STOWARZYSZENIE EKONOMISTÓW ROLNICTWA I AGROBIZNESU
Roczniki Naukowe ● tom XI ● zeszyt 4

Artur Winnicki

Wyższa Szkoła Policji w Szczytnie

BEZPIECZEŃSTWO INFORMATYCZNE OBSZARÓW WIEJSKICH NA PRZYKŁADZIE JEDNOSTEK SAMORZĄDU TERYTORIALNEGO WOJEWÓDZTWA WARMIŃSKO-MAZURSKIEGO

THE COMPUTER SECURITY SYSTEMS OF RURAL AREAS BASED ON THE LOCAL AUTHORITY UNITS OF THE WARMIŃSKO-MAZURSKIE VOIVODESHIP

Słowa kluczowe: bezpieczeństwo informatyczne, obszary wiejskie, samorząd terytorialny
Key words: computer systems security, computer security systems, rural areas, local authority

Synopsis. Podjęto próbę zaprezentowania stanu bezpieczeństwa systemów informatycznych użytkowanych przez jednostki samorządu terytorialnego na terenach wiejskich. Bezpieczeństwo tych systemów ma ogromne znaczenie dla funkcjonowania każdej instytucji. Przeanalizowano liczbę stosowanych zabezpieczeń oraz rodzaje zagrożeń z jakimi zetknęli się pracownicy urzędów.

Wstęp

Informacja we współczesnym społeczeństwie stała się towarem często cenniejszym niż inne dobra. Wiąże się ona z realizacją podstawowych funkcji zarządzania to jest planowania, organizowania, kierowania i kontrolowania. Powinna ona spełniać następujące funkcje [Niedźwiedzka 2005]:
– pełnić istotną rolę w procesie podejmowania decyzji w różnego rodzaju transakcjach związanych z działalnością produkcyjno-handlową,
– stanowić podstawę podejmowania decyzji w transakcjach na rynku papierów wartościowych,
– stanowić element oceny działalności przedsiębiorstwa przez właścicieli,
– umożliwiać sprawowanie kontroli przez wyspecjalizowane agendy rządowe.

Sprawne i bezpieczne przetwarzanie informacji jest gwarancją właściwego zarządzania daną organizacją. Ogromna liczba informacji przetwarzanych każdego dnia powoduje, iż systemy informatyczne stały się podstawowym narzędziem pracy. Funkcjonowanie współczesnych urzędów i instytucji trudno sobie wyobrazić bez komputerów i oprogramowania komputerowego, czyli systemów informatycznych. Bezpieczeństwo sytemu informacyjnego musi zgodnie z polską normą PN-13335-1spełniać określone kryteria [Białas 2007]:
– poufność (*confidentiality*), właściwość zapewniająca, że informacja nie jest udostępniana lub ujawniana nieautoryzowanym osobom, podmiotom lub procesom,
– autentyczność (*authenticity*), właściwość zapewniająca, że tożsamość podmiotu lub zasobu jest taka jak deklarowana; dotyczy użytkowników, procesów, systemów lub nawet instytucji; autentyczność jest związana z badaniem, czy ktoś lub coś jest tym lub czym za kogo lub za co się podaje,
– dostępność (*availability),* właściwość bycia dostępnym i możliwym do wykorzystania na żądanie w założonym czasie przez kogoś lub coś, kto lub co ma do tego prawo,
– integralność danych (*data integrity*) właściwość zapewniająca, że dane nie zostały zmienione lub zniszczone w sposób nieautoryzowany,
– integralność systemu (system *integrity*) właściwość polegająca na tym, że system realizuje swoją zamierzoną funkcję w nienaruszony sposób, wolny od nieautoryzowanej manipulacji, celowej lub przypadkowej,
– integralność (*integrity*) danych oraz systemu,
– rozliczalność (*accountability*) właściwość zapewniająca, że działania podmiotu (np. użytkownika) mogą być jednoznacznie przypisane tylko temu podmiotowi,
– niezawodność (*reliability*) właściwość oznaczająca spójne, zamierzone zachowanie i skutki.

Brak odpowiednich zabezpieczeń systemów informatycznych może doprowadzić do awarii i przynieść niewyobrażalne szkody.

Cel i metoda

Podstawowym celem badań było ustalenie stanu zabezpieczeń przed przestępczością komputerową systemów informatycznych użytkowanych w instytucjach samorządowych.

