Roczniki Kolegium Analiz Ekonomicznych
nr 29/2013

Ryszard Cierocki, Przemysław Jatkiewicz

Wydział Zarządzania
Uniwersytet Gdański

Bezpieczeństwo informacji w jednostkach samorządu terytorialnego

1. Wstęp

Codzienne obcowanie z komputerem jest obecnie zajęciem niemal powszechnym. Stanowi on zarówno niezbędne narzędzie pracy, jak i źródło wiedzy czy rozrywki. Pełni rolę komunikatora, dzięki któremu możemy rozmawiać, korespondować lub wymieniać się myślami, dokumentami i plikami multimedialnymi na forach lub portalach społecznościowych, takich jak popularne obecnie Facebook, Nasza Klasa czy Twitter. Jednak użytkownicy bardzo rzadko zastanawiają się nad tym, jak przebiega wymiana informacji w sieci. Z tego też powodu świadomość zagrożeń i niebezpieczeństw płynących z Internetu jest bardzo niska.

Z jakimi zagrożeniami możemy się spotkać w trakcie użytkowania komputera podłączonego do Internetu? Jest ich naprawdę wiele. Do najbardziej istotnych należą wirusy komputerowe, włamania czy też wyłudzenia informacji. Uniknięcie tych zagrożeń możliwe jest tylko wtedy, gdy oprócz bieżąco aktualizowanego systemu operacyjnego, użytkowanych aplikacji oraz oprogramowania antywirusowego będziemy mieć świadomość niebezpieczeństw czyhających na użytkownika Internetu oraz zdroworozsądkowe podejście do zagadnienia wymiany danych w sieci.

W każdym systemie informatycznym, począwszy od najprostszego, składającego się z pojedynczego użytkownika siedzącego przy komputerze, na wielkich, korporacyjnych sieciach z dziesiątkami tysięcy pracowników skończywszy, gdy rozważać będziemy kwestie bezpieczeństwa, to zawsze człowiek będzie najsłabszym ogniwem. Wydaje się, że urzędnicy znacznie poważniej traktują

zagrożenia bezpieczeństwa informacji oraz są na nie mniej podatni niż przeciętni użytkownicy systemów informatycznych. W dalszej części artykułu zostały przedstawione wyniki badań przeprowadzonych w pięciu jednostkach samorządów terytorialnych. Ich nazwy, ze względu na możliwe konsekwencje prawne, nie zostały ujawnione.

2. Wprowadzenie do tematu bezpieczeństwa informacji

Bezpieczeństwo informacji, wraz z jego istotnym elementem, jakim jest bezpieczeństwo systemów informatycznych, ma niebagatelny wpływ na działalność organizacji. Dlatego też najważniejsze zasady obowiązujące w tej dziedzinie zostały opisane, a także unormowane dokumentami stworzonymi przez organizacje powołane właśnie w tym celu.

W literaturze można znaleźć wiele definicji bezpieczeństwa, które jest terminem polisemantycznym. Na potrzeby artykułu proponuje się przyjęcie definicji zawartej w normie PN-ISO/IEC 27001[1], według której bezpieczeństwo informacji to „zachowanie poufności, integralności i dostępności informacji. Dodatkowo, mogą być brane pod uwagę inne własności, takie jak autentyczność, rozliczalność, niezaprzeczalność i niezawodność". Z kolei norma PN-ISO/IEC 17799 wskazuje na cele ochrony informacji, którymi są[2]:

- zapewnienie ciągłości działania,
- minimalizacja ryzyka,
- maksymalizacja zwrotu z inwestycji,
- maksymalizacja możliwości biznesowych.

Jeżeli założymy, że w chwili obecnej informacja stanowi dla przedsiębiorstwa taką samą – lub nawet większą – wartość niż maszyny i urządzenia, budynki czy zasoby ludzkie, to dojdziemy do wniosku, iż ochrona danych jest bardziej istotna niż fizyczna ochrona mienia tego podmiotu.

Z pewnością nie jest to wniosek bezpodstawny. Stosunkowo niedawno popularne było powiedzenie, że najważniejszą wartością przedsiębiorstwa

[1] *Polska Norma PN-ISO/IEC 27001 Technika informatyczna. Techniki bezpieczeństwa. Systemy zarządzania bezpieczeństwem informacji. Wymagania*, Polski Komitet Normalizacyjny, Warszawa 2007.

