które łączy dwie metody biometryczne np. badanie linii papilarnych i układu naczyń krwionośnych. Zazwyczaj oznacza to wyższe nakłady finansowe oraz konieczność rozważania innych czynników wpływających na wybór np. inwazyjność metody.

6.5. UWIERZYTELNIENIE MIESZANE

Urządzenia stosowane do potwierdzenia tożsamości użytkownika zwykle bazują na kombinacjach różnych metod uwierzytelnienia.

6.5.1. URZĄDZENIA Z WERYFIKACJĄ DWUSTOPNIOWĄ

Najczęściej stosowaną kombinacją jest połączenie przedmiotu z zabezpieczeniem kryptograficznym (hasłem). Tak działają np. tokeny OTP typu kalkulator. Przyciski zamontowane w obudowie stosowane są do wprowadzenia PINu (Rys. 1). Poprawnie wprowadzony PIN skutkuje wygenerowaniem jednorazowego hasła. Hasło jako drugi poziom weryfikacji zwiększa znacząco bezpieczeństwo uwierzytelnienia, zmniejszając jednak komfort jego stosowania.

Innym wariantem jest kombinacja przedmiot + zabezpieczenie biometryczne np. karta inteligentna / token OTP zabezpieczone czytnikiem linii papilarnych (Rys. 7).

Przed dokonaniem autoryzacji działań, użytkownik musi wczytać swoje dane biometryczne, które są porównywane z wzorcem referencyjnym. To porównanie może się odbywać na dwóch zasadach [STR05]:

- Poza kartą (w systemach match-off-card), gdy próbka oraz wzorzec referencyjny są wysyłane do systemu informatycznego, w którym następuje porównanie.
- W karcie (w systemach typu match-on-token), który przetwarza dane zarówno próbki, jak i wzorca, a do systemu wysyła potwierdzenie dopasowania.

Rysunek 7. Token OTP zabezpieczony czytnikiem linii papilarnych
Źródło: [SOF14a]

Trzecim wariantem dwustopniowej weryfikacji jest połączenie biometrii z zabezpieczeniem kryptograficznym. Z uwagi na FRR umożliwia się użytkownikowi potwierdzenie swojej tożsamości w inny sposób niż tylko z użyciem biometrii, czyli poprzez podanie hasła. Hasło jest zatem niejako zapasowym sposobem potwierdzenia uprawnień do zasobów. Im większe FRR, tym większa jego przydatność. Przykładem zastosowania tego sposobu może być zabezpieczenie

dostępu do komputera metodą weryfikacji geometrii twarzy. Z uwagi na np. inne oświetlenie, stosowanie okularów korekcyjnych, czy uszkodzenia (opuchlizna po ukąszeniu owada), może nastąpić odmowa dostępu i możliwość skorzystania z opcji wprowadzenia hasła.

6.5.2. URZĄDZENIA Z WERYFIKACJĄ TRÓJSTOPNIOWĄ

Przykładem urządzenia posiadającego zabezpieczenie kryptograficzne i biometryczne jest token USB zaopatrzony w czytnik odcisków palców (Rys. 8). PIN jest wprowadzany podczas procesu autoryzacji.

Rysunek 8. Token USB zabezpieczony czytnikiem linii papilarnych
Źródło: [SOF14b]

6.6. WYBÓR METODY UWIERZYTELNIENIA

Nie ma metody, którą można uznać za najlepszą w oderwaniu od charakterystyki przedsiębiorstwa i zasobów, do których ochrony będzie służyć. Stąd wybór właściwego rozwiązania powinien być poprzedzony badaniem zarówno potrzeb przedsiębiorstwa, jak i analizą dostępnej oferty.

6.6.1. PORÓWNANIE ROZWIĄZAŃ

Zarówno metody oparte o posiadanie urządzeń, jak i biometrię mają swoje wady i zalety. Zostały one ujęte w poniższej tabeli.

Tabela 1. Podstawowe wady i zalety metod uwierzytelniania

Metoda	Zalety	Wady
Co masz? (przedmiot)	• Utrata przedmiotu nie ma wpływu na życie osobiste pracownika • Duże bezpieczeństwo danych (silna kryptografia, aktualizacje szyfru itp.)	• Zależność od czynników technicznych (wyczerpanie baterii, uszkodzenie) • Możliwość utraty, kradzieży • Pewna uciążliwość szczególnie przy wielu operacjach dziennie • Konieczność instalowania dodatkowego oprogramowania (w niektórych przypadkach)
Czym jesteś? (cecha)	• W większości przypadków duży komfort użytkowania • Brak konieczności posiadania dodatkowych przedmiotów • Duże bezpieczeństwo danych	• Kompromitacja (wyciek) danych biometrycznych (wzorca referencyjnego) jest czasem nieodwracalna (np. badanie tęczówki) • Trudno zmienić wzorzec referencyjny • Powiązanie z życiem osobistym pracownika • Brak akceptacji pewnej grupy osób (jej wielkość zależy od metody, szczególnie inwazyjności) • Możliwość nie uzyskania uprawnionego dostępu (FRR) lub uzyskania nieuprawnionego dostępu (FAR)

Źródło: opracowanie własne

W ramach metod opartych o posiadanie przedmiotu istnieje szereg czynników, które mogą wpłynąć na wybór konkretnego rozwiązania. Zestawienie czynników przedstawia Tabela 2.

Tabela 2. Porównanie rozwiązań opartych o posiadanie przedmiotu

	Token sprzętowy	Token software'owy	Karta inteligentna
Bezpieczeństwo	Wysokie	Wysokie	Wysokie
Zasilanie	Baterie	Baterie innego urządzenia	Baterie/cewka/inne urządzenie
Czas życia	Ograniczony (24, 36, 48, 60 mcy)	Ograniczony (6, 12, 24, 36, 48, 60, 120 mcy)	Nieograniczony
Dodatkowe zabezpieczenie w razie kradzieży	Tak/Nie	Tak	Tak
Główne czynniki ryzyka przechwycenia danych	Podatność na atak Man-In-The-Middle, Man-In-The-Browser	Bezpieczeństwo aplikacji zależne od bezpieczeństwa urządzenia, na którym jest zainstalowana	Podatność na Side Channel Attack
Konieczność instalowania oprogramowania	Nie/Tak	Tak	Tak
Ryzyko dodatkowe	Rozsynchronizowanie licznika lub czasu	Skopiowanie klucza	-
Koszt urządzeń	Średni	Niski	Średni
Wielkość urządzeń	Mała	-*	Mała
Wygoda użytkowania	Średnia	Wysoka	Średnia

* - wynik zależny od konkretnego przypadku

Źródło: opracowanie własne na podstawie: [RSA14], [SZY03], [KRO08], [VER14], [PAS07]

Sektorem, który prawdopodobnie najbardziej powszechnie wykorzystuje uwierzytelnienie biometryczne i jednocześnie najintensywniej je rozwija, jest sektor bankowy (liczne wdrożenia bankomatów biometrycznych w Japonii, Indiach, Brazylii czy w Polsce). Stąd liczne analizy przydatności poszczególnych rozwiązań biometrycznych. W Tabeli 3 zaprezentowano porównanie metod, które mogą być użyte także poza sektorem usług finansowych.

Tabela 3. Porównanie rozwiązań opartych o badane cechy biometryczne

Metoda	Bezpieczeństwo metody	Koszt urządzeń	Wielkość urządzeń	Akceptacja użytkowników
Odcisk palca	Średnie	Niski/Średni	Mały/Średni	Niska
Tęczówka oka	Wysokie	Wysoki	Duży	Niska
Naczynia krwionośne palca	Wysokie	Średni	Mały/Średni	Wysoka
Naczynia krwionośne dłoni	Wysokie	Średni	Średni/Duży	Średnia
Geometria twarzy	Niskie	Średni	Średni/Duży	Średnia
Geometria dłoni	Niskie	Średni	Duży	Średnia
Głos	Średnie	- *	-*	Wysoka
Podpis odręczny	Niskie	Średni	Średni/Duży	Wysoka

* - wynik zależny od konkretnego przypadku

Źródło: [BAN13]

Tabela 4 prezentuje ranking metod biometrycznych w sześciu kategoriach:

- akceptowalności – która ma szczególne znaczenie z uwagi na stosunkowo niewielki kontakt przeciętnego użytkownika z biometrią oraz dylematy natury etycznej,
- łatwości użycia – która wpływa na akceptację rozwiązania oraz jego koszto- i czasochłonność,

- czas weryfikacji (przykładowe wartości to: 0,5s – analiza linii papilarnych, 14s – analiza głosu) [PLU14],
- czas rejestracji użytkownika, wpływający na czas i koszty wdrożenia rozwiązania
- wiarygodność metody mierzona wielkością EER (przykładowe wartości to: <0,5% – analiza tęczówki, 5% – analiza linii papilarnych) [PLU14],
- wielkości wzorca, wpływającej na ilość pamięci koniecznej do gromadzenia danych biometrycznych pracowników (przykładowe wielkości to: 9 B – wzorzec geometrii dłoni, 2500 B – wzorzec naczyń krwionośnych dłoni) [PLU14].

Dane zaprezentowano w układzie od pozycji najkorzystniejszej do najmniej korzystnej.