Materiał badawczy stanowiły dane pozyskane z urzędów gmin wiejskich. Badaniami objęto 64 urzędy gmin wiejskich województwa warmińsko-mazurskiego, tj. 100% urzędów gmin wiejskich tego województwa. Analizie badawczej poddano 11 ankiet dotyczących stanu bezpieczeństwa informatycznego jednostki z następujących gmin: Kowlalewo Oleckie, Kurlanki, Kozłowo, Płośnica, Janowiec Kościelny, Kalinowo, Piecki, Świętajno, Wielbark, Wydminy, Rychliki. Pozostałe gminnie nie odpowiedziały na przesłane ankiety.

Do analizy danych wykorzystano kwestionariusz ankiety, składający się z 23 pytań, dzięki którym zostały zestawione dane dotyczące: posiadania przez urząd własnej strony WWW (pytanie 1), podmiotu zajmującego się codzienną obsługą informatyczną urzędu (pytanie 2), faktu połączenia komputerów firmowych w sieć (pytanie 3), sposobu łączenia się z Internetem (pytanie 4), stopnia ważności technologii informatycznych dla urzędu (pytanie 5), stopnia ochrony komputerów podłączonych do Internetu (pytanie 6), a także zagrożeń związanych z przestępczością w Internecie – ich stopnia (pytanie 7), częstotliwości występowania (pytanie 8). W oparciu o przedmiotową ankietę dokonano analizy zdarzeń związanych z bezpieczeństwem w sieci będących problemem dla urzędu (pytanie 9), zabezpieczeń stosowanych w urzędzie (pytanie 10), a także stopnia systematyczności aktualizacji oprogramowania (pytanie 11), sposobu przechowywania haseł dostępowych, jeśli są używane w firmie (pytanie 12), faktu skanowania komputerów programami antywirusowymi (pytanie 13), faktu skanowana odbieranej poczty programem antywirusowym (pytanie 14) i szyfrowania korespondencji elektronicznej (pytanie 15), faktu kasowania lub czyszczenia danych ze zużytych nośników danych (pytanie 16), robienia kopii zapasowych (pytanie 17), ze wskazaniem liczby kopii (pytanie 18).

Dzięki ankiecie zestawiono dane dotyczące wykorzystywania w urzędzie podpisu elektronicznego (pytanie 19), rodzajów obaw towarzyszących przy załatwianiu ważnych spraw przez Internet (pytanie 20), a także czynników wpływających lub mogących wpłynąć na poprawę stanu bezpieczeństwa w firmie (pytanie 21), powodów istnienia braku zabezpieczeń komputerowych w firmach (pytanie 22) oraz faktu przeszkolenia z zakresu bezpieczeństwa IT osoby zajmującej się komputerami w firmie (pytanie 23).

Wyniki badań

W badanych gminach 91% posiadało własną stronę www poza obowiązkową stroną BIP. Internetowa witryna jest często określana jako oś komunikacji marketingowej, to za jej pomocą realizowanych jest większość działań promocyjnych [Mazurek 2008]. 82% badanych jednostek codzienną obsługę informatyczną urzędu zapewniał etatowy pracownik, w pozostałych osiemnastu procentach obsługę informatyczną realizował pracownik zatrudniony na umowę-zlecenie.

Sto procent badanych jednostek posiadało komputery połączone w sieć, a więc posiadało system teleinformatyczny. Definicję sytemu teleinformatycznego odnajduje się w ustawie *o świadczeniu usług drogą elektroniczną* [Dz.U. 2002, nr 144 poz. 1204 z późn.zm.]. Systemem teleinformatycznym zgodnie z wymienioną ustawą ustala zespół współpracujących ze sobą urządzeń informatycznych i oprogramowania, zapewniający przetwarzanie i przechowywanie, a także wysyłanie i odbieranie danych przez sieci telekomunikacyjne za pomocą właściwego dla danego rodzaju sieci urządzenia końcowego.

