Teresa Mendyk-Krajewska, Zygmunt Mazur, Hanna Mazur

Wypływ danych wrażliwych z internetowych systemów bazodanowych w aspekcie bezpiecznego zarządzania wiedzą

Ekonomiczne Problemy Usług nr 68, 396-403

2011

ZESZYTY NAUKOWE UNIWERSYTETU SZCZECIŃSKIEGO

NR 651 EKONOMICZNE PROBLEMY USŁUG NR 68 2011

TERESA MENDYK-KRAJEWSKA, ZYGMUNT MAZUR, HANNA MAZUR
Politechnika Wrocławska

WYPŁYW DANYCH WRAŻLIWYCH Z INTERNETOWYCH SYSTEMÓW BAZODANOWYCH W ASPEKCIE BEZPIECZNEGO ZARZĄDZANIA WIEDZĄ

Wprowadzenie

Na rozwój usług w sieci Internet (bankowości elektronicznej, e-biznesu, pozyskiwania wiedzy itd.) ma wpływ polityka bezpieczeństwa prowadzona w organizacjach (firmach, instytucjach), w tym bezpieczne zarządzanie danymi. Realizacja usług sieciowych oparta jest na danych gromadzonych i przetwarzanych w bazach danych, a następnie przesyłanych w sieci rozległej. Oferta usług jest nieustannie poszerzana, także ich dostępność staje się coraz bardziej bezproblemowa, jednak prowadzenie wszelkiej działalności w sieci Internet nie jest całkowicie bezpieczne. Narastający problem zagrożeń bezpieczeństwa danych, w tym ich wypływ, dotyczy wykorzystywanych internetowych systemów bazodanowych.

Do najpowszechniejszych zagrożeń należą różnego rodzaju wirusy powodujące niekiedy bardzo poważne szkody (np. utratę danych), ataki blokujące usługi i ataki socjotechniczne, których skutkiem może być włamanie do systemu. W ostatnim okresie daje się zaobserwować niebezpieczne zjawisko wypływu danych z serwerów różnych organizacji, czego konsekwencją jest najczęściej kradzież tożsamości umożliwiająca przestępcze działania w sieci. Za wypływ (wyciek) danych uważa się celowe lub przypadkowe ujawnianie danych, które powinny być prawnie chronione, na przykład danych osobowych, wyników finansowych przedsiębiorstw, danych o stanie zdrowia czy dotyczących transakcji bankowych. Niestety, nie wszyscy użytkownicy usług sieciowych mają świadomość, że korzystanie z Internetu niesie wiele zagrożeń.

1. Bezpieczne zarządzanie wiedzą

Informacje, w których posiadaniu jest organizacja, stanowią jej ogromny i cenny majątek, dlatego potrzebne są systemy do odpowiedniego zarządzania wiedzą (danymi zgromadzonymi w systemach informatycznych oraz informacjami wynikającymi z doświadczeń i talentów pracowników). Zarządzanie wiedzą to ogół procesów umożliwiających tworzenie, upowszechnianie i wykorzystywanie wiedzy do realizacji celów organizacji.

Do koordynacji pracy w firmie oraz wykorzystywania i wytwarzania wiedzy (m.in. do operowania przechowywanymi danymi – ich aktualizacji, sortowania, prezentacji) wykorzystuje się system zarządzania wiedzą. Aby zapewnić jego właściwe działanie, musi on być monitorowany i weryfikowany (w celu wykrywania nieprawidłowości funkcjonowania, identyfikowania incydentów i naruszeń bezpieczeństwa, określania skuteczności) oraz modyfikowany (m.in. zgodnie ze zmianami i wynikami kontroli jego działania).