[2] *Polska Norma PN-ISO/IEC 17799 Technika informatyczna. Techniki bezpieczeństwa. Praktyczne zasady zarządzania bezpieczeństwem informacji*, Polski Komitet Normalizacyjny, Warszawa 2007.

są zasoby ludzkie. Jednak fakty wskazują, że firmy, które straciły budynki, maszyny czy też całe wartościowe zespoły ludzi, o których powszechnie mówiło się, iż są niezastąpieni, potrafiły przetrwać, pomimo poniesionych strat. Często nawet zdarzenia takie stawały się przyczyną ich jeszcze bardziej efektywnego rozwoju. Jednak utrata informacji, takich jak bazy danych klientów i pracowników, projekty produktów czy wyniki badań działów zajmujących się rozwojem produktu, może spowodować upadek, z którego przedsiębiorstwo nie będzie potrafiło się podnieść. Informacje takie mają bezcenną wartość dla konkurencji. Ich ujawnienie może spowodować bezpowrotną utratę klientów, wartościowych i doświadczonych pracowników oraz przewagi technologicznej wynikającej z prowadzonych przez organizację badań i doświadczeń. Przykładem jest holenderska firma DigiNotar, która ogłosiła upadłość po przejęciu przez hakerów 563 cyfrowych certyfikatów[3].

W literaturze przedmiotu napotkać można wiele różnych klasyfikacji zagrożeń bezpieczeństwa informacji. Podział zagrożeń ze względu na lokalizację ich źródeł przedstawia się następująco[4]:

- wewnętrzne (powstające wewnątrz organizacji), obejmujące zagrożenie utratą, uszkodzeniem lub brakiem dostępu do danych spowodowane błędem, przypadkiem albo celowym działaniem nieuczciwych użytkowników;
- zewnętrzne (powstające poza organizacją), które obejmują zagrożenie utratą, uszkodzeniem danych lub pozbawieniem możliwości obsługi przez celowe lub przypadkowe działanie ze strony osób trzecich w stosunku do sieci lub systemu;
- fizyczne, w których utrata, uszkodzenie danych lub brak możliwości obsługi następuje z powodu wypadku, awarii, katastrofy lub innego nieprzewidzianego zdarzenia wpływającego na system informacyjny bądź urządzenie sieciowe.

Przedstawione kryteria obecnie są coraz trudniejsze do zastosowania. Współczesne systemy informacyjne, a w szczególności systemy instytucji publicznych, są często obsługiwane przez szeroką rzeszę użytkowników, niezatrudnionych przez organizację, której system jest własnością. Jednakże ze względu na jego przeznaczenie (publiczne) nie można ich nazwać osobami trzecimi. Niesłuszne wydaje się również wydzielenie zagrożenia fizycznego. Jest ono skutkiem działania lub częściej zaniechania działania osób odpowiedzialnych za eksploatację i nadzór nad systemami informacyjnymi. Należy także zwrócić uwagę na to,

[3] Raport firmy F-Secure, *DigiNotar Hacked by Black. Spook and Iranian Hackers*, 30.08.2011.

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

iż bezzasadnie dokonano rozdziału systemu informacyjnego oraz urządzeń sieciowych.

Na potrzeby artykułu proponuje się przyjąć podział zagrożeń ze względu na źródło ich powstawania:

1) awarie sieci elektrycznej,
2) awarie sprzętu,
3) fizyczna kradzież dokumentów,
4) kradzieże sprzętu,
5) pomyłki i zaniedbania użytkowników systemu informatycznego,
6) pożar, zalanie, inne zdarzenia losowe,
7) wirusy,
8) włamania do systemu informatycznego,
9) wyłudzenie informacji,
10) utrata wsparcia technicznego.

Całkowite wyeliminowanie zagrożeń jest nieosiągalne dla większości organizacji. Nie znaczy to, że nie powinny one czynić starań, aby zmniejszyć podatność eksploatowanych systemów. Podatność systemu teleinformatycznego została zdefiniowana w rozporządzeniu Rady Ministrów z dnia 12 kwietnia 2012 r. jako „właściwość systemu teleinformatycznego, która może być wykorzystana przez co najmniej jedno zagrożenie”[5]. Przeprowadzone badania, udokumentowane w dalszej części niniejszej pracy, pozwalają uzyskać obraz tego, jak organizacje samorządu terytorialnego przygotowane są na wystąpienie wyszczególnionych zagrożeń.