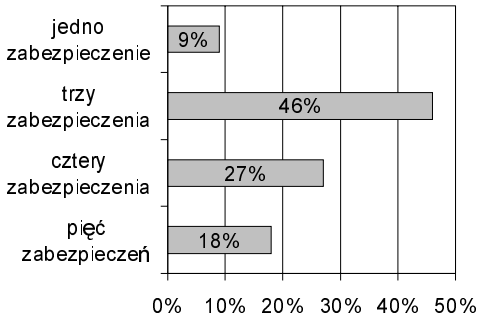
Dla 73% badanych urzędów technologie informatyczne są bardzo ważne, dla 18% ważne, a dla 9% średnio ważne. Cała populacja badanych jednostek posiadała stałe łącze z Internetem, w dziewięciu procentach stosowano stałe łącze, dostęp przez modem i telefonię komórkową. Tylko 18% uznało, że komputery w urzędach są chronione przed zagrożeniami z sieci w sposób zupełnie wystarczający, 55% za raczej wystarczający, zaś 18% uznało, że komputery są „średnio" zabezpieczone. Jednocześnie 55% twierdzi, że zagrożenia związane z przestępczością w Internecie należy uznać za bardzo duże, 36% określiło te zagrożenia jako duże, natomiast 9% uznało, iż zagrożenia są średnie. Większość to jest 82% badanych stwierdziło, że nie miało żadnych kłopotów z naruszeniem bezpieczeństwa w sieci.

W pytaniu o zagrożenia jakie występują w systemach informatycznych możliwe było zaznaczenie kilku odpowiedzi. Za najczęściej występujące zagrożenia związane z bezpieczeństwem respondenci uznali otrzymywanie niechcianej poczty, czyli spamu 82%.

Kolejnym zagrożeniem wymienianym przez ankietowanych 64% jest zainfekowanie komputerów wirusami. Inne zagrożenia to zainfekowanie programami szpiegowskimi, utrata zgromadzonych danych w wyniku awarii sprzętu lub oprogramowania, jak też próby zmiany treści na stronie www urzędu – na każde z tych zagrożeń wskazało równomiernie po 18% respondentów.

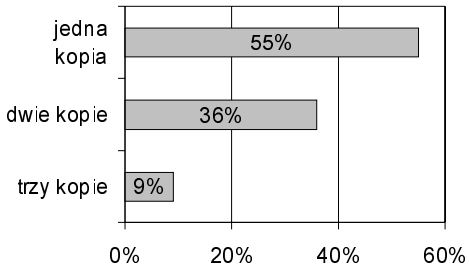
Najczęściej stosowanym zabezpieczeniem systemów informatycznych były programy antywirusowe, tj. 100% badanych, dodatkowo 73% używało haseł dostępowych, jednocześnie 64% stosowało także oprogramowanie typu firewall. Liczbę zabezpieczeń stosowanych przez badane jednostki obrazuje rysunek 1.

Wszyscy ankietowani stwierdzili, że zakupione oprogramowanie jest systematycznie aktualizowane, jednak należy zauważyć, iż ważna jest tu częstotliwość z jaką dokonuje się aktualizacji. W przypadku 18% badanych jednostek oprogramowanie aktualizowano raz w tygodniu. Hasła użytkowane do zabezpieczenia dostępu najczęściej przechowywano jedynie w formie papierowej – 55%, na papierze i nośnikach elektronicznych – 18%, wyłącznie na nośnikach elektronicznych – 9%. Wszyscy ankietowani systematycznie skanowali programami antywirusowymi komputery oraz odbieraną pocztę elektroniczną. Tylko 9% urzędów szyfrowało korespondencję elektroniczną.



Rysunek 1. Liczba zabezpieczeń stosowanych jednocześnie przez badane jednostki
Źródło: badania własne.

Wśród badanych 73% zużyte nośniki danych fizycznie niszczy, zaś 27% czyści zużyte nośniki. Metoda ta, nie jest najlepszym sposobem ochrony przetwarzanych informacji w sieci, ponieważ można odnaleźć wiele programów służących do odzyskiwania danych nawet po wielu formatowaniach. Wszyscy ankietowani robili kopie zapasowe danych przechowywanych w systemach informatycznych. Jest to sposób zabezpieczenia danych na wypadek awarii, a czasem są one jedynym sposobem odzyskania utraconych danych. Liczba wykonywanych kopii zapasowych obrazuje rysunek 2.



Rysunek 2. Liczba kopii zapasowych wykonywanych w badanych urzędach
Źródło: badania własne.