Tabela 4. Klasyfikacja technik biometrycznych

Parametr	Biometria
Akceptowalność	Głos, rysy twarzy, naczynia palca, linie papilarne, kształt dłoni, tęczówka, podpis odręczny, siatkówka
Łatwość użycia	Głos, rysy twarzy, kształt dłoni, naczynia palca i dłoni, linie papilarne, tęczówka, siatkówka
Czas weryfikacji	Linie papilarne, naczynia palca, tęczówka, kształt dłoni, naczynia dłoni, siatkówka, głos
Czas rejestracji	Linie papilarne, naczynia palca, naczynia dłoni, tęczówka
Wiarygodność – bezpieczeństwo	Siatkówka, tęczówka, naczynia palca, linie papilarne, kształt dłoni, głos, sposób pisania na klawiaturze
Wielkość wzorca	Kształt dłoni, siatkówka, tęczówka, naczynia palca, linie papilarne, sposób pisania na klawiaturze, głos, naczynia dłoni

Źródło: [PLU14]

6.6.2. PRZESŁANKI WYBORU ROZWIĄZANIA ZWIĄZANE Z PRZEDSIĘBIORSTWEM

Jest wiele czynników, które należy uwzględnić dokonując wyboru rozwiązań służących uwierzytelnieniu. Poniżej zaprezentowano wybrane z nich:

1. Zasoby podlegające ochronie i sposób ich wykorzystywania

Określenie zasobów, które powinny być chronione w przedsiębiorstwie jest uzależnione m.in. od przepisów prawa (Ustawa z dn. 29 sierpnia 1997 r. o ochronie danych osobowych; 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; inne przepisy szczególne) i wyboru przedsiębiorcy.

Zasoby przedsiębiorstwa, czyli dane (w formie papierowej i cyfrowej), urządzenia, aplikacje, towary, środki pieniężne i inne przedmioty podlegające ochronie przed ujawnieniem, nieuprawnionym użyciem, kradzieżą i zniszczeniem, mogą być zabezpieczone z użyciem opisanych uprzednio metod. Przedsiębiorca powinien zidentyfikować te zasoby, określić potrzebę i poziom bezpieczeństwa, który należy im zapewnić uwzględniając optymalizację kosztów, racjonalizację ryzyka i straty czasu pracy. Przykładowo posiadane przedmioty lub cechy osobiste pracowników mogą być wykorzystane nie tylko do zabezpieczenia logicznego (uwierzytelnienie w systemie informatycznym), ale i fizycznego zasobów. Karty inteligentne mogą służyć jako zamiennik klucza do pomieszczeń z zakazem wstępu dla osób nieautoryzowanych. Inna będzie jednak potrzeba zabezpieczenia drzwi do klubu sportowego, a inna do laboratorium.

Zarówno przedmioty uwierzytelniające, jak i dane biometryczne też są zasobami podlegającymi ochronie. Możliwość zapewnienia im bezpieczeństwa oraz odpowiednio pojemne nośniki (zależne od wielkości wzorca) powinny być również uwzględnione. Dane biometryczne, a w szczególności wzorzec referencyjny wymagają bardzo silnej ochrony, jeśli są przechowywane w bazie danych biometrycznych. Alternatywą jest przechowywanie ich w urządzeniu uwierzytelniającym, co może obniżyć koszty funkcjonowania całego systemu.

Ważny jest także sposób korzystania z zasobów. Inaczej wygląda sytuacja, gdy pracownik uwierzytelnia się w zakładzie pracy, korzystając z własnego komputera bez dostępu do Internetu, a inaczej, gdy istotnym narzędziem jego pracy jest urządzenie mobilne lub, gdy często opuszcza miejsce pracy lub współużytkuje komputer. Wtedy takie czynniki jak wielkość urządzenia czy jego zabezpieczenie przez nieuprawnionym użyciem stają się bardzo istotne.

Na wyniki przedsiębiorstwa przekłada się brak możliwości korzystania z zasobów osób uprawnionych, co może być spowodowane: awariami urządzeń, wyczerpaniem się baterii (tokeny) czy kradzieżą, co też powinno być uwzględnione.

2. Wielkość przedsiębiorstwa, jego zasoby finansowe oraz liczba jego pracowników

Dokonując wyboru konkretnego rozwiązania, szczególnie wyboru metody uwierzytelnienia między przedmiotami a biometrią, przedsiębiorca powinien zadać sobie pytania:

- Jakie będą straty czasu pracy spowodowane korzystaniem z danego narzędzia uwierzytelnienia (przekłada się to na straty finansowe)?
- Jeśli rozwiązanie będzie zastosowane do kontrolowania dostępu fizycznego lub/i rejestrowania czasu pracy, jaka jest wymagana szybkość działania (przepustowość)?
- Co jest bardziej korzystne przy danej wielkości zatrudnienia: jednorazowy zakup drogich urządzeń biometrycznych (oraz zakup i utrzymanie urządzeń pomocniczych, przetwarzających dane), czy wyposażenie pracowników w indywidualne urządzenia, które muszą być wymieniane co kilka – kilkadziesiąt miesięcy (oraz zakup i instalacja ew. urządzeń pomocniczych)?
- Czy obecna infrastruktura przedsiębiorstwa może zostać użyta jako element systemu uwierzytelnienia np. zamontowane kamery mogą być wykorzystane do uwierzytelnienia z użyciem geometrii twarzy?
- Na ile można zintegrować nowe rozwiązanie z obecną infrastrukturą? Czy zastosowane rozwiązania mogą zapewniać także dodatkowe funkcjonalności, czy jest to korzystne?

- Jak będzie wyglądała administracja systemu, czyli ile czasu zajmie i w jaki sposób będzie rozwiązywana kwestia przypadków fałszywego odmówienia dostępu osobie uprawnionej (FRR) lub obsługa przedmiotów (przygotowanie pod indywidualnego użytkownika, dystrybucja, obsługa zgłoszeń utraty/uszkodzenia przedmiotu, wydanie nowego w jak najkrótszym czasie)? Jakie dodatkowe systemy można wdrożyć i czy jest to opłacalne?

3. Akceptacja wśród użytkowników

Akceptacja planowanego rozwiązania jest czynnikiem bardzo istotnym, gdyż jej brak może skutkować protestami, niewłaściwym użytkowaniem przedmiotów (próby obejścia i lekceważenie zasad) aż po nieudane wdrożenie. Stąd powinno się uwzględnić następujące elementy:

- Komfort pracownika przy korzystaniu z danego rozwiązania (szybkość działania) i jego nieuciążliwość (niskie FRR).
- Średnią i maksymalną liczbę dziennych uwierzytelnień i jej wpływ na efektywność pracy.
- Postrzeganie rozwiązania jako bezpiecznego dla zdrowia (nieinwazyjnej, higienicznej) oraz nieingerującego w życie osobiste pracownika (obawa przed niewłaściwym użyciem wzorca referencyjnego).
- Dostosowanie rozwiązania do warunków pracy i wymagań metody (np. konieczność posiadania czystych rąk, braku okularów ochronnych itp. podczas uwierzytelnienia).

4. Dłuższa perspektywa

Inwestycja w zabezpieczenie zasobów z użyciem przedmiotów lub systemów opartych o biometrię może być i zwykle jest inwestycją na lata. Wiązać się może z ponoszeniem konkretnych kosztów eksploatacji oraz współpracą z dostawcą urządzeń. Stąd przed wyborem warto uwzględnić takie czynniki jak:

- Wiarygodność, dojrzałość technologii (FAR, FRR, EER) oraz dokładność i cena urządzeń.
- Wiarygodność dostawcy i możliwość wsparcia.

- Standardy i normalizacje.
- Koszty eksploatacji.
- Trendy i udane wdrożenia.
- Możliwość zintegrowania z innymi, planowanymi w przyszłości systemami.

6.7. PODSUMOWANIE

Wraz ze zwiększeniem się mocy obliczeniowej komputerów oraz przesunięciem zainteresowania przestępców internetowych także na małe i średnie przedsiębiorstwa, zabezpieczenie zasobów oparte o same hasła, staje się niewystarczające.

Wybór innej, bezpieczniejszej metody powinien być poprzedzony gruntowną analizą potrzeb i specyfiki samego przedsiębiorstwa oraz analizą rozwiązań i dostawców obecnych na rynku. Warto zaplanować kompleksowy system uwierzytelniania tak, by był on jak najmniej kosztochłonny, uciążliwy i jak najmniej wpływał na efektywność pracy.

7

Programowe rozwiązania informatyczne zapewniające bezpieczeństwo tożsamości cyfrowej

Jednym z najistotniejszych problemów wpływających na bezpieczeństwo tożsamości cyfrowej jest problem skutecznego zabezpieczenia dostępu do loginów i haseł wykorzystywanych przez użytkownika do identyfikowania się w przestrzeni internetu.

W obecnych realiach dostęp do internetu jest często uzyskiwany za pomocą osobistych urządzeń mobilnych takich jak notebooki, tablety lub smartfony, a instalowane na tych urządzeniach systemy operacyjne dają możliwość zapamiętywania parametrów logowania. W sytuacji gdy użytkownik wykorzystuje liczne usługi lub systemy dla których konieczne jest podawanie unikalnych danych identyfikacyjnych, dla swojej wygody często ulega pokusie „zapamiętania" tych danych w pamięci podręcznej przeglądarki internetowej lub innego narzędzia wykorzystywanego w procesie logowania. Powstaje wówczas ryzyko związane z możliwością utraty urządzenia mobilnego (w wyniku zagubienia lub kradzieży) a wraz z nim zapisanych danych identyfikacyjnych, do których wraz z urządzeniem mogą uzyskać dostęp osoby niepowołane. Dlatego ważne jest, aby dostęp do tych danych zabezpieczać na poziomie dostępu do samego urządzenia mobilnego. Przydatne mogą być również funkcje lub usługi umożliwiające zdalną lokalizację utraconego urządzenia (co może ułatwić jego odzyskanie) oraz blokadę dostępu lub kasację zawartości (wraz z danymi

wrażliwymi) w przypadku braku możliwości odzyskania urządzenia. Dostępne do zastosowania rozwiązania są ściśle związane z rodzajem systemu operacyjnego zainstalowanego na urządzeniu.

