PRACE NAUKOWE Akademii im. Jana Długosza w Częstochowie
SERIA: Edukacja Techniczna i Informatyczna 2011 z. VI

Edmund Golis, Jan Banasiak
Akademia im. Jana Długosza w Częstochowie

BADANIA REALIZACJI ZASAD BEZPIECZEŃSTWA DANYCH W SYSTEMACH KOMPUTEROWYCH MAŁYCH FIRM

Streszczenie

W pracy przedstawiono podstawowe zagadnienia dotyczące zasad bezpieczeństwa oraz metod ochrony danych w systemach komputerowych w firmach. Stan realizacji tych zasad w wybranych małych firmach obrazują przeprowadzone badania. Wyniki badań wskazują na wiele uchybień i braków w polityce bezpieczeństwa danymi w małych firmach oraz sugerują prowadzenie działań w kierunku uświadamiania ich właścicieli o zagrożeniach bezpieczeństwa danych.

słowa kluczowe: bezpieczeństwo danych, ochrona danych, system komputerowy, mała firma

Wprowadzenie

Powszechnie stosowane w wielu obszarach działalności współczesnego człowieka systemy komputerowe przechowują i przetwarzają wielkie ilości danych, dla których bezpieczeństwo ma priorytetowe znaczenie.

Pod pojęciem „bezpieczeństwa danych" należy rozumieć ich ochronę, „czyli zabezpieczenia przed nieupoważnionym lub nieprawidłowym, przypadkowym bądź umyślnym ujawnieniem, modyfikacją lub zniszczeniem"[1]. Ze względu na możliwe zagrożenia dla każdego systemu komputerowego konieczne jest wprowadzenie zbioru zasad, których zastosowanie wyeliminuje istniejące zagrożenia, zmniejszając przez to ryzyko utraty danych w firmie. Jest to

przesłanka do tworzenia formalnych, obowiązujących powszechnie na różnych szczeblach organizacyjnych systemów bezpieczeństwa informatycznego. „System bezpieczeństwa informatycznego jest to zestaw praw, zasad i reguł opisujących w formie zaleceń i procedur określających , w jaki sposób istotna, ważna dla firmy informacja powinna być w niej zarządzana i zabezpieczana, w jaki sposób dystrybuowana wewnątrz firmy, pomiędzy jej jednostkami organizacyjnymi i jak udostępnia kontrahentom oraz partnerom zewnętrznym”[2].

Celem pracy jest zaprezentowanie zagadnień dotyczących zasad bezpieczeństwa oraz metod ochrony danych w systemach komputerowych w firmach. W pracy przedstawiono również wyniki badań realizacji zasad bezpieczeństwa danych w małych firmach.

Bezpieczeństwo danych

Wyróżnia się trzy podstawowe aspekty bezpieczeństwa danych: poufność; integralność i dostępność.

Poufność danych oznacza „niedostępność treści zawartej w danych dla wszystkich podmiotów nie uprawnionych do jej odczytania”[1]. W zależności od znaczenia danych, których naruszenie poufności mogło być szczególnie niewskazane lub też kosztowne, nadaje się odpowiednio wysokie poziomy bezpieczeństwa (poufne, tajne, ściśle tajne itp.).

Podstawowym sposobem zapewnienia poufności danym jest szyfrowanie danych. Wszelkie procedury uwierzytelniania oraz ograniczania uprawnień dostępu czy też ograniczenie fizycznego dostępu do systemu komputerowego nazywamy środkami pośrednimi. Mimo zastosowania obu sposobów zapewniających poufność istnieje niebezpieczeństwo przypadkowego lub celowego jej naruszenia. Dlatego też systemy ochrony powinny nie tylko zapewniać poufność, lecz także zapewniać możliwość wykrycia prób i przypadków jej naruszenia.

Integralność danych oznacza, „że dane nie zostaną w żaden nieupoważniony sposób zmienione, a tym samym ich stan pozostanie zgodny z wymaganym i oczekiwanym stanem właściwym”[1] .

Naruszenia integralności danych mogą wyniknąć z:

- działań nieupoważnionego użytkownika;
- zaniedbań oraz błędów użytkowników upoważnionych;
- awarii;
- zakłóceń w transmisji;
- błędów w oprogramowaniu;
- działania wirusów.