Duże znaczenie w bezpiecznym zarządzaniu wiedzą ma szybkie reagowanie na zachodzące zmiany. Wprowadzanie nowych technologii, form komunikacji czy nowych nośników danych wymusza dostosowanie systemu zarządzania wiedzą do nowych warunków. Z kolei nowe rozwiązania powodują pojawianie się nowych zagrożeń (np. dedykowanych szkodliwych kodów), co również wymusza konieczność szybkich reakcji.

W przypadku sieci komputerowych do zarządzania wiedzą służą systemy bazodanowe, które gromadząc i przetwarzając dane pozwalają na pozyskiwanie, analizowanie i wykorzystanie wiedzy w celu podejmowania możliwie optymalnych decyzji. Niestety, systemy teleinformatyczne narażone są na różnego rodzaju zagrożenia, których skutkiem może być przejęcie danych, ich modyfikacja, usunięcie lub uniemożliwienie niezawodnej pracy systemu. Następstwa tych działań są trudne do przewidzenia i często pociągają za sobą ogromne koszty. W ramach realizowanej polityki bezpieczeństwa każda organizacja musi przeprowadzić analizę ryzyka – określić rodzaj zagrożeń, prawdopodobieństwo ich wystąpienia oraz oszacować następstwa, w zależności od wartości zasobów (także danych). Celem tych czynności jest m.in. określenie poziomu akceptowalnego ryzyka oraz właściwy dobór zabezpieczeń.

W celu zapewnienia środków ochrony adekwatnych i proporcjonalnych do prowadzonej działalności oraz zasobów organizacji (firmy, instytucji), należy zaprojektować i wdrożyć system zarządzania bezpieczeństwem informacji (SZBI). Z polskiej normy PN-ISO/IEC 27001:2007 wynika, że każda organizacja powinna: *ustanowić, wdrożyć, eksploatować, monitorować, przeglądać, utrzymywać i stale*

doskonalić udokumentowany SZBI w kontekście prowadzonej przez nią działalności i ryzyka występującego w organizacji[1].

2. Podatność systemów na zagrożenia

Bazy danych zawsze stanowiły atrakcyjny cel ataków. Na bezpieczeństwo przechowywanych i przesyłanych danych istotnie wpływa jakość użytkowanego oprogramowania, a więc systemu operacyjnego, przeglądarki internetowej, systemu zarządzania bazą danych itd. Systemy oprogramowania są coraz bardziej złożone, stąd coraz więcej w nich błędów i trudności z testowaniem. Wady oprogramowania stwarzają możliwość podejmowania skutecznych ataków za pomocą specjalnych narzędzi (exploitów) i postrzegane są jako główna przyczyna zagrożeń bezpieczeństwa sieciowego. Użytkownicy o wykryciu luk są informowani na bieżąco, a rozwiązaniem problemu jest instalacja dostarczanych przez producentów nakładek systemowych (tzw. łat) lub nowych, poprawionych wersji oprogramowania. Zawsze jednak istnieje możliwość usunięcia nakładki, a nowa wersja też może okazać się wadliwa.

W celu określenia minimalnych wymagań dla tworzonego oprogramowania trzydzieści organizacji związanych z jego wytwarzaniem opracowało i opublikowało w 2009 roku listę najpoważniejszych błędów popełnianych przez programistów[2].

Przede wszystkim w starszych wersjach oprogramowania (niestety, nadal powszechnie używanych) znajdowane są liczne wady pozwalające na podjęcie ataku, czasem nawet na zdalne wykonanie szkodliwego kodu (jeśli mają znaczenie krytyczne). Wiele popularnych systemów zarządzania bazami danych, mimo stosowania w ich nowych wersjach coraz bardziej zaawansowanych mechanizmów ochrony, nadal nie jest pozbawionych błędów. Na przykład firma Oracle, która kładzie duży nacisk na bezpieczeństwo swoich produktów, na początku 2009 roku opublikowała 41 dalszych poprawek, choć rok wcześniej udostępniła ich aż 51 (w tym usuwające pięć luk krytycznych, znalezionych m.in. w Oracle Database, Oracle Application Serwer, Oracle E-Business Suite)[3]. Ten przykład pokazuje wyraźnie skalę problemu. Najbardziej narażony na ataki jest komponent Oracle Listener odpowiedzialny za komunikację pomiędzy klientem a serwerem oraz między serwerami. Jeśli nie jest on zabezpieczony hasłem (ustawienie domyślne) – istnieje możliwość uzyskania szeregu informacji na temat atakowanego systemu bazy danych za pomocą dostępnego w Internecie skryptu tnscmd.