SYSTEMEM ANDROID

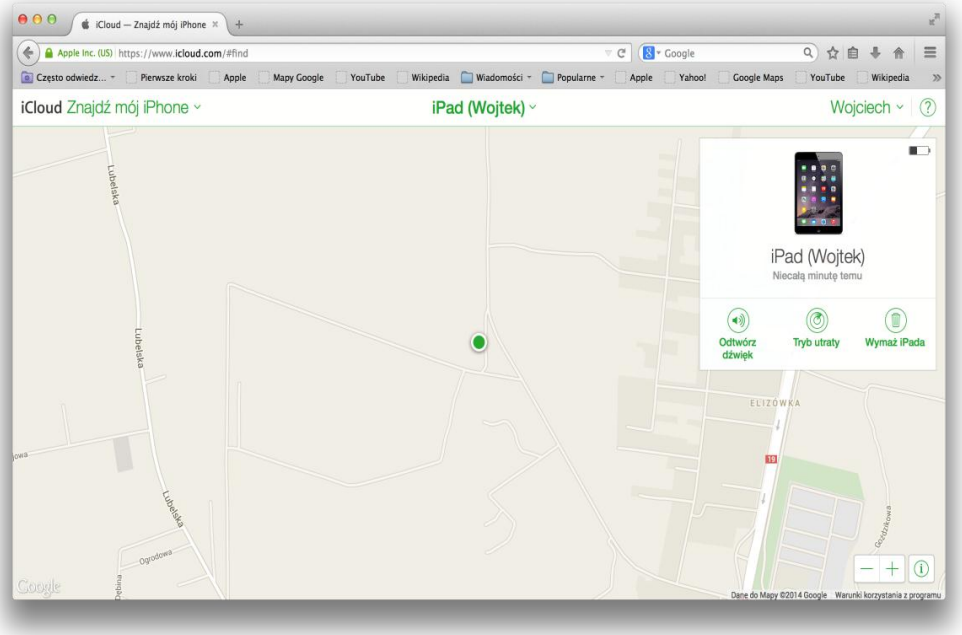
W przypadku urządzeń mobilnych z zainstalowanym systemem Android (tablety i smartfony), system umożliwia uzyskanie następujących funkcjonalności:

- użytkownik ma możliwość zabezpieczenia dostępu do pulpitu wykorzystując PIN-kod lub symbol logowania,
- użytkownik ma możliwość zaszyfrowania zawartości urządzenia,
- użytkownik ma możliwość wykorzystania dostępnej na witrynie Google usługi „menadżer urządzeń z Androidem" do lokalizacji urządzenia, jego zdalnej blokady lub zdalnej kasacji przechowywanych na nim danych.

SYSTEMEM IOS

W przypadku urządzeń mobilnych z zainstalowanym systemem iOS (tablety i smartfony), system umożliwia następujące funkcjonalności:

- użytkownik ma możliwość zabezpieczenia dostępu do pulpitu wykorzystując PIN-kod lub skaner linii papilarnych Touch ID,
- użytkownik ma możliwość zaszyfrowania zawartości urządzenia,
- użytkownik ma możliwość wykorzystania dostępnej na witrynie Apple iCloud usługi „znajdź mój iPhone" do lokalizacji urządzenia, jego zdalnej blokady lub zdalnej kasacji przechowywanych na nim danych,
- po włączeniu funkcji „znajdź mój iPhone" na poziomie urządzenia, blokowana jest możliwość reaktywacji urządzenia przez osobę niepowołaną, nie znającą danych identyfikacyjnych uprawnionego użytkownika.



Rys. 1. Wygląd interfejsu usługi „Znajdź mój iPhone" umożliwiającej lokalizację urządzenia i zdalne nim zarządzanie

SYSTEM MAC OS X

W przypadku urządzeń mobilnych z zainstalowanym systemem Mac OS X (notebooki Apple MacBook), system umożliwia następujące funkcjonalności:

- użytkownik ma możliwość zabezpieczenia dostępu do pulpitu wykorzystując hasło sprzętowe oraz hasło systemowe,
- użytkownik ma możliwość wykorzystania dostępnej na witrynie Apple iCloud usługi „znajdź mój iPhone" do lokalizacji urządzenia, jego zdalnej blokady lub zdalnej kasacji przechowywanych na nim danych,
- użytkownik ma możliwość zaszyfrowania pamięci masowych.

Szyfrowanie danych w systemie Mac OS X (mechanizm określany przez producenta systemu operacyjnego jako FileVault 2) wykorzystuje algorytm XTS-AES 10 z 128 bitowym kluczem. Zakodowany dysk jest zablokowany przed odczytem. W razie potrzeby odblokowania dysku do odczytu konieczne jest podanie klucza

odzyskiwania który jest generowany w momencie włączenia funkcji szyfrowania. Użytkownik ma możliwość zabezpieczenia (zapisania) klucza we własnym zakresie lub może zlecić przechowywania klucza przez serwery Apple. W przypadku zlecenia przechowywania klucza na serwerach zewnętrznych jest on dodatkowo zabezpieczony serią pytań kontrolnych, (do których unikalne odpowiedzi powinny być znane wyłącznie uprawnionemu użytkownikowi). Według zapewnień firmy Apple, nie ma możliwości pozyskania klucza z ich serwerów bez znajomości prawidłowych odpowiedzi na pytania kontrolne (klucz jest odtwarzany na bazie udzielonych odpowiedzi, w przypadku gdy są błędne również odtworzony klucz nie będzie prawidłowy).

Rys. 2. Definiowanie pytań kontrolnych powiązanych z kluczem odzyskiwania składowanym na serwerach Apple

SYSTEM MICROSOFT WINDOWS 8.X

W przypadku urządzeń mobilnych z zainstalowanym systemem Microsoft Windows 8.x (tablety, smartfony, notebooki), system umożliwia następujące funkcjonalności:

- użytkownik ma możliwość zabezpieczenia dostępu do pulpitu wykorzystując hasło systemowe. W przypadku części urządzeń (dla których producent zaimplementował odpowiednią funkcjonalność) użytkownik ma również możliwość zabezpieczenia dostępu do pulpitu z wykorzystaniem hasła sprzętowego.
- w przypadku niektórych urządzeń (dla których producent zaimplementował odpowiednią funkcjonalność w formie sprzętowej i programowej) użytkownik ma możliwość dodatkowego zabezpieczenia urządzenia (blokada startu lub dostępu do pulpitu) wykorzystując czytnik kart procesorowych oraz skaner linii papilarnych.
- użytkownik ma możliwość zaszyfrowania pamięci masowych.

Szyfrowanie danych w systemie Microsoft Windows 8.x (mechanizm określany przez producenta systemu operacyjnego jako BitLocker) wykorzystuje algorytm AES 10 lub 14 (ze 128 lub 256 bitowym kluczem). Elementem koniecznym do uruchomienia szyfrowania jest moduł TPM który musi być zintegrowany z płytą główną urządzenia. Szyfrowanie dostępne jest tylko w wybranych wersjach systemu operacyjnego Windows (Professional, Ultimate oraz Enterpise). Do odszyfrowania danych konieczne jest podanie klucza odzyskiwania. Klucz generowany jest w momencie włączenia funkcji szyfrowania. Użytkownik ma możliwość zabezpieczenia (zapisania) klucza w formie notatki, pliku składowanego na nośniku wymiennym (np. pendrive) lub może powiązać klucz odzyskiwania za swoim kontem Microsoft (wskazanym przez indywidualny Microsoft ID).

SYSTEM LINUX

W przypadku urządzeń mobilnych z zainstalowanym systemem Linux (notebooki), system umożliwia następujące funkcjonalności:

- użytkownik ma możliwość zabezpieczenia dostępu do pulpitu wykorzystując hasło systemowe. W przypadku części urządzeń (dla których producent zaimplementował odpowiednią funkcjonalność) użytkownik ma również możliwość zabezpieczenia dostępu do pulpitu z wykorzystaniem hasła sprzętowego.
- w przypadku niektórych urządzeń (dla których producent zaimplementował odpowiednią funkcjonalność w formie sprzętowej i programowej) użytkownik ma możliwość dodatkowego zabezpieczenia urządzenia (blokada startu lub dostępu do pulpitu) wykorzystując czytnik kart procesorowych oraz skaner linii papilarnych.
- użytkownik ma możliwość zaszyfrowania pamięci masowych.

Szyfrowanie danych w systemach typu Linux zazwyczaj nie wymaga aby urządzenie było wyposażone w dodatkowe moduły sprzętowe. Szyfrowanie realizowane jest programowo z wykorzystaniem wbudowanych funkcji systemu lub za pomocą oprogramowania firm trzecich. Nie ma jednolitego i ogólnie przyjętego standardu, użytkownik decydując się na włączenie szyfrowania wybiera rozwiązanie odpowiadające jego osobistym preferencjom.

SYSTEM CHROME OS

W przypadku urządzeń mobilnych z zainstalowanym systemem Chrome OS (chromebooki) brak jest jakichkolwiek zabezpieczeń lokalnych. Ponieważ weryfikacja danych logowania i identyfikacja użytkownika odbywa się na zdalnym serwerze Google (z którym system Chrome OS łączy się po uruchomieniu) w lokalnych zasobach urządzenia nie są przechowywane loginy i hasła które wymagałyby ochrony. Urządzenia nie mają również lokalnej pamięci masowej, dane użytkownika przechowywane są na dyskach wirtualnych funkcjonujących w przestrzeni chmury obliczeniowej.