Integralność musi być zapewniona podczas przetwarzania, przechowywania i przesyłania informacji podobnie jak poufność. Sposobami pośrednimi przyczyniającymi się do zapewnienia integralności danych są:

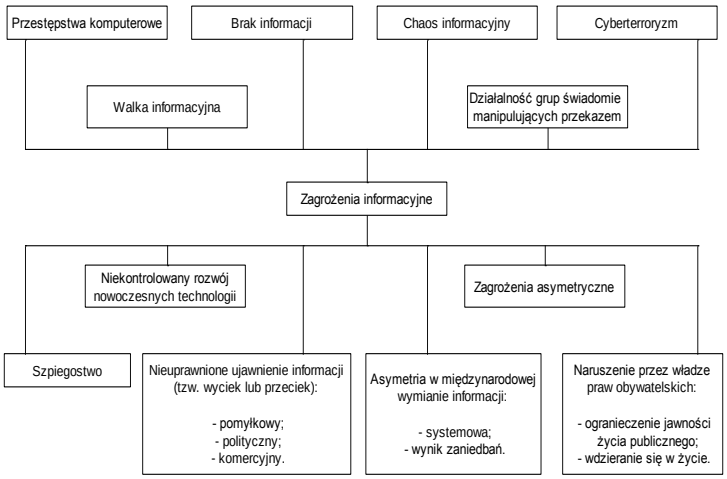
- stosowanie procedur uwierzytelniania;
- ograniczanie uprawnień dostępu;
- ograniczanie fizycznego dostępu do systemu komputerowego;
- stosowanie metod zwiększających niezawodność sprzętu oraz tolerancję na błędy;
- wykrywanie każdego przypadku lub próby naruszenia integralności danych.

Dostępność danych oznacza „niczym nieograniczoną możliwość korzystania z danych przez uprawnionych do tego użytkowników”[1]. Dostępność danych może być naruszana tymi samymi sposobami co integralność.

Dostępność zapewniana jest przez:

- stosowanie odpowiednio zabezpieczonych systemów operacyjnych;
- stały nadzór nad stopniem wykorzystania zasobów;
- stosowanie systemów sterowania ruchem sieciowym i obciążeniowym serwerów;
- stosowanie metod zwiększających niezawodność sprzętu i tolerancję na błędy.

Pojęcie bezpieczeństwa informacyjnego można przybliżyć poprzez identyfikację obszarów zagrożeń. Podział zagrożeń informacyjnych przedstawia rysunek 1.



Rys. 1. Podział zagrożeń informacyjnych [3]

Metody ochrony danych

Do zapobiegania utraty poufności, dostępności i integralności danych w systemie komputerowym stosowane są następujące metody zabezpieczeń:

Zabezpieczenia fizyczne przed nieupoważnionym dostępem oraz ogniem i wodą. Przedsięwzięcia składające się na ochronę fizyczną to:

- Kontrola dostępu do obiektów i pomieszczeń oraz monitoring;
- Systemy antywłamaniowe (urządzenia alarmowe);
- Stosowanie systemów zabezpieczeń przeciwpożarowych.

Zabezpieczenia organizacyjne, realizowane przez:

- Specjalne procedury postępowania dla osób korzystających z systemu komputerowego;
- Przygotowanie i stosowanie polityki bezpieczeństwa;
- Specjalna polityka przy kupowaniu sprzętu i oprogramowania;

Zabezpieczenia programowo-sprzętowe, realizowane przez:

- Specjalnie określone procedury stosowane przy projektowaniu i kodowaniu programów;
- Wykorzystanie odpowiednich platform oraz prawidłowo skonfigurowanego oprogramowania;
- Stosowanie: macierzy dyskowych, zasilaczy bezprzerwowych (UPS);
- Urządzenia oraz procedury do tworzenia kopii zapasowych danych;
- Wykorzystanie algorytmów szyfrowania informacji.

Kadrowe metody ochrony, do których zaliczamy:

- Specjalną kontrolę pracowników dopuszczonych do poufnych danych przez wyspecjalizowane służby;
- Przestrzeganie procedur zwalniania oraz zatrudniania pracowników;
- Stosowanie motywowania pracowników;
- Prowadzenie szkoleń pracowników [4].

Bezpieczeństwo danych w systemach komputerowych w małych firmach.

Badania przeprowadzone zostały za pomocą ankiet wypełnianych przez osoby zajmujące się bezpośrednio bezpieczeństwem w firmach, głównych 116 informatyków oraz właścicieli firm. Zamysłem było przeprowadzenie wielu ankiet lecz pomimo zapewnień i samego faktu, że proponowana ankieta jest

anonimowa wiele firm ze względu na specyfikę i poufność niektórych danych odmawiało współpracy. Przeważnie odmowy argumentowano bezpieczeństwem przedsiębiorstw oraz realizowaną polityką bezpieczeństwa informacji w przedsiębiorstwach. W kategorii małych firm czyli przedsiębiorstw o niewielkiej liczbie pracowników, od 1 do 9 osób, informacji udzieliły zaledwie cztery firmy: dwie to jednoosobowe oraz dwie kilkuosobowe.

Wyniki przeprowadzonych badań pokazują, że w przypadku małych firm żadna nie wdrożyła formalnego modelu bezpieczeństwa informacji.