Sto procent badanych gmin używa podpisu elektronicznego. Podpis stosowany w procesie elektronicznej wymiany danych jest odpowiednikiem podpisu odręcznego stosowanego w środowisku dokumentów papierowych [Jurkowski 2001]. Zgodnie z polską normą PN-I- 02000 podpis elektroniczny to przekształcenie kryptograficzne danych, umożliwiające odbiorcy danych sprawdzenie autentyczności i integralności danych oraz zapewniające nadawcy ochronę przed zafałszowaniem danych przez odbiorcę lub osobę postronną [Siemieniuk 2002]. Według respondentów najwięcej obaw przy realizacji spraw przez Internet budzi kradzież tożsamości 55%, oraz brak pewności czy sprawa dotrze do właściwej instytucji i zostanie rozpatrzona – 27%. W celu poprawienia stanu bezpieczeństwa ankietowani, są zdania, że należy zakupić nowe lepsze oprogramowanie (typu firewall lub firewall sprzętowy), tj. 64%, ponadto należy również przeprowadzić szkolenia wszystkich pracowników, tj. 55% ankietowanych. Według 27% poza wymienionymi działaniami należy zatrudnić w urzędach pracowników znających się na bezpieczeństwie sieciowym. Ankietowani za przyczynę braku właściwych zabezpieczeń uznali brak wiedzy osób zarządzających jednostkami oraz brak środków na zakup zabezpieczeń po 55% (możliwe było wskazanie kilku czynników). Koleina przyczyna według badanych to brak środków na zatrudnienie specjalistów (45%) oraz na szkolenia (36%).

Tylko w 27% ankietowanych gmin osoba zajmująca się systemem informatycznym była na szkoleniu z zakresu bezpieczeństwa komputerowego w ostatnim roku, a 18% badanych pracownik w ogóle nie był szkolonych w tym zakresie.

Wnioski

1. Badane gminy wiejskie w większości posiadały własną stronę internetową, która jest niedrogim i atrakcyjnym środkiem promocji samorządów oraz źródłem informacji dla jej mieszkańców.
2. Obsługę informatyczną w większości badanych jednostek zapewniali pracownicy etatowi, świadczy to o sporym zapotrzebowaniu na wykonywaną przez nich pracę.
3. Technologie informatyczne są uznawane przez respondentów za bardzo ważne i ważne, oznacza to, iż są one otoczone szczególną troską przez badanych.
4. Wszystkie badane urzędy posiadają stały dostęp do Internetu oraz wewnętrzny system teleinformatyczny umożliwiający szybką komunikację.
5. Większość ankietowanych uznaje zabezpieczenie stosowane w firmie za raczej wystarczające oraz stosuje więcej niż jedno zabezpieczenie.
6. Mimo uznawania zabezpieczeń za wystarczające większość respondentów widzi obszary, w których można jeszcze zwiększyć bezpieczeństwo.
7. Widoczne są braki w szkoleniu z zakresu bezpieczeństwa informatycznego. W tym zakresie w ciągu jednego roku powstaje dużo nowych zagrożeń. Zaznaczyć tu jednak należy, że wiedzę tę częściowo pracownicy mogą uzupełniać przez samodoskonalenie.

Literatura

Białas A. 2007: Bezpieczeństwo informacji i usług w nowoczesnej instytucji i firmie. 34.
Dziennik Ustaw z 09 września 2002, nr 144 poz. 1204 z późn.zm.
Jurkowski A. 2001: Bankowość elektroniczna. Materiały i Studia, z. 125 NBP, 26.
Mazurek G. 2008: Promocja w Internecie. Narzędzia, zarządzanie, praktyka. 17.
Niedźwiedzka E. 2005: Informacja jako nadrzędny instrument zarządzania przedsiębiorstwem. Nowoczesne technologie informatyczne i ich wpływ na funkcjonowanie podmiotów gospodarczych. Wyższa Szkoła Finansów i Zarządzania w Białymstoku, 106.
Siemieniuk N. 2002: Zarządzanie finansami. Wyższa Szkoła Finansów i Zarządzania w Białymstoku, 86-87.

Summary

A computer security system is a crucial element of local institutions. The paper presents results from the research carried out in the offices of rural districts of the warmińsko-mazurske province. The security systems of these offices and the ways of computer data storing were analysed.

Adres do korespondencji:

mgr inż. Artur Winnicki
Wyższa Szkoła Policji w Szczytnie
Instytut Badań nad Przestępczością Zorganizowaną i Terroryzmem
ul. Marszałka Józefa Piłsudskiego 111
12-100 Szczytno
tel. (0 89) 621 59 68
e-mal: awinnic@wspol.edu.pl