OCHRONA DANYCH NA DYSKACH WIRTUALNYCH

Zagadnienie ochrony danych użytkownika, przechowywanych na dyskach wirtualnych jest kolejnym z poważnych problemów wiążących się nierozerwalnie z bezpieczeństwem tożsamości cyfrowej. Dyski wirtualne są dostępne i wykorzystywane nie tylko w urządzeniach z zainstalowanym systemem Chrome OS, ale również w innych konfiguracjach sprzętowo-systemowych. Dysk wirtualny, staje się obecnie standardowym mechanizmem dostępnym we współczesnym systemie operacyjnym. Jako technologia zapewniająca wyjątkowo skuteczną oraz łatwą w obsłudze synchronizację danych pomiędzy licznymi, powiązanymi urządzeniami, jest idealnym rozwiązaniem dla użytkowników mobilnych, często zmieniających miejsce pracy i wykorzystywane urządzenie. Dlatego wszyscy wiodący producenci systemów operacyjnych oferują bezpłatne dyski wirtualne, jako uzupełnienie dla systemów operacyjnych. Firma Microsoft, producent systemów z grupy Windows oferuje usługę OneDrive (dawniej SkyDrive) udostępniającą przestrzeń dyskową użytkownikom systemów Windows, iOS oraz Android. Firma Apple, producent systemów Mac OS X oraz iOS, oferuje usługę iCloud udostępniającą przestrzeń dyskową użytkownikom tych systemów, ale integrującą się również z systemem Windows. Firma Google oferuje usługę Dysk (Google Drive) dostępną dla użytkowników systemów: Android, Windows, Mac OS X, iOS.

Na rynku istnieją również niezależni dostawcy usługi dysków wirtalnych (np. DropBox, BOX itp.) zapewniający obsługę dowolnego rodzaju urządzenia i systemu operacyjnego (Windows, Mac OS X, Linux, Android, iOS, BlackBerry, Kindle itp.).

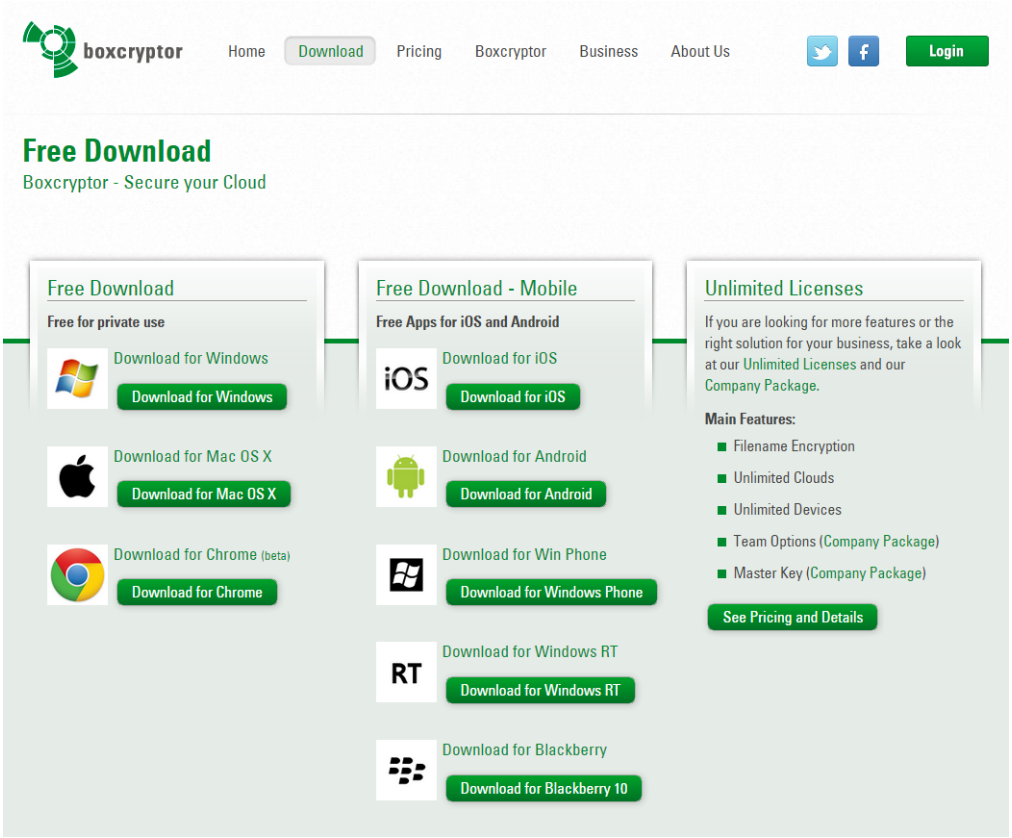
Mnogość usług i wspomniana wcześniej łatwość obsługi powoduje że dyski wirtualne są powszechnie wykorzystywane. Do podłączenia istniejącego dysku wirtualnego (założonego wcześniej i skonfigurowanego do pracy) do nowego urządzenia najczęściej wystarcza znajomość identyfikatora użytkownika (zazwyczaj jest to adres e-mail) oraz hasła. Po podłączeniu dysku, nowe urządzenie uzyskuje dostęp do zgromadzonych tam danych. W tym momencie można zadać sobie pytanie, czy aby na pewno rozwiązanie takie jest bezpieczne. Znane z historii przypadki wycieku danych z dysków wirtualnych, niezależnie od tego czy nastąpiły w wyniku problemów technicznych (awaria usługi DropBox) czy ataku hackerskiego (wyciek

danych z prywatnych kont iCloud), przekonują, że korzystanie z dysku wirtualnego wiąże się jednak z pewnym ryzykiem. Dla zwiększenia poziomu bezpieczeństwa i ochrony danych (zwłaszcza danych wrażliwych) konieczne jest wprowadzenie dodatkowego mechanizmu ochronnego w postaci szyfrowania. Do skutecznej ochrony optymalne jest zastosowanie narzędzia szyfrującego niezależnego od dostawcy usługi dysku wirtualnego. W takim przypadku, dane pozyskane z dysku wirtualnego przez osobę nieuprawnioną (zaszyfrowane za pomocą nieznanego jej narzędzia) będą dla intruza całkowicie bezużyteczne.

Na rynku dostępne są liczne narzędzia (CloudFogger, DiskCryptor, TrueCrypt, SecretFolder, BoxCryptor, itp.), zarówno bezpłatne jak i komercyjne, umożliwiające szyfrowanie zawartości dysków, w tym również dysków wirtualnych. Możliwości ich wykorzystania w ochronie danych przedstawię na przykładzie aplikacji BoxCryptor oraz CloudFogger.

APLIKACJA BOXCRYPTOR

BoxCryptor jest aplikacją bezpłatną w przypadku zastosowań niekomercyjnych z ograniczeniem do maksymalnie dwóch urządzeń, które mogą być zarejestrowane i powiązane z kontem użytkownika na portalu *boxcryptor.com*. Użytkownik komercyjny lub mający potrzebę powiązania ze swoim kontem większej liczby urządzeń powinien wykupić roczny abonament na usługę. Klienta usługi BoxCryptor można pobrać i zainstalować na urządzeniach pracujących pod kontrolą systemów operacyjnych: Windows, Mac OS X, Chrome, iOS, Android, Windows Phone, Windows RT oraz Blackberry.

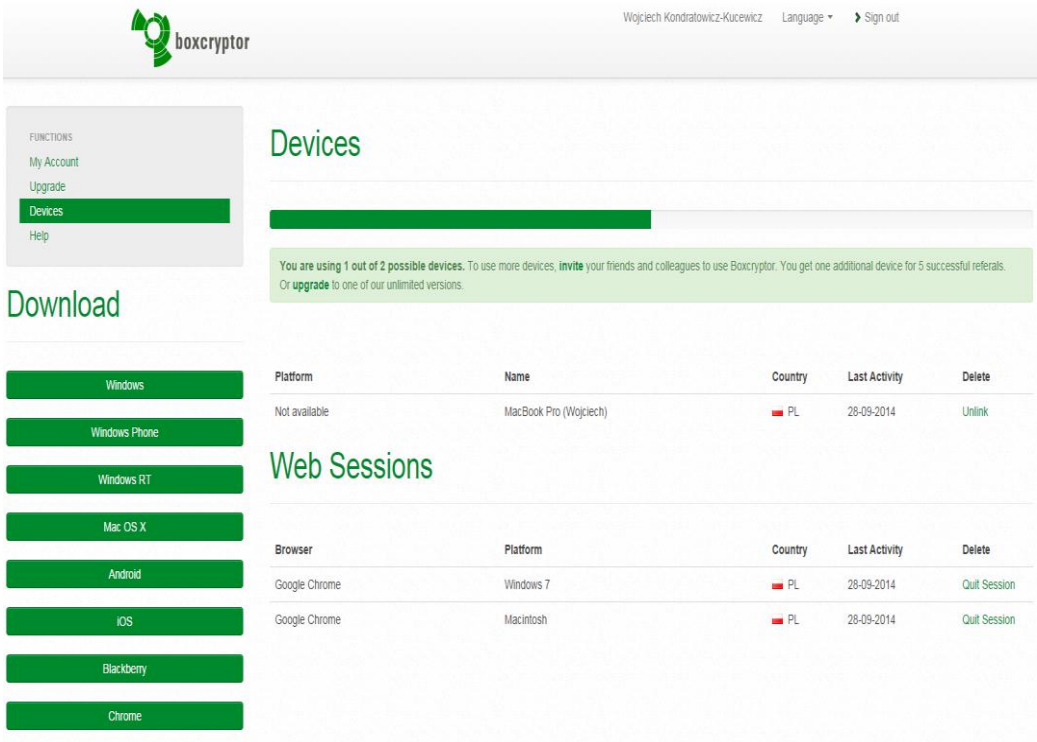


Rys.3. Widok strony producenta, z której można pobrać oprogramowanie klienta dla posiadanego urządzenia