---

[1] PN-ISO/IEC 27001:2007 *Technika informatyczna. Techniki bezpieczeństwa. Systemy zarządzania bezpieczeństwem informacji. Wymagania*, PKN, Warszawa 2007.

[2] *The 2009 CWE/SANS Top 25 Most Dangerous Programming Errors Common Weakness Enumeration Report*, cwe.mitre.org 2009.

[3] www.internetnews.com/security/article.php/3796076

Zagrożenia wynikają też z użytkowania programów napisanych w językach Java oraz JavaScript, w których modułach często wykrywane są wady.

Ponieważ wymaga się, by aplikacje internetowe zapewniały użytkownikowi komfort pracy, dostarczane są opcje ułatwiające wykonywanie różnych czynności, np. w formularzach przy wprowadzaniu danych możliwość dokonywania wyboru danych z przygotowanej listy lub korzystanie z podpowiedzi systemu. Niestety, rozwiązania takie mogą stwarzać niebezpieczeństwo pozyskania danych przez osoby do tego nieupoważnione.

W 2009 roku badania polskich witryn rządowych ujawniły dla 16 witryn aż 431 błędów, przy czym 73% z nich cechowało niski stopień zagrożenia, a 17% – bardzo wysoki. Główne zagrożenia to podatność na ataki XSS (*Cross Site Scripting* – infekowanie aplikacji sieciowej i przekazywanie dowolnego szkodliwego kodu użytkownikowi w chwili korzystania ze strony WWW) oraz SQL/XPath Injection (wykorzystuje podatność aplikacji na obsługę spreparowanych zapytań SQL – konsekwencją może być dostęp do bazy). Wiele badanych stron używało nieaktualnego oprogramowania (np. wersji protokołu SSL, modułu PHP, serwera Apache).

3. Ochrona danych w systemach informatycznych

Aby cele biznesowe organizacji realizowane z wykorzystaniem systemów informatycznych były osiągane niezawodnie, systemy muszą być chronione przed zagrożeniami. Jakość systemu bazy danych jest ściśle powiązana z bezpieczeństwem środowiska, w którym system jest eksploatowany. Wiele systemów bazodanowych (jak systemy bankowe, finansowe, medyczne, administracji państwowej) operuje na danych wrażliwych – poufnych, tajnych lub ściśle tajnych. Podstawowym zadaniem baz danych jest przechowywanie danych w usystematyzowany sposób. Aplikacje bazodanowe umożliwiają wykonywanie na zgromadzonych danych różnych operacji, sporządzanie raportów, statystyk i prezentowanie danych w czytelnej postaci. Zapewnienie danym wysokiego poziomu ochrony w celu zminimalizowania zagrożeń wymusza zastosowanie odpowiednich mechanizmów bezpieczeństwa, zapewniających m.in.: kontrolę dostępu do danych, tworzenie kopii zapasowych (z użyciem testów poprawności), archiwizację danych, uwierzytelnianie stron (nadawcy i odbiorcy), zabezpieczenie danych przed modyfikacją, zapewnienie poufności danym niejawnym, zapewnienie dostępności danych uprawnionym użytkownikom, zabezpieczenie przed nielegalnym kopiowaniem. Ponadto należy przestrzegać podstawowych zaleceń, do których zalicza się: systematyczną aktualizację systemu bazodanowego, nadawanie użytkownikom minimalnych uprawnień, uniemożliwianie dostępu za pomocą domyślnych nazw i haseł, stosowanie haseł o odpowiedniej złożoności, a także silnych mechanizmów uwierzytelniania, oraz przesyłanie i przechowywanie danych w postaci zaszyfrowanej (wymuszane przez

system). Problemem systemów zarządzania prawami do informacji (*Information Rights Management*) jest np. możliwość wykonania zrzutu zawartości ekranu lub jej sfotografowanie.