3. Metodyka badań

Badaniami przeprowadzonymi w latach 2010–2011 zostało objętych pięć jednostek o różnych wielkościach i usytuowanych na różnych stopniach samorządu terytorialnego. Przed przystąpieniem do badań uzyskano zgodę od kierownictwa jednostek na ich przeprowadzenie. Był to najtrudniejszy i najbardziej czasochłonny etap. Najczęściej spotykano się z brakiem akceptacji bez podania przyczyn. Argumentami podawanymi przy odmowie były pozyskanie

[5] Rozporządzenie Rady Ministrów z dnia 12 kwietnia 2012 r. w sprawie Krajowych Ram Interoperacyjności, minimalnych wymagań dla rejestrów publicznych i wymiany informacji w postaci elektronicznej oraz minimalnych wymagań dla systemów teleinformatycznych (Dz.U. z 2012 r., poz. 526).

przez badającego, jako osoby niezależnej, wiedzy o słabościach systemu przy jednoczesnym, długotrwałym procesie ich usuwania oraz zapisy umów zawartych z wykonawcami systemu, zabraniające przeprowadzania takich testów przez strony trzecie. Warto zwrócić uwagę, iż wspomniane zapisy są sprzeczne z pkt A.6.1.8 normy ISO 27001, mówiącym o niezależnych przeglądach bezpieczeństwa informacji.

Zaniepokojenie wzbudzić może również brak jakiejkolwiek weryfikacji tożsamości badacza. Urzędnicy nie zażądali żadnego dokumentu mogącego ją potwierdzić. Nie podjęli też innych czynności, aby osiągnąć ten cel, np. kontakt z uczelnią. Autor nie podpisywał oświadczenia o zachowaniu poufności, nie otrzymał również odpowiedniego upoważnienia.

Zastosowano następujące metody badawcze:

- ankietowanie,
- wywiad standaryzowany,
- testy penetracyjne.

Ankiety w liczbie odpowiadającej liczbie pracowników badanych organizacji, tj. 893, zostały dostarczone do ich kancelarii, które dystrybuowały je wśród urzędników. Zwróconych zostało 527 ankiet, czyli ponad 59%. Tak niski zwrot może być tłumaczony tym, iż ankietowani nie przywiązywali wagi do badań lub, pomimo zapewnienia o anonimowości, obawiali się wyrazić własną opinię. Ankiety zawierały 12 pytań, wszystkie o charakterze zamkniętym.

Wywiad standaryzowany oparty został na załączniku A normy ISO 27001, która w domyśle zalecana jest dla systemów informatycznych używanych przez podmioty publiczne do realizacji zadań publicznych. Rozporządzenie Rady Ministrów z dnia 11 października 2005 r. mówi, iż powinny one spełniać właściwości i mieć cechy określone w normach ISO w zakresie[6]:

1) funkcjonalności,
2) niezawodności,
3) używalności,
4) wydajności,
5) przenoszalności,
6) pielęgnowalności.

Podmiot publiczny jest zobligowany do wdrożenia polityki bezpieczeństwa dla wspomnianych systemów. Normą ISO zatwierdzoną przez PKN, a odnoszącą się do bezpieczeństwa informacji jest właśnie PN-ISO/IEC 27001:2007.

[6] Rozporządzeniu Rady Ministrów z dnia 11 października 2005 r. w sprawie minimalnych wymagań dla systemów teleinformatycznych (Dz.U. z dnia 28 października 2005 r.).

Wywiady przeprowadzone były z właścicielami procesu zarządzania bezpieczeństwem informacji. Funkcję tę zwykle pełnili administratorzy systemów informatycznych, kierownicy działów IT lub Administratorzy Bezpieczeństwa Informacji. Zostały one poprzedzone analizą dokumentów, takich jak Polityka bezpieczeństwa czy Procedury operacyjne. Pozwoliła ona zawęzić liczbę pytań i skupić się na sposobie realizacji zawartych w dokumentacji zapisów. Oprócz pytań powiązanych ze wspomnianą normą starano się uzyskać informacje dotyczące wielkości organizacji, struktury organizacyjnej wyodrębnionej do zarządzania bezpieczeństwem informacji oraz wielkości systemu informatycznego.

Na testy penetracyjne składały się:

- skany sieci wewnętrznych,
- test socjotechniczny.

Skany sieci wewnętrznych jednostek miały wykryć słabość jej zabezpieczeń przed atakami dokonanymi wewnątrz organizacji. Ataki te mogą być przeprowadzane przez nieuczciwych pracowników, kontrahentów wykonujących prace w siedzibie firmy lub inne osoby, które ze względu na niedoskonałości organizacyjne zdobyły bezpośredni dostęp do infrastruktury technicznej systemu informacyjnego. Skany były przeprowadzane przy użyciu skanera sieciowego GFI LanGuard[7]. We wrześniu 2010 r. zdobył on pierwsze miejsce w rankingu skanerów sieciowych prowadzonym prze „Information Security Magazine"[8]. Potrafi wykryć ponad 15 000 zagrożeń dotyczących platform Windows, Linux i MacOS włącznie z maszynami wirtualnymi. Pobiera aktualne informacje o podatności na atak z takich baz, jak SANS Top 20, opracowanej przez SANS Institute (SysAdmin, Audit, Network, Security), i korzysta z języka OVAL (ang. *Open Vulnerability and Assessment Language*), opracowanego przez amerykański NIST (National Institute Standards and Technology). Język ten, oparty na XML (ang. *Extensible Markup Language*), standaryzuje etapy procesu testowania systemu[9]. GFI Languard, skanując sieć, odszukuje oraz kategoryzuje zagrożenia związane z otwartymi portami, słabymi hasłami, niebezpiecznymi urządzeniami i programami oraz brakiem zainstalowanych uaktualnień systemu i aplikacji.