W zakresie realizacji poszczególnych metod ochrony danych otrzymano następujące wyniki:

Zabezpieczenia fizyczne

Tylko jedna z przebadanych firm nie stosuje fizycznych zabezpieczeń, co uzasadnione zostało prowadzeniem działalności w lokalu mieszkalnym. Pozostałe wykorzystują zapobiegawczo czujniki alarmu przeciw włamaniowego oraz przeciwpożarowe. Ponadto tylko jedno przedsiębiorstwo korzysta z usług firmy ochroniarskiej.

Zabezpieczenia organizacyjne

W przypadku stosowanych metod organizacyjnych jedna przebadana firma nie wdrożyła żadnych. Pozostałe firmy wdrożyły specjalne reguły polityki zakupu sprzętu i oprogramowania wykorzystywanego do przetwarzania, przechowywania i przesyłania informacji oraz specjalne reguły postępowania ze zużytymi nośnikami magnetycznymi.

Zabezpieczenia programowo-sprzętowe

Wszystkie firmy deklarują stosowanie metod programowo, sprzętowych ochrony systemu komputerowego. W przypadku tworzenia kopii zapasowych dwie z czterech wykorzystują backup lustrzany, pozostałe dwie nie archiwizują danych, które wymagałyby tego typu zabezpieczeń. Połowa z podanych badaniu wykorzystuje zasilacze UPS typu on-line. Firewall oraz oprogramowanie antywirusowe okazały się najpopularniejszymi narzędziem do ochrony komputerów przed atakami z sieci rozległej. Dwie przebadane firmy wykorzystują programy szyfrujące w swoich działalności. Natomiast żadna nie stosuje oprogramowania do tworzenia wirtualnych sieci prywatnych (VPN).

Kadrowe metody ochrony

Połowa z firm biorąca udział w badaniu stosuje podział kompetencji i ról poszczególnych osób lub komórek firmy pod kątem realizacji polityki bezpieczeństwa w firmie. Jedno przedsiębiorstwo nie stosuje uwierzytelniania informacji i użytkowników, z kolei pozostałe trzy stosują mechanizmy haseł stałych lub zmiennych. Trzy z czterech poddanych analizie firm przyporządkowuje

pracowników do klas bezpieczeństwa. Żadna nie prowadzi kontroli pracy systemu komputerowego na podstawie zapisów jego aktywności.

Wnioski

Z przeprowadzonych badań wynika, że w małych firmach pomimo ogólnego zadowolenia z poziomu bezpieczeństwa stwierdzić można wiele uchybień i braków w polityce bezpieczeństwa danymi. Taki stan rzeczy może być spowodowany nieświadomością zagrożeń przez pracowników tych firm oraz brakiem funduszy na drogie systemy zabezpieczające. Sami ankietowani oceniają wysoko poziom bezpieczeństwa danych w swoich firmach i tylko jedna osoba udzielająca odpowiedzi w ankiecie była w stanie wskazać, co można zmienić w polityce bezpieczeństwa firmy, aby go zwiększyć. Należy więc prowadzić szeroko pojęte działania szkoleniowe w kierunku uświadamiania ich właścicieli o brakach i zagrożeniach bezpieczeństwa danych. Przeprowadzanie okresowych badań ankietowych stanu bezpieczeństwa danych w firmach i przekazywanie ich wyników zainteresowanym może w istotny sposób wpłynąć na poprawienie poziomu ich bezpieczeństwa.

Literatura

[1] Stokłosa J., Bilski T., Pankowski T.: Bezpieczeństwo danych w systemach informatycznych. Wydawnictwo Naukowe PWN. Warszawa – Poznań 2001

[2] Barczak A., Sydoruk T.: Bezpieczeństwo Systemów Informatycznych. Wydawnictwo Akademii Podlaskiej. Siedlce 2002

[3] Bączek P., Zagrożenia informacyjne a bezpieczeństwo państwa Polskiego, Wydawnictwo Adam Marszałek, Toruń 2006

[4] Liderman K., Bezpieczeństwo informacji w systemach informatycznych, WSISiZ, Warszawa 2001

Edmund Golis, Jan Banasiak
Akademia im. Jana Długosza w Częstochowie

RESEARCH ON SECURITY RULES EXECUTION, REGARDING DATA IN COMPUTER SYSTEMS OF SMALL BUSINESS

Summary

The paper describes issues concerning security rules execution of data in computer systems. The theoretical part focuses on the basics of corporate security as such and presents different kinds of threats together with corporate security methods. The described security methods might be divided into: physical, organizational, equipment and program. The second part of the paper concerns the results of research performed by means of anonymous surveys as well as conclusions drawn from them. Conclusions of the performed research will be aimed at security level evaluation in small business entities.

Keywords: security rules, data in computer systems, small business