Systemy baz danych szczególnie chronionych powinny więc mieć wiele zabezpieczeń, takich jak: monitorowane pomieszczenia, nadzorowany dostęp do systemu, odnotowywanie operacji wykonywanych na danych, brak możliwości kopiowania danych na urządzenia przenośne, a nawet kserowania danych wydrukowanych. Zastosowane mechanizmy bezpieczeństwa powinny być jednak adekwatne do stopnia ważności danych i nie mogą wpływać negatywnie na jakość systemu, spowalniając jego pracę np. poprzez nadmierne kontrole czy zbyt częste wykonywanie kopii zapasowych.

4. Ataki na systemy baz danych – problem wycieku danych

Mimo stosowanych zabezpieczeń w ciągu ostatnich lat coraz częściej dochodzi do naruszenia bezpieczeństwa sieciowych systemów bazodanowych i kradzieży czy ujawnienia danych poufnych. Najczęściej przedmiotem kradzieży są dane osobowe, ale problem dotyczy też danych firmowych (informacji stanowiących o przewadze konkurencyjnej, np. technologii – tzw. szpiegostwo przemysłowe). Częstym celem ataków są serwery bankowe, a konsekwencją tych działań mogą być nieuprawnione przelewy, blokady dostępności danych lub wyciek danych. Przykładów jest wiele.

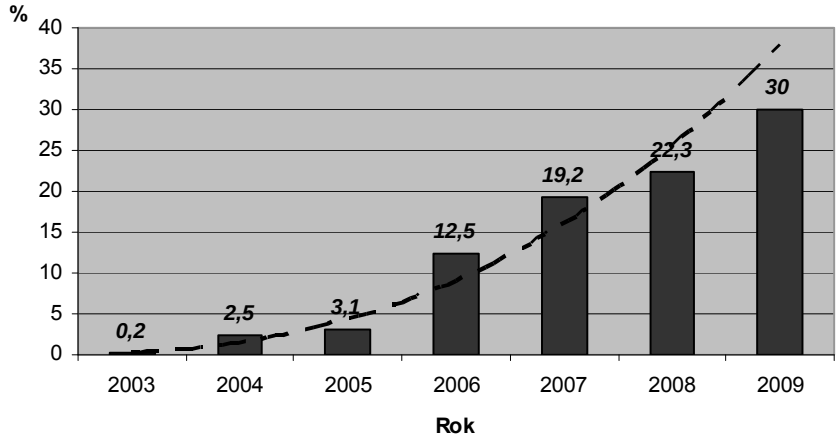
Znany jest przypadek wypływu danych z internetowego systemu rezerwacji biletów na Euro 2008 (po zalogowaniu widoczne były dane osób zapisanych do udziału w losowaniu, m.in. numery PESEL i dowodów osobistych). W 2007 r. wyciekły dane z holenderskich medycznych baz danych. W lipcu 2008 w internetowym systemie rekrutacji do pracy w Pekao SA upublicznione zostały listy motywacyjne i życiorysy kandydatów, gdyż pliki z danymi były umieszczone na serwerze w ogólnodostępnym katalogu. Z kolei przy użyciu koni trojańskich (np. TrojanPSW.Win32.Dybalom.aoo) w listopadzie 2009 r. przechwycono około 50 tys. nazw i haseł kont z serwisów społecznościowych (potem je opublikowano w Internecie).