Test socjotechniczny polegał na próbie wyłudzenia hasła do komputera. Zakładając, że realny atak mógłby nastąpić z zewnątrz, przy użyciu poczty elektronicznej, przetestowano grupę użytkowników posiadających służbowy,

[7] http://www.gfi.com/lannetscan, 30.03.2011.

[8] *2010 Information Security magazine Readers' Choice Awards*, „Information Security Magazine" 2010, no. 9.

[9] *An Introduction to the OVAL™ Language Version 5.0*, MITRE Corporation 2006.

zewnętrzny adres. W celu uwiarygodnienia zapytania o hasło wiadomość musiała być wysłana z adresu możliwie najbardziej podobnego do adresów firmowych. Technika podszywania się pod innego użytkownika sieci, zwana spoofingiem, jest bardzo popularna wśród hakerów. Założono domenę, której nazwa była łudząco podobna do nazwy domeny badanej jednostki. Różnica między ich nazwami ograniczała się do odmienności w zakresie jednego znaku. Kolejnym krokiem było skorzystanie z usługi Google Apps, która umożliwiła przypisanie uzyskanej domeny do prostego serwera poczty. Utworzono konto pocztowe, którego adres był identyczny z adresem Administratora Bezpieczeństwa Informacji testowanej organizacji, oczywiście z wyjątkiem części domenowej. Po dokonaniu wymienionych operacji wysłano do losowo wybranej grupy 51 osób wiadomość o temacie „Powiadomienie" i następującej treści:

„Witam,
w związku z rekonfiguracją kontrolera domeny w dniu 30.03.2012 i przeprowadzaniem w związku z tym zmian na komputerach osobistych proszę o przesłania loginu i hasła dostępowego do Pani/Pana komputera.
Z poważaniem
Administrator Bezpieczeństwa Informacji
Imię i Nazwisko ABI"

Z powodu wysłania powyższej wiadomości w dniu 29 marca 2012 r. użytkownicy nie mieli zbyt wiele czasu na odebranie wiadomości i zareagowanie na jej treść.

4. Wyniki badań

Wyniki badań zostaną omówione w kontekście wdrożenia i skuteczności zabezpieczeń przed poszczególnymi zaproponowanymi w artykule grupami zagrożeń. Ze względu na objętość artykułu zostaną zaprezentowane jedynie w odniesieniu do:

1) błędów i zaniedbań użytkowników systemu informatycznego,
2) włamań do systemu informatycznego,
3) wyłudzenia informacji.

Do błędów zaliczamy zachowania użytkowników nierozumiejących w pełni funkcji oprogramowania oraz zasad działania systemów informatycznych. Są

to błędy popełniane bardzo często i dlatego statystycznie przynoszą najwięcej szkód[10].

Firma Kroll Ontrack Inc., zajmująca się odzyskiwaniem danych, opublikowała wyniki badań przeprowadzonych w 17 krajach, w tym w Polsce, dotyczących przyczyn utraty danych. W okresie kwiecień–czerwiec 2010 r. ankietowano 2000 respondentów, wśród których znaleźli się użytkownicy prywatni oraz przedstawiciele biznesu, instytucji publicznych (w tym rządowych) oraz partnerzy i sprzedawcy rynku IT. Około 40% z nich uznało, że to błąd człowieka przyczynił się do utraty przez nich danych. W stosunku do badań przeprowadzonych w 2005 r. nastąpił 29% wzrost udziału tego właśnie czynnika[11].

Zaniedbania użytkowników systemu informatycznego to jedno z najczęściej występujących zagrożeń systemów informatycznych. Rzadko kiedy ich skutki odczuwalne są bezpośrednio po wystąpieniu, a rozmiar jest wprost proporcjonalny do istotności zadań oraz uprawnień użytkownika. Przeprowadzone skany sieci wewnętrznej mogą ujawnić zaniedbania służb informatycznych, które mają największy wpływ na działanie systemu informatycznego.

W ramach badań przeskanowano 463 węzły sieci w czterech z pięciu organizacji. Odnaleziono 2787 zagrożeń, co daje średnio ok. sześć przypadających na pojedynczy węzeł. Szczegółowe dane liczbowe dotyczące węzłów i zagrożeń w każdej badanej organizacji przedstawia tabela 1.