Po zainstalowaniu klienta użytkownik może zdecydować czy będzie korzystał z konta lokalnego, czy globalnego (kontrolowanego przez serwer BoxCryptor). W przypadku wybrania konta lokalnego i pierwszej instalacji usługi BoxCryptor zostanie wygenerowany klucz szyfrowania dla urządzenia, na którym została wykonana instalacja i dostęp do tego klucza będzie miał wyłącznie użytkownik. W przypadku utraty klucza, odszyfrowanie danych nie będzie możliwe (BoxCryptor nie będzie dysponował kopią klucza). Aby umożliwić odszyfrowywanie danych na innym urządzeniu wykorzystywanym przez użytkownika, konieczne jest utworzenie kolejnego konta lokalnego i ręczne zaimportowanie posiadanego już klucza. Ten model pracy umożliwia bezpłatne skorzystanie z usługi na większej liczbie urządzeń (konta lokalne

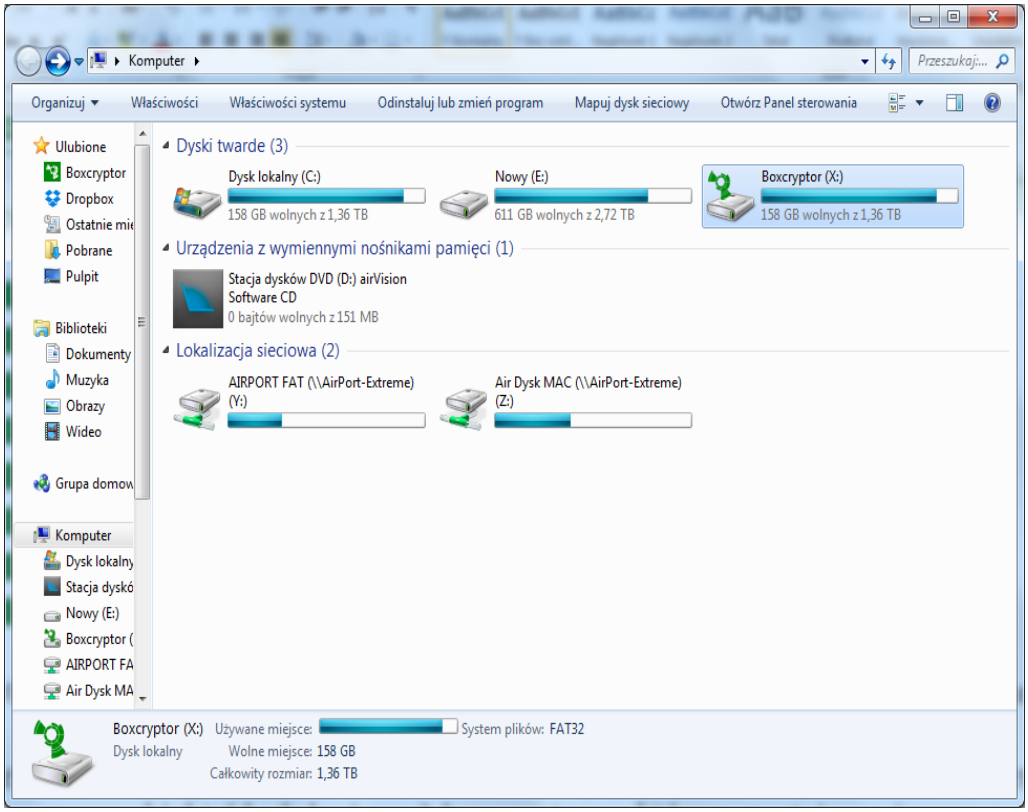
nie są zliczane przez serwer BoxCryptor) ale osiągany poziom bezpieczeństwa jest niższy, gdyż klucz szyfrowania jest przechowywany na urządzeniu i wraz z jego utratą może zostać wykorzystany przez osobę niepowołaną. Uzyskujemy jednak zabezpieczenie przed atakiem na dane dokonywanym z poziomu internetu.

Wyższy poziom bezpieczeństwa zapewnia model pracy oparty o konto globalne, w którym klucz szyfrowania przypisany do użytkownika przechowywany jest na serwerze BoxCryptor. Do odszyfrowania danych, urządzenie musi zostać zalogowane na serwerze (w granicach przysługującego limitu). Jeżeli login i hasło dostępowe do serwera BoxCryptor nie zostaną „zapamiętane" na urządzeniu mobilnym, to jego utrata nie zagraża bezpieczeństwu zaszyfrowanych danych.

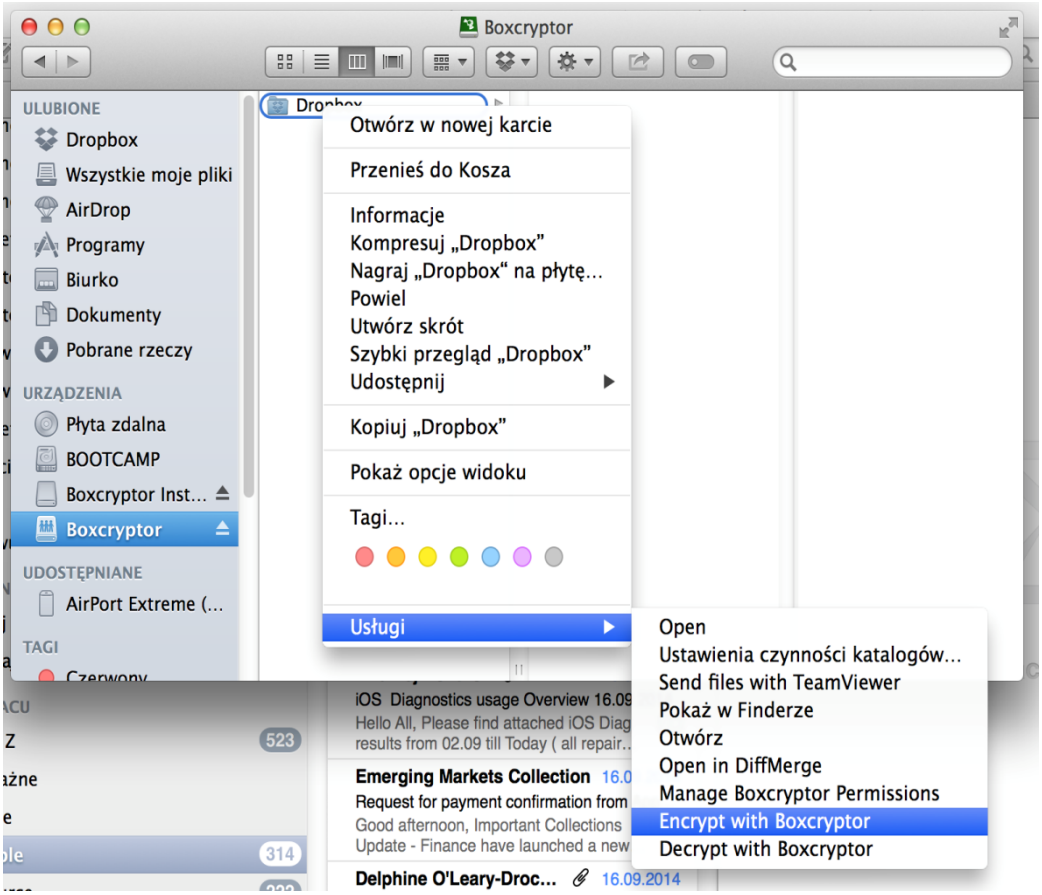


Rys.4. Widok witryny na której zliczane są urządzenia zarejestrowane do korzystania z usługi w ramach konta globalnego

Niezależnie od sposobu instalacji (lokalnie czy globalnie) w systemie urządzenia zostaje utworzony obiekt (dysk logiczny) boxcryptor w którym zostają umieszczone wcześniej podłączone dyski wirtualne. Zawartość tych dysków nie jest domyślnie szyfrowana, decyzję o tym które z danych (foldery lub pojedyncze pliki) mają być zaszyfrowane podejmuje użytkownik wskazując wybrane zasoby. Uzyskanie dostępu do zaszyfrowanych danych w przypadku konta lokalnego nie wymaga dodatkowych działań, (jeżeli z kontem powiązany jest prawidłowy klucz szyfrujący) natomiast w przypadku konta globalnego konieczne jest podanie prawidłowego loginu i hasła.