Jak wynika z raportu firmy Kaspersky Lab *Globalne badanie wycieków danych 2006*, problem dotyczy głównie firm biznesowych. W 12% przypadków wypływ danych nastąpił przez Internet, w 50% – z powodu wykorzystywania przez pracowników urządzeń przenośnych, w 10% – w wyniku *outsourcingu*.

Firma Panda Security, tworząca systemy zabezpieczeń, opublikowała w marcu 2009 r. wyniki badań dotyczących kradzieży tożsamości. Analiza 67 mln komputerów wykazała, że 1,1% użytkowników Internetu było narażonych na działanie oprogramowania wykradającego dane osobowe, chociaż 35% zainfekowanych nim

komputerów posiadało aktywną ochronę antywirusową[4]. Trend tego niepokojącego zjawiska przedstawiono na rysunku 1.

Jak wynika z raportów *Computer Emergency Response Team Polska* (CERT), w większości przypadków zgłaszane ataki dotyczyły firm komercyjnych. Przyczyny tego upatruje się w coraz częstszym zaopatrywaniu się firm w komercyjne łącza internetowe z jednoczesnym brakiem odpowiedniego ich zabezpieczania. Z kolei około 25% atakujących nie zostało zidentyfikowanych z powodu ich ukrywania się za serwerami Proxy, wykorzystywania botnetów czy przejętych komputerów[5].



Rys. 1. Udział kradzieży tożsamości w incydentach w Polsce w latach 2003–2009

Źródło: opracowanie własne na podstawie raportów CERT Polska.

Raport firmy Trend Micro Incorporated z 2008 r. wskazuje, że choć utrata danych stanowi jedno z najpoważniejszych zagrożeń, to aż 46% badanych firm nie dysponowało żadnymi zasadami zapobiegania ich wypływowi. Problem jest w tym, że pracownicy powszechnie wykorzystują sieć firmową do działań niemających związku z wykonywanymi przez nich zadaniami (odbierają prywatne wiadomości e-mailowe, przeglądają strony internetowe, dokonują zakupów przez Internet, korzystają z serwisów społecznościowych, pobierają programy z niepewnych źródeł, transmitują pliki multimedialne), a także gubią służbowe laptopy i pendrivy[6]. Jeszcze innym problemem jest świadome działanie pracowników na szkodę macierzystej instytucji. Z badań przeprowadzonych przez firmę Cyber-Ark Software

[4] www.bestsecuritytips.com/news+article.storyid+763.htm

[5] *Raport 2009*, CERT Polska.

[6] egospodarka.pl/32129,Wyciek-danych-glownym-problemem-firm,1,39,1.html

w grupie pracowników biurowych w Nowym Jorku wynika, że 25% z nich byłoby zdecydowanych wykraść poufne informacje (dane klientów firmy, nazwy i hasła dostępu, informacje o produktach, plany itp.), przy czym aż 85% z nich zrobiłoby to, mając świadomość nielegalności takiego czynu. Najczęściej podawane powody decyzji kradzieży danych to zwolnienie przez pracodawcę, wiadomość o możliwości utraty pracy oraz możliwość wykorzystania danych do uzyskania nowej posady dla siebie lub osób bliskich. Około 60% ankietowanych stwierdziło, że kradzież danych nie byłaby szczególnie trudna[7]. Nie sposób nie wspomnieć tu o administratorach, którzy z racji pełnionych funkcji mają łatwy dostęp do chronionych danych, a rzadko są kontrolowani. Jak wynika z ankiety przeprowadzonej przez firmę Cyber-Ark Software w 2008 roku wśród pracowników działów IT dużych przedsiębiorstw, aż 47% z nich korzysta z dostępu do informacji niezwiązanych z wykonywanymi obowiązkami (połowa nie korzysta z żadnej dodatkowej autoryzacji), a co trzeci nadużywa uprawnień (przegląda listy płac, plany firmy, czyta prywatną korespondencję)[8].