Tabela 1. Węzły i ich zagrożenia w badanych organizacjach

	Org. B	Org. C	Org. D	Org. E
Liczba węzłów	315	60	48	40
Liczba zagrożeń	2198	183	358	48
Średnia liczba zagrożeń przypadająca na węzeł	7	3	7	<1
Mediana	10	1	10	0
Maksimum	66	66	11	20

Źródło: opracowanie własne.

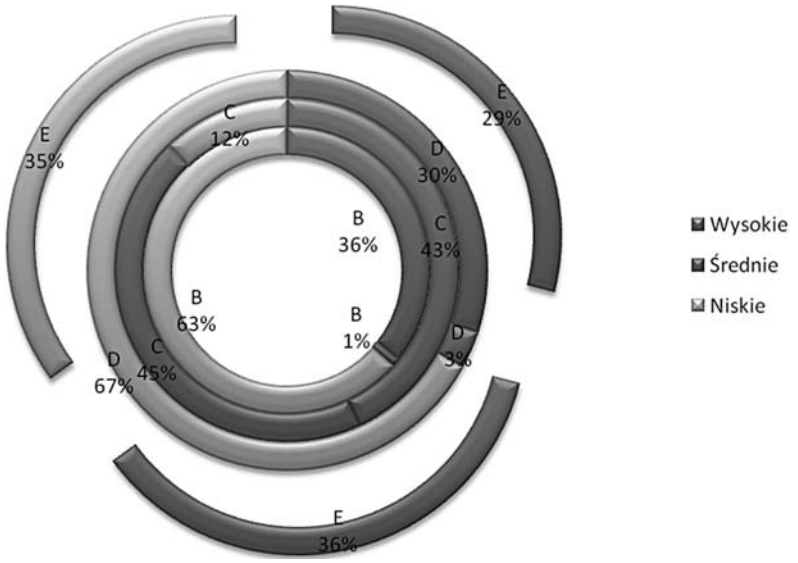
Analizując dane z tabeli 1, można dostrzec dużą różnicę pomiędzy medianą czy średnią liczbą zagrożeń przypadającą na pojedynczy węzeł sieci. Odstępstwem od tej obserwacji jest organizacja D. Przeprowadzona bardziej szczegółowa

[10] A. Barczak, T. Sydoruk, *Bezpieczeństwo systemów informatycznych zarządzania*, Bellona, Warszawa 2003.

[11] *Użytkownicy komputerów z całego świata wskazali, jak i dlaczego tracą dane*, komunikat prasowy, Kroll Ontrack Inc. z dnia 27.07.2010.

kontrola pozwoliła na ustalenie, iż w organizacjach B, C i E wszystkie najbardziej zagrożone węzły sieci to komputery eksploatowane przez informatyków. Wynika to zarówno z szerokich uprawnień, m.in. do instalacji wszelkiego typu oprogramowania, jak i z testowania przez właśnie tę grupę zawodową nowych rozwiązań informatycznych. Można dojść do paradoksalnego wniosku, że największym zagrożeniem dla organizacji są właśnie jej służby informatyczne. Potwierdzają się informacje uzyskane podczas wywiadów, mówiące o jedynie okazjonalnym wydzielaniu środowisk testowych.

Dane przedstawione na rysunku 1 pozwalają na stwierdzenie, iż zagrożenia stopnia wysokiego nie są sytuacją wyjątkową. Kontrole przeprowadzane nawet najbardziej prostym, darmowym oprogramowaniem powinny wykazać ich istnienie.



Rysunek 1. Rozkład zagrożeń według poszczególnych klas i organizacji

Źródło: opracowanie własne.

Spośród ok. 100 rodzajów zagrożeń tylko nieliczne dotyczą więcej niż kilku węzłów sieci. Wzorując się na zasadzie Pareto, mówiącej, iż 20% badanych obiektów związane jest z 80% pewnych zasobów, postanowiono wyodrębnić rodzaje zagrożeń o największej liczebności. Jedynie 12 rodzajów odpowiada za 80% lub większą liczbę wszystkich zagrożeń. Na pierwszym miejscu plasują się niezainstalowane uaktualnienia. Z uzyskanych dodatkowo wyjaśnień wynika, że aktualizacje instalowane są z centralnego serwera WSUS (ang. *Windows*

Server Update Services) po uprzednim zatwierdzeniu ich przez pracownika działu informatycznego. Problemem są aktualizacje wymagające do instalacji praw administratora systemu, których użytkownicy są pozbawieni. Z tego też względu instalacja ta odbywa się podczas świadczenia innych usług pracownikom.