Rys. 5. Widok obiektu BoxCryptor w systemie Windows

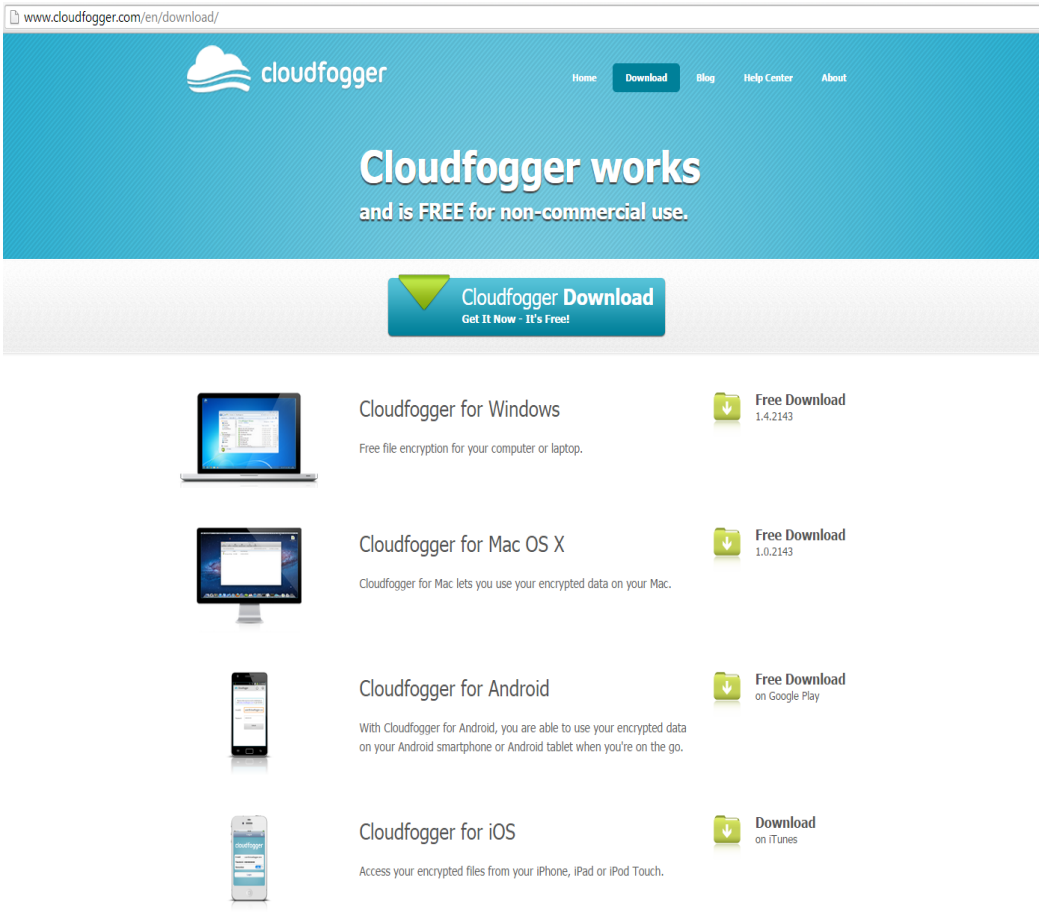


Rys. 6. Widok obiektu BoxCryptor w systemie Mac OS X

APLIKACJA CLOUDFOGGER

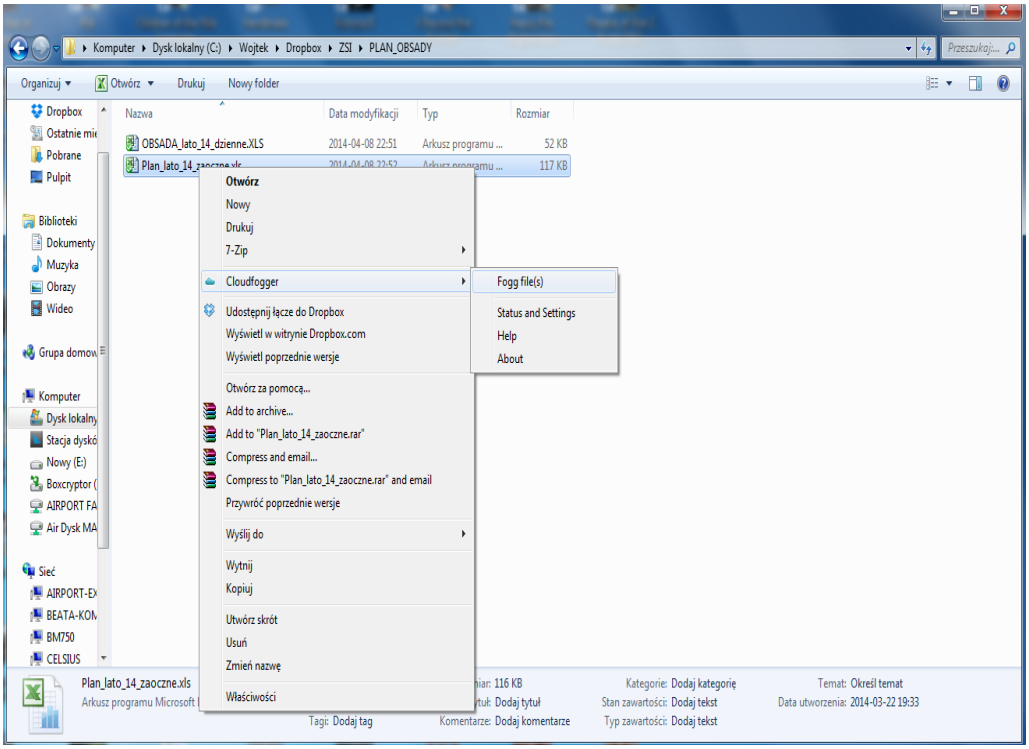
Podobny poziom zabezpieczenia możemy osiągnąć wykorzystując aplikację CloudFogger, również bezpłatną przy zastosowaniach niekomercyjnych (wersja płatna do zastosowań komercyjnych ma być udostępniona w przyszłości). Obecnie użytkownik wykorzystujący tą usługę podlega ograniczeniu do maksymalnie pięciu chronionych folderów sieciowych (niezależnych od siebie dysków chmurowych w rodzaju DropBox, OneDrive, Google Drive itp.) na jednym komputerze (przy czym podfoldery dysków chmurowych nie są zliczane do limitu). W usłudze CloudFogger

wykorzystywany jest wyłącznie profil globalny z kontem użytkownika zakładanym na serwerze producenta. Nie ma limitu na ilość urządzeń mobilnych na których użytkownik chciałby skorzystać z usługi. Klienta usługi CloudFogger można pobrać i zainstalować na urządzeniach pracujących pod kontrolą systemów operacyjnych: Windows, Mac OS X, iOS oraz Android.

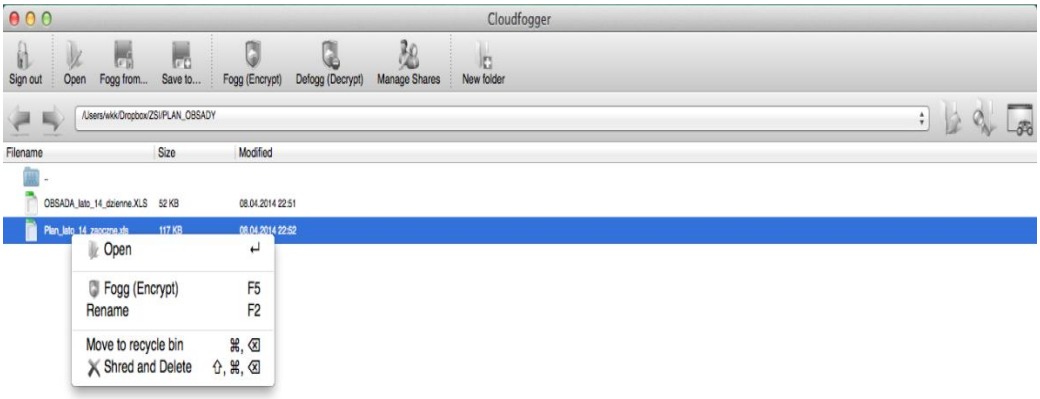


Rys. 7. Widok strony producenta, z której można pobrać oprogramowanie klienta dla posiadanego urządzenia

Po zainstalowaniu aplikacji konieczne jest utworzenie nowego konta użytkownika (przy pierwszej instalacji) lub podłączenie się do konta istniejącego poprzez podanie loginu i hasła. Standardowo loginem jest adres e-mail użytkownika. Po zalogowaniu klienta i uruchomieniu usługi można przystąpić do szyfrowania i deszyfrowania zasobów.



Rys.8. Dostęp do funkcji szyfrowania w systemie Windows

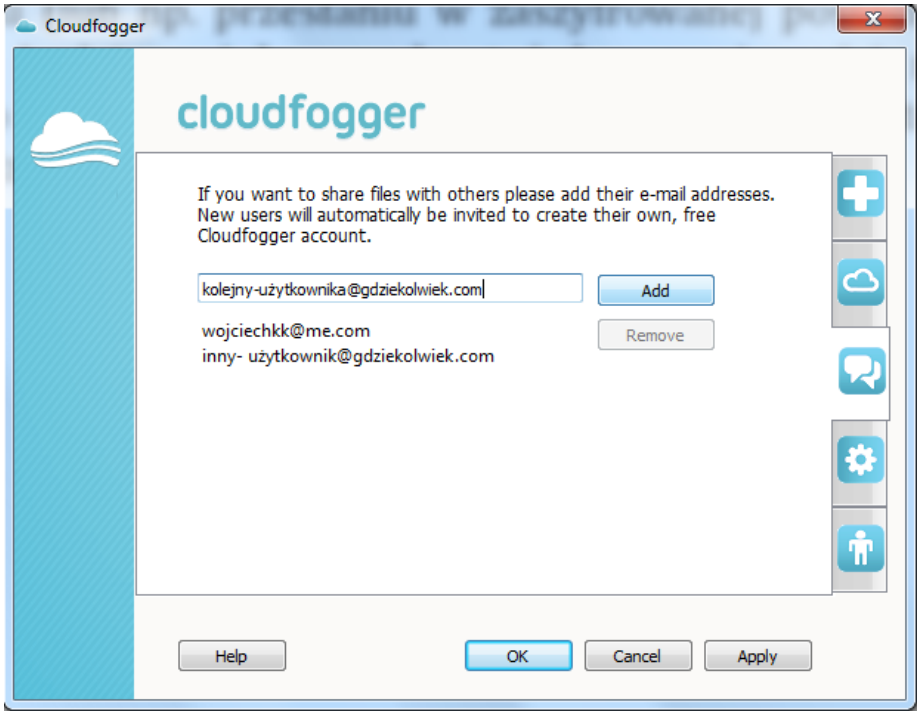


Rys. 9. Dostęp do funkcji szyfrowania w systemie Mac OS X

Ciekawą funkcjonalnością jest możliwość współdzielenia zaszyfrowanych plików z innym użytkownikiem. Aby skorzystać z tej funkcjonalności, w oknie interfejsu usługi CloudFogger należy dodać adres e-mail (indentyfikator CloudFogger) użytkownika, z którym chcemy dany plik współdzielić. Oczywiście dodany użytkownik powinien być zarejestrowanym użytkownikiem usługi CloudFogger. Po udostępnieniu mu zaszyfrowanego pliku (lub np. przesłaniu w zaszyfrowanej postaci, jako załącznik do wiadomości e-mail) będzie mógł go odczytać bez znajomości naszego hasła, po zalogowaniu się do serwera CloudFogger na swój identyfikator. Pliki możemy udostępniać i współdzielić z wieloma osobami.