Z wyciekiem danych kojarzy się też internetowa witryna WikiLeaks, działająca od końca 2006 roku, umożliwiająca anonimowe publikowanie rządowych i korporacyjnych dokumentów (poufnych, często tajnych) w celu wskazania działalności niezgodnej z prawem. W 2010 roku opublikowano tam setki tysięcy dokumentów dotyczących m.in. wojen toczonych w Afganistanie i w Iraku oraz depesz z amerykańskich placówek dyplomatycznych na całym świecie (w tym 970 dokumentów z Polski). Kolejny wyciek danych miał dotknąć największe banki USA, jednak w grudniu 2010 roku amerykański serwis płatności internetowej PayPal zablokował konta WikiLeaks z powodu naruszenia regulaminu.

Podsumowanie

Ochrona danych i usług w sieciach lokalnych oraz Internecie staje się coraz trudniejsza mimo stosowania odpowiednio dobranych systemów zabezpieczeń i przestrzegania przyjętych przez organizację zasad eksploatacji systemu. Handel danymi osobowymi jest intratny, coraz powszechniejszy i stanowi poważny problem. Bezpieczeństwo zasobów i usług sieciowych zależy od wielu czynników, nie tylko od jakości użytkowanego oprogramowania, właściwego zabezpieczania i administrowania danymi. Nie bez znaczenia są błędy ludzkie, dostępność narzędzi umożliwiających podjęcie ataku nawet osobie niedoświadczonej oraz brak dostatecznych zabezpieczeń przed nowymi typami ataków lub atakami skutecznie maskowanymi.

---

[7] Cyber-ark.com/news-events/pr_20091123.asp

[8] di.com.pl/news/21438,0,Co_trzeci_administrator_przeglada_poufne_dane.html

Najważniejsze dla firmy dane (a także ich kopie) powinny być przechowywane w postaci zaszyfrowanej na nośnikach zewnętrznych (trwałych i chronionych) lub na komputerze niepodłączonym do sieci, posiadającym ekranowane okablowanie, obudowę zabezpieczającą przed wyciekiem poprzez promieniowanie elektromagnetyczne i znajdującym się w pomieszczeniu o kontrolowanym dostępie. Rola wiedzy w gospodarce, biznesie i codziennym życiu stale rośnie, jednak przedsiębiorstwa dotąd nie wypracowały skutecznych mechanizmów zabezpieczających przed niekontrolowanym jej wypływem.

Literatura

1. PN-ISO/IEC 27001:2007 *Technika informatyczna. Techniki bezpieczeństwa. Systemy zarządzania bezpieczeństwem informacji. Wymagania*, PKN, Warszawa 2007.
2. *The 2009 CWE/SANS Top 25 Most Dangerous Programming Errors Common Weakness Enumeration Report*, cwe.mitre.org 2009.
3. *Raport 2009*, CERT Polska 2009.
4. Cyber-ark.com/news-events/pr_20091123.asp
5. di.com.pl/news/21438,0,Co_trzeci_administrator_przeglada_poufne_dane.html
6. di.com.pl/news/29584,0,Kolejny_wyciek_danych_w_polskim_internecie.html
7. egospodarka.pl/32129,Wyciek-danych-glownym-problemem-firm,1,39,1.html
8. www.bestsecuritytips.com/news+article.storyid+763.htm
9. www.internetnews.com/security/article.php/3796076

LEAK OF SENSITIVE DATA FROM INTERNET DATABASE SYSTEMS IN THE CONTEXT OF SECURE KNOWLEDGE MANAGEMENT

Summary

Data protection in Internet is becoming a more and more difficult task, in spite of applying relevant security systems. In this paper we discuss the issue of dangerous data leaking from corporate servers and, in consequence, identity theft for the purpose of carrying out criminal acts in the network.

Translated by Teresa Mendyk-Krajewska, Zygmunt Mazur, Hanna Mazur