Większość pozostałych zagrożeń związana jest ze standardową konfiguracją instalowanych systemów operacyjnych. W jednostkach nie opracowano procedur dotyczących konfiguracji nowo wprowadzanych elementów systemu, wszystkie jednak są łatwe do usunięcia poprzez GPO (ang. *Group Policy Object*), stanowiącego element Active Directory[12]. Reszta wynika z braku wiedzy fachowej. Na uzupełniające pytanie o przyczynę niezabezpieczenia konta administratora uzyskano odpowiedź, iż informatyk nie zdawał sobie sprawy, że konto takie jest standardowo instalowane w systemie Windows.

Ciekawą informację uzyskano w organizacji D. Informatyk, pod kontrolą którego wykonywany był skan, wyjaśnił, iż części uaktualnień nie zainstalował świadomie, gdyż funkcjonujące w urzędzie oprogramowanie nie zawsze pracuje prawidłowo po ich zaimplementowaniu. Przykładem jest system bankowy wymagający starej wersji środowiska Java.

Zarówno małą różnorodność zagrożeń, jak i niską ich liczbę w organizacji E można tłumaczyć tym, że badania wykonywane były w momencie kończenia wdrażania domeny wraz z Active Directory. Świeżo zainstalowane systemy operacyjne na końcówkach sieci nie były obciążone usługami implementowanymi w czasie dłuższej eksploatacji.

Włamanie do systemu informatycznego to nic innego jak nieautoryzowany dostęp do niego, skutkujący wyciekiem danych lub utratą kontroli. Najprostszym, a zarazem najskuteczniejszym sposobem nielegalnego dostania się do systemu jest odgadnięcie lub zdobycie hasła i nazwy użytkownika. W dużych organizacjach zatrudniających licznych pracowników użytkujących komputery nazwy użytkowników przyznawane są według określonych zasad, np. pierwsza litera imienia, znak kropki i nazwisko. Informacja o sposobie ich generowania jest powszechnie znana wśród kadry pracowniczej i nieuznawana jest za szczególnie chronioną. Do rzadkości należy również usuwanie standardowych nazw użytkowników administrujących systemem, takich jak „admin", „administrator" czy „manager". Stąd odgadnięcie ich nie jest zadaniem trudnym, szczególnie w jednostkach publicznych, w których nazwiska urzędników są jawne i często wypisane na drzwiach biur. Każdy administrator spotkał się również z proble-

[12] A.G. Lowe-Norris, R. Allen, B. Desmond, J. Richards, *Windows 2000 Active Directory*, O'reilly Vlg. Gmbh & Co., 2008.

mem zapisywania haseł przez pracowników i pozostawiania ich w dostępnym dla innych miejscu. Ponieważ pamięć ludzka jest zawodna, poza zapisywaniem, panuje też tendencja do konstruowania najprostszych i najkrótszych haseł.

Rozprowadzone wśród pracowników badanych instytucji ankiety pozwalają na ocenę sposobu korzystania z loginów i haseł. Dane uzyskane z ankiet zamieszczone zostały w tabeli 2. Generalnie większość pracowników nie korzysta z cudzych loginów, lecz niewiele mniej wykorzystuje je często lub sporadycznie. Nieliczni uważają, że użyczanie swoich loginów jest naganne.

Tabela 2. Korzystanie z cudzych loginów i ocena ich użyczania

		Organizacja				
		A	B	C	D	E
Korzystanie z cudzych loginów	Nie korzysta	58%	54%	49%	67%	76%
	Sporadycznie korzysta	37%	34%	35%	24%	21%
	Korzysta	5%	12%	16%	9%	3%
Ocena użyczania loginów	Naganne	27%	16%	14%	15%	40%
	Dopuszczalne w szczególnych przypadkach	67%	73%	84%	82%	41%
	Dopuszczalne	6%	11%	2%	3%	19%

Źródło: opracowanie własne.

Pożądane zachowanie, tzn. pracownik nie używa cudzych loginów i haseł, a użyczanie ich uważa za naganne, przejawia – poza organizacją E – mniej niż 20% respondentów. Można również wyodrębnić grupę, która zna zasady, ale ich nie stosuje (lp. 3, 4 z tabeli 3).