Jedynym istotnym ograniczeniem przy korzystaniu z usługi CloudFogger jest brak możliwości pracy off-line z zaszyfrowanymi zasobami. Ponieważ klucze szyfrujące wykorzystywane podczas kodowania zasobów są przechowywane i udostępniane przez serwer CloudFogger, klient aplikacji musi mieć dostęp do serwera (znajdującego się w przestrzeni chmurowej) w trakcie swojego działania (kodowanie i dekodowanie plików). Wobec czego konieczne jest działające połączenie

z Internetem. Ale ponieważ podstawowym zastosowaniem dla tego typu usług jest ochrona zasobów, które w tymże Internecie są przechowywane, nie wydaje się to być poważnym ograniczeniem.



Rys.10 Okno interfejsu CloudFogger umożliwiające współdzielenie plików

Bibliografia

[AND14] Anderson J., Rainie L., *The Internet of Things will thrive by 2025*, May 2014, (http://www.pewinternet.org/files/2014/05/PIP_Internet-of-things_0514142.pdf, dostęp: 1.09.2014).

[BAC06] Bączek P.*, Zagrożenia informacyjne a bezpieczeństwo państwa polskiego,* Wydawnictwo Adam Marszałek, Toruń 2006.

[BAN13] Bankowość biometryczna, Raport Biometryczny 2.0, red: Woszczyński T., Grupa FTB ds. Biometrii, Warszawa 2013, [dostęp: 21.10.2014], online: http://zbp.pl/public/repozytorium/dla_bankow/rady_i_komitety/technologie_bankowe/publikacje/Raport_Biometryczny_2.0_strona_FTB.pdf.

[BAT13] Batorski D., (2013). Polacy wobec technologii cyfrowych – uwarunkowania dostępności i sposobów korzystania. Diagnoza Społeczna 2013 Warunki i Jakość Życia Polaków – Raport. [Special issue]. Contemporary Economics, 7, 317–341 DOI: 10.5709/ce.1897-9254.114.

[BBN] www.bbn.gov.pl/download/1/1002/bezpieczenstwoinformacji. [05.10.2014].

[BIZ] www.biznes.newseria.pl/komunikaty/firma/intel_polacy_najwiecej,b1390747873.

[CAM11] Campolargo M., *The Bright Future of the Internet of Things*, [w:] Internet of Things – Converging Technologies for Smart Environments and Integrated Ecosystems, [red.] Vermesan O., Friess P., River Publishers, Aalborg, Denmark 2011, (http://www.internet-of-things-research.eu/pdf/Converging_Technologies_for_Smart_Environments_and_Integrated_Ecosystems_IERC_Book_Open_Access_2013.pdf, dostęp: 10.10.2014).

[CAS11] CASAGRAS, *RFID and the inclusive model for the Internet of Things report*, EU Project Number 216803, pp 16–23, 2011, (http://grifs-project.uniweb.be/data/File/CASAGRAS FinalReport (2).pdf, dostęp: 14.10.2014).

[CEL] www.callcenternews.pl/2014/09/26/co-trzecia-firma-zwiekszy-budzet-na-ochrone-informacji.

[CHI12] Chia T., Confidentiality, Integrity, Availability: The three components of the CIA Triad, 20.08.2012, online: http://security.blogoverflow.com/2012/08/confidentiality-integrity-availability-the-three-components-of-the-cia-triad/.

[CHŁ04] Chłodnicki M., *Usług*i *profesjonalne. Od jakości do lojalności klientów,* WAE Poznań 2004.

[CIE12] Cieciura M., *Wybrane problemy społeczne i zawodowe informatyki*, WSFiZ, W-wa 2012.

[CIE12] Cieciura Marek, *Wybrane problemy społeczne i zawodowe informatyki*, Warszawa 2012.

[COE11] Coetzee L., Eksteen J., *The Internet of Things – Promise for the Future? An Introduction*, IST-Africa, Gaborne, Botswana 2011.

[COM] BYOD w polskich i zagranicznych firmach http://www.computerworld.pl/news/393282/BYOD.w.polskich.i.zagranicznych.firmach.html.

[DAG14] Dagessa. Biometria. [dostęp: 21.10.2014], online: http://dagessa.pl/index.php?option=com_content&task=view&id=44&Itemid=72.

[DIN] www.din66399.pl.

[DYR] www.dyrektorzy-handlowi.menedzersprzedazy.pl/a/charakterystyka-profesjonalisty.

[EMC14] EMC, RSA SecuredID Software Authenticators, [dostęp: 12.10.2014], online: http://www.emc.com/security/rsa-securid/rsa-securid-software-authenticators/toolbar.htm.

[EST14] Estimote, (estimote.com, dostęp: 1.10.2014).

[EVA11] Evans D., *The Internet of Things. How the Next Evolution of the Internet Is Changing Everything*, Cisco IBSG, April 2011, (http://www.cisco.com/web/about/ac79/docs/innov/IoT_IBSG_0411FINAL.pdf, dostęp: 1.09.2014).

[FAB14] Fabiszewski D., *INTERNET (WSZECH)RZECZY motorem rozwoju gospodarczego*, Cisco, (www.ican.pl/files/137-138 SS_Cisco.pdf, dostęp: 10.10.2014).

[GAR13] Gartner Inc., *Gartner's 2013 Hype Cycle for Emerging Technologies Maps Out Evolving Relationship Between Humans and Machines*, [w:] Press Release, August 2013, (http://www.gartner.com/newsroom/id/2575515, dostęp: 01.10.2014).

[GAR14] Gartner Inc., *Top 10 Strategic Technology Trends for 2014*, (http://www.gartner.com/technology/research/top-10-technology-trends/, dostęp: 1.09.2014).

[GER12] Geron G., *Business Aspects of the Internet of Things: Mobile Marketing*, [w:] Business Aspects of the Internet of Things, [red.] Florian Michahelles, ETH Zurich 2012, (http://www.im.ethz.ch/education/FS12/iot_lec, dostęp: 10.10.2014).

[GIO07] GIODO, ABC bezpieczeństwa danych osobowych przetwarzanych przy użyciu systemów informatycznych, Wyd. Sejmowe, 2005.

[GOL] www.goldenline.pl/grupy/Pozostałe/profesjonalisci//na-czym-wlasciwie-polega-ten-nasz-prtofesjonalizm,941200.

[GOO14] Google Trends, (https://www.google.pl/trends, dostęp: 01.10.2014).

[GUS13] Społeczeństwo informacyjne w Polsce w 2013 r. Główny Urząd Statystyczny, Warszawa, 2013, [http://stat.gov.pl/download/cps/rde/xbcr/gus/nts_spolecz_inform_w_polsce-2013.pdf].

[HID14] Hidglobal, ActivID(R) One-Time Password (OTP) tokens, [dostęp: 11.10.2014], online: http://www.hidglobal.com/products/cards-and-credentials/activid/one-time-password-tokens.

[IER] http://www.ie-ries.com.pl/archiwum/artykuly/RIES_201110241034_Etyka.pdf.

[IER12] IERC – Internet of Things European Research Cluster, *The Internet of Things 2012 New Horizons*, Halifax 2012, (http://www.internet-of-things-research.eu/pdf/IERC_Cluster_Book_2012_WEB.pdf, dostęp: 10.10.2014).

[ISO] www.iso.org.pl/iso-27001.

[ITP] http://itpedia.pl/index.php/Ochrona_informacji_w_sieci_przedsi%C4%99biorstwa.

[JAB09] Jabłoński M., Mielus M., Zagrożenia bezpieczeństwa informacji w przedsiębiorstwie. Część 1, Zabezpieczenia 1/2009. http://www.zabezpieczenia.com.pl/ochrona-informacji/zagrozenia-bezpieczenstwa-informacji-w-przedsiebiorstwie-czesc-1.

[KAF12] Kafel T., *Cechy profesjonalizmu-analiza pojęciowa oraz oczekiwania stawiane zarządzającym podmiotami ekonomii społecznej* http://fundacja.e-gap.pl/mowes/wp-content/uploads/2012/11/BES-nr-1-Artyku%C5%82-3.pdf.

[KOS08] Kosewski M., *Wartości-Godność, Władza. Dlaczego porządni ludzie czasem kradną, a złodzieje ujmują się honorem*, VIZJA PRESS & IT, W-wa 2008.

[KRO08] Królikowski P., Silne uwierzytelnianie z użyciem tokenów, 11.09.2008, online: http://www.computerworld.pl/artykuly/324895_2/Silne.uwierzytelnianie.zuzyciem.tokenow.kryptograficznych.html.

[KRY14] Kryptoteka, sklep internetowy, [dostęp: 11.10.2014], online: http://www.kryptoteka.pl/index.php?k10,tokeny-usb.

[KSO] www.ksoin.pl/bezpieczenstwo_informacji_w_firmie-strony,11,381.html#.VEoNRxb3WM8.