Tabela 3. Stosowanie zasad postępowania z loginami i hasłami

		Procent respondentów organizacji				
Lp.	Łączna odpowiedź na pytanie nr 11 i 12	A	B	C	D	E
1.	Nie używa, a użyczanie uważa za naganne	19,51	13,01	13,73	12,12	37,93
2.	Nie używa, a użyczanie uważa za dopuszczalne w szczególnych wypadkach	34,15	39,02	35,29	54,55	18,97
3.	Sporadycznie używa, a użyczanie uważa za naganne	4,07	1,63	0,00	0,00	1,72
4.	Używa, a użyczanie uważa za naganne	4,07	1,22	0,00	3,03	0,00

5.	Sporadycznie używa, a użyczanie uważa za dopuszczalne w szczególnych wypadkach	30,89	30,89	35,29	21,21	18,97
6.	Używa, a użyczanie uważa za dopuszczalne w szczególnych wypadkach	1,63	6,50	13,73	6,06	3,45
7.	Nie używa, a użyczanie uważa za dopuszczalne	3,25	3,25	0,00	0,00	18,97
8.	Używa sporadycznie, a użyczanie uważa za dopuszczalne	2,44	4,47	1,96	3,03	0,00

Źródło: opracowanie własne.

Sprawdzono, jak odnosi się deklarowana znajomość dokumentów związanych z bezpieczeństwem informacji do stosowania i znajomości zasad postępowania z loginami i hasłami. Przeprowadzone testy statystyczne nie wykazały zależności w organizacji E. W pozostałych jednostkach jest ona co najwyżej umiarkowana. Można wyciągnąć wniosek, że pracownicy kierują się raczej wygodą i wydajnością pracy niż przepisami.

Podsumowując wyniki próby wyłudzenia hasła do komputera, zastosowano bardziej obrazowy opis reakcji użytkowników na wiadomość otrzymaną od domniemanego Administrator Bezpieczeństwa Informacji. Pierwsza odpowiedź nastąpiła po upływie 14 minut i zawierała login i hasło. Jednak w miarę upływu czasu rozdzwoniły się telefony i w sumie odnośnie do tego tematu odebrano ich 23. W 22 przypadkach była to informacja o otrzymaniu listu, po której następowały różnego rodzaju pytania. Były one formułowane w następujący sposób:

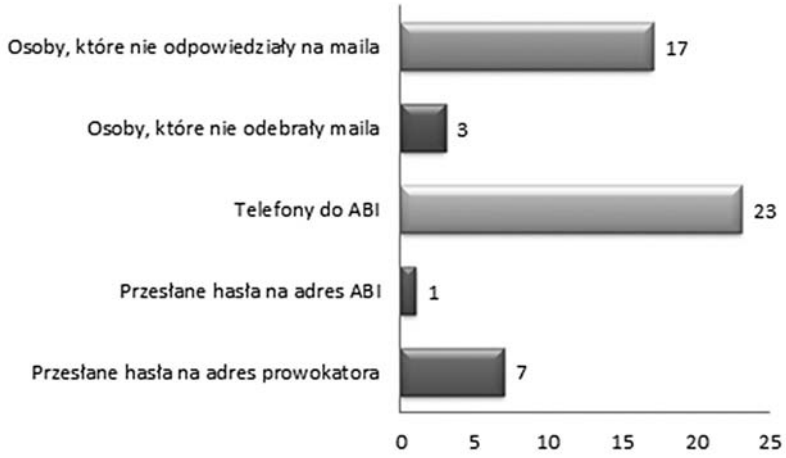
1. Dlaczego ABI żąda loginów i haseł skoro administratorzy nie potrzebują takich danych, bo mają dostęp do „wszystkiego”?
2. Dlaczego ABI żąda loginów i haseł, skoro hasło jest to ściśle prywatną sprawą?
3. Dlaczego ABI żąda loginów i haseł, jeżeli pracownicy IT zawsze podkreślają, że nie chcą znać naszych haseł?
4. Dlaczego ABI żąda loginów i haseł, skoro jest to niezgodne z dokumentem Polityka bezpieczeństwa?

Tylko jedna z poddanych testowi osób zgłosiła do Administratora Bezpieczeństwa Informacji problem dotyczący tego, że otrzymała list elektroniczny z fałszywego adresu. Dla równowagi kolejny z telefonów do ABI był informacją, że użytkownik nie chce podać hasła mailem, lecz jest gotowy podać je osobiście przez telefon. Podsumowanie badania przedstawione zostało na rysunku 2.

Osoby, które przesłały swoje loginy i hasła, to grupa pracowników biurowych. Swoich danych niezbędnych do zalogowania w systemie nie udostępniła ani jedna osoba będąca na stanowisku kierowniczym. Pomimo przeprowadzenia

rozmów uświadamiających z respondentami, którzy przesłali swoje loginy i hasła w liście elektronicznym, jedna z osób miesiąc później, a dokładnie 31 maja 2012 r., wysłała na fałszywą skrzynkę elektroniczną wiadomość służbową – niezwiązaną z badaniami – do ABI.

Badanie pozwoliło na wyciągnięcie wniosku, iż osoby biorące udział w badaniu czytają tylko treść otrzymanej wiadomości. Traktują podpis umieszczony pod wiadomością jako wystarczające uwiarygodnienie. Tylko jedna z 51 badanych osób potrafiła zweryfikować adres mailowy nadawcy.