[KSO14] www.ksoin.pl/bezpieczenstwo_informacji_jako_wazny_element_bezpieczenstwa_calej_organizacji-strony,11,278.html#.VDIn4jh03WG, [05.10.2014].

[KUT03] Kuta M., Polityka bezpieczeństwa informacji w przedsiębiorstwie – aspekty praktyczne, [w:] Borowiecki R., Kwieciński M., Monitorowanie otoczenia, przepływ i bezpieczeństwo informacji. W stronę integralności przedsiębiorstwa, Zakamycze 2003.

[LIS02] Lissowski G., hasło *Informacja*, [w:] *Wielka Encyklopedia Powszechna*, 2002.

[ŁUC04] Łuczak J. (red.), Zarządzanie bezpieczeństwem informacji, Oficyna Współczesna, Poznań 2004.

[MAN] http://manager.nf.pl/czyli-bezpieczenstwo-informacji-w-firmie-iso-iec-27001,3,43303,55.

[MCA12] McAulay A., *As cheap as chips: turning the 'internet of things' into business benefits*, [w:] Computer Weekly, 5 July 2012, (http://www.computerweekly.com/opinion/As-cheap-as-chips-turning-the-internet-of-things-into-business-benefits, dostęp: 10.10.2014).

[MCK13] McKinsey Global Institute, *Disruptive technologies: Advances that will transform life, business, and the global economy*, May 2013, (http://www.mckinsey.com, dostęp: 1.09.2014).

[MIC] Dokumentacja producenta systemu Microsoft Windows 8.x.

[MOR14] http://www.morele.net/microsoft-czytnik-linii-papilarnych-usb-65379/ [dostęp: 21.10.2014].

[MRA] http://www.mragowo.pti.org.pl.

[NOW] Nowak J., Społeczeństwo informacyjne – geneza i definicje, [http://www.silesia.org.pl/upload/Nowak_Jerzy_Spoleczenstwo_informacyjne-geneza_i_definicje.pdf].

[PAL14] Palo Alto Networks, [dostęp: 12.10.2014], online: http://www.hidglobal.com/partners/palo-alto-networks.

[PAN13] Panek, T., Czapiński, J. (2013). Wykluczenie społeczne. Diagnoza Społeczna 2013 Warunki i Jakość Życia Polaków – Raport. [Special issue]. Contemporary Economics, 7, 342–375 DOI: 10.5709/ce.1897-9254.115.

[PAS07] Paszkiel S., Zastosowanie autoryzacji i uwierzytelniania w systemach DSS oraz ich wpływ na efektywność zarządzania organizacją, Zeszyt Naukowy SCENO 5A, materiały II Konferencja SCENO – wrzesień 2007.

[PER] www.perspektywy.pl.

[PLU14] Plucińska M., Wójtowicz J., Analiza technik biometrycznych do uwierzytelniania osób, Elektronika 4/2014, s. 64–66.

[PTI] http://www.pti.org.pl.

[RAI] Bezpieczeństwo w Internecie Raport, [http://www.interaktywnie.com/biznes/raporty].

[RMP10] Rozporządzenie Min. Pracy i Pol. Społ. Z 27.04.2010 r Dz. U. 2010 nr.82 poz. 537.

[ROS13] Rosiński J., *Postawy zawodowe informatyków: jednostka, zespół, organizacja*, WUJ Kraków 2013.

[RSA14] RSA Authentication Manager 8. Przewodnik po metodach uwierzytelniania [dostęp: 23.10.2014], online: http://www.arrowecs.pl/WWW/News.nsf/Bitmaps/ulotki_rsa/$FILE/RSA_Authentication_Manager_8_metody_uwierzytelniania.pdf.

[SEC] www.securitum.pl/baza-wiedzy/publikacje/przykladowa-polityka-bezpieczenstwa.

[SIE13] Sienkiewicz P, Świeboda H., Kształtowanie kompetencji obywatelskich na potrzeby rozwoju społeczeństwa informacyjnego, W: Europejska przestrzeń komunikacji elektronicznej, Uniwersytet Szczeciński, Zeszyty Naukowe nr 763, Ekonomiczne problemy usług nr 105, Wydawnictwo Naukowe Uniwersytetu Szczecińskiego, Szczecin, 2013, [http://www.wzieu.pl/zn/763/ZN_763.pdf].

[SOF14a] http://www.softlock.net/ePass-OTP-Token [dostęp: 21.10.2014].

[SOF14b] http://www.softlock.net/eSign-Smart-Token [dostęp: 21.10.2014].

[SOL14] Solidpass, Windows Mobile Software Security Token, [dostęp: 12.10.2014], online: http://www.solidpass.com/platforms/windows-mobile-software-token.html.

[STR05] Strzelczyk P., Chochowki M., Pacut A., Czajka A., Biometryczna karta elektroniczna, prezentacja z Konferencji na temat bezpieczeństwa teleinformatycznego Secure 2005, Warszawa październik 2005.

[SZY03] Szymański M., Smart Cards (ICC), 2003, online: http://students.mimuw.edu.pl/SO/Projekt02-03/temat4-g2/miroslaw_szymanski/sc.htm.

[ŚWI13] Świeboda H., Problem prywatności w społeczeństwie informacyjnym, W: Europejska przestrzeń komunikacji elektronicznej, Uniwersytet Szczeciński, Zeszyty Naukowe nr 763, Ekonomiczne problemy usług nr 105, Wydawnictwo Naukowe Uniwersytetu Szczecińskiego, Szczecin, 2013, [http://www.wzieu.pl/zn/763/ZN_763.pdf].

[TAJ] http://tajemnica-przedsiebiorstwa.pl/category/nieuczciwa-konkurencja.

[UOD97] Ustawa o ochronie danych osobowych z 29.08.1997, Dz.U. 1997 nr 133.

[UST97] Ustawa z dnia 29 sierpnia 1997 r. o ochronie danych osobowych.

[VER11] Vermesan O., Friess P., Guillemin P., Sundmaeker H., Eisenhauer M., Moessner K., Le Gall F., Cousin P., *Internet of Things Strategic Research and Innovation Agenda*, [w:] Internet of Things – Converging Technologies for Smart Environments and Integrated Ecosystems, [red.] Vermesan O., Friess P., River Publishers, Aalborg, Denmark 2011, (http://www.internet-of-things-research.eu/pdf/Converging_Technologies_for_Smart_Environments_and_Integrated_Ecosystems_IERC_Book_Open_Access_2013.pdf, dostęp: 10.10.2014).

[VER14] Verax Systems, Tokeny software'owe, przegląd rozwiązań [dostęp: 22.10.2014], online: http://bs.net.pl/upload/File/pdf/tokeny.pdf.

[WAL] Walczak-Duraj Danuta., Art."*Kontekst etyczny zawodów informatycznych*".

[WAR11] Waraksa M., Żurek J., *Bezpieczeństwo transmisji danych w sieciach sensorowych*, [w:] Zeszyty Naukowe Akademii Morskiej w Gdyni. Wybrane zagadnienia telekomunikacji, Gdynia, str. 88–98, 2011.

[WAW03] Wawszczyk A., *E-gospodarka. Poradnik przedsiębiorcy*, Warszawa 2003, (http://www.parp.gov.pl/files/74/81/88/e_gospodarka.pdf, dostęp: 10.11.2014).

[WIK14] Wikipedia, SecurID, [dostęp: 11.10.2014], online: http://en.wikipedia.org/wiki/SecurID.

[WIK14a] Wikipedia, Karta kryptograficzna, [dostęp: 11.10.2014], online: http://pl.wikipedia.org/wiki/Karta_kryptograficzna.

[WIK14b] Wikipedia, Karta elektroniczna, dostęp: 11.10.2014], online: http://pl.wikipedia.org/wiki/Karta_elektroniczna.

[ZEG14] Zegarek P., Dokumentacja ochrony danych osobowych w firmie, [dostęp: 11.10.2014], online: http://www.een.org.pl/index.php/ochrona-konkurencji-i-konsumentow---spis/page/3/articles/dokumentacja-ochrony-danych-osobowych-w-firmie.html.

[ZHE11] Zheng L., Zhang H., Han W., Zhou X., He J., Zhang Z., Gu J., Wang J., *Technologies, Applications, and Governance in the Internet of Things,* [w:] Internet of Things – Global Technological and Societal Trends from Smart Environments and Spaces to Green Ict, [red.] Vermesan O., Friess P., River Publishers, Aalborg, Denmark 2011.

[ŻEB00] Żebrowski A., Kwiatkowski M., *Bezpieczeństwo informacji III Rzeczypospolitej*, Oficyna Wydawnicza Abrys, Kraków 2000.

Wykaz autorów

Cichorzewska Marzena	Politechnika Lubelska Wydział Zarządzania Katedra Zarządzania Zakład Zarządzania Potencjałem Społecznym
Depta Lidia	
Dzieńkowski Mariusz	Politechnika Lubelska Wydział Elektrotechniki i Informatyki Zakład Inżynierii Oprogramowania i Systemów Baz Danych
Gulańczyk Elżbieta	
Haleniuk Mariusz	Politechnika Lubelska Wydział Zarządzania Katedra Zarządzania Zakład Systemów Informatycznych
Juszczyk Marta	Politechnika Lubelska Wydział Zarządzania Katedra Zarządzania Zakład Systemów Informatycznych
Miłosz Elżbieta	Politechnika Lubelska Wydział Elektrotechniki i Informatyki Zakład Programowania i Grafiki Komputerowej
Rudy Lidia	
Wit Bogdan	Politechnika Lubelska Wydział Zarządzania Katedra Zarządzania Zakład Systemów Informatycznych