Rysunek 2. Reakcje na próbę wyłudzenia hasła

Źródło: opracowanie własne.

Liczna grupa osób przyswoiła sobie propagowaną przez pracowników działu IT regułę, że pracownik IT nie ma potrzeby znać hasła do komputera. Częste powtarzanie tej informacji spowodowało jej trwałe zapisanie w świadomości niektórych użytkowników, dzięki czemu potrafili oni we właściwy sposób zareagować na próbę wyłudzenia hasła.

Zadziałał mechanizm obronny, którego autorzy niniejszego artykułu nie brali pod uwagę. Uczestnicy testu, którzy znajdowali się w obrębie jednego oddziału lub pokoju, konsultowali między sobą treść wiadomości. Wynikiem dyskusji były telefony do ABI z informacją o otrzymaniu wiadomości oraz prośby o ustne potwierdzenie polecenia. Sam fakt, że dział IT otrzymał bardzo szybko informację o próbie wyłudzenia loginów i haseł, w przypadku rzeczywistego ataku byłby bardzo pomocny w likwidacji jego skutków. Pozwoliłby na zabezpieczenie poszczególnych kont poprzez administracyjną zmianę haseł, powiadomienie

o ataku wszystkich użytkowników i inne akcje przeciwdziałające ewentualnym jego skutkom.

5. Podsumowanie i kierunki dalszych badań

Nasuwa się jasny wniosek, iż zagadnienia bezpieczeństwa informacji w badanych organizacjach, a prawdopodobnie także w innych jednostkach samorządu terytorialnego, traktowane są powierzchownie. Urzędnicy przedkładają komfort pracy oraz wydajność nad stosowanie bezpiecznych procedur eksploatacji systemu informatycznego. Należy bardziej szczegółowo przyjrzeć się organizacji pracy służb informatycznych, które mogą stać się największym zagrożeniem dla organizacji. Wskazane jest przeprowadzenie szerszych badań nad zabezpieczeniami systemu, które negatywnie wpływają na efektywność pracy.

Bibliografia

1. Barczak A., Sydoruk T., *Bezpieczeństwo systemów informatycznych zarządzania*, Bellona, Warszawa 2003.
2. Lowe-Norris A.G., Allen R., Desmond B., Richards J., *Windows 2000 Active Directory*, O'reilly Vlg. Gmbh & Co., 2008.
3. *Polska Norma PN-ISO/IEC 17799 Technika informatyczna. Techniki bezpieczeństwa. Praktyczne zasady zarządzania bezpieczeństwem informacji*, Polski Komitet Normalizacyjny, Warszawa 2007.
4. *Polska Norma PN-ISO/IEC 27001 Technika informatyczna. Techniki bezpieczeństwa. Systemy zarządzania bezpieczeństwem informacji. Wymagania*, Polski Komitet Normalizacyjny, Warszawa 2007.
5. Rozporządzeniu Rady Ministrów z dnia 11 października 2005 r. w sprawie minimalnych wymagań dla systemów teleinformatycznych (Dz.U. z dnia 28 października 2005 r.).
6. Rozporządzenie Rady Ministrów z dnia 12 kwietnia 2012 r. w sprawie Krajowych Ram Interoperacyjności, minimalnych wymagań dla rejestrów publicznych i wymiany informacji w postaci elektronicznej oraz minimalnych wymagań dla systemów teleinformatycznych (Dz.U. z 2012 r., poz. 526).
7. Żebrowski A., Kwiatkowski M., *Bezpieczeństwo informacji III Rzeczypospolitej*, Abrys, Kraków 2000.

Źródła sieciowe

1. http://media.krollontrack.pl/pr/166123/uzytkownicy-komputerow-z-calego-swiata-wskazali-jak-i-dlaczego-traca-dane [dostęp 13.09.2012].
2. http://oval.mitre.org/documents/docs-06/an_introduction_to_the_oval_language.pdf [dostęp 13.09.2012].
3. http://searchsecurity.techtarget.com/magazineContent/2010-Information-Security-magazine-Readers-Choice-Awards [dostęp 13.09.2012].
4. http://www.f-secure.com/weblog/archives/00002228.html [dostęp 13.09.2012].
5. http://www.gfi.com/network-security-vulnerability-scanner/network-auditing--software [dostęp 13.09.2012].

* * *

Security of information in local government units

Summary

This paper presents the results of safety information in the local government units. The study included case studies of 5 institutions. They used a survey, standardized interviews with security managers, penetration testing and vulnerability scanning internal networks.

Keywords: security of information, local government, penetration test, password protection, social engineering test