

4

Podpis elektroniczny

Więcej ułatwień
dla urzędów i firm

Michał Dyszyński

7

Elektroniczne zamówienia publiczne

Czy to już rewolucja

Jacek Barwicki

10

Bezpieczna strona internetowa

Jak zapewnić bezawaryjne
działanie stron www urzędu

Michał Piszczek

13

E-administracja wciąż na papierze

Wnioski z kontroli NIK

Iwona Jeleń

15

E-mail z urzędu

Decyzje w skrynkach poczty
elektronicznej

Iwona Jeleń

15

Spis hoteli

Abonenci bazy
www.publiczni.pl/hotele

17

Spis firm szkoleniowych

Abonenci bazy
www.publiczni.pl/szkolenia



Szanowni Państwo!

Czy Kowalski może już swobodnie załatwiać sprawy w urzędach za pomocą swego nowoczesnego komputera? Po lekturze raportu Najwyższej Izby Kontroli odpowiedź na to pytanie nie pozostawia złudzeń. Tak, ale w ograniczonym zakresie, przynajmniej do czasu, aż tworzone w tym celu ogólnopolskie systemy teleinformatyczne rozpoczną bezawaryjne działanie. I niewielkim pocieszeniem jest fakt, że do końca 2009 r. rząd zamierza wydać 350 mln zł z funduszy europejskich na budowanie elektronicznej administracji.

Pocieszające są natomiast informacje, że wiele urzędów zabrało się samodzielnie za usługi w sieci tworząc coraz więcej elektronicznych udogodnień. Przy tym instytucje inwestują w ludzi – intensywnie ich szkoląc – i rozbudowują infrastrukturę teleinformatyczną.

Dlatego warto przeczytać, jakim ułatwieniem dla urzędów i firm jest stosowanie podpisu elektronicznego. Polecamy także artykuł dotyczący elektronicznych zamówień publicznych. O korzyściach z takiego rozwiązania przekonano się już po dwóch pierwszych miesiącach działania e-licytacji gdy okazało się, że firmy walczące o zamówienia publiczne w Internecie potrafią zejść nawet do jednej trzeciej początkowej ceny.

Zachęcamy również do lektury artykułu poświęconego bezpieczeństwu urzędowych stron internetowych, bowiem dbałość o jak najlepsze zabezpieczenie danych to dziś kwestia wiarygodności instytucji.

Iwona Jeleń
i.jelen@publiczni.pl

Poradnik Urzędnika • Pismo nowoczesnej administracji publicznej • NR 1/2009 (7)
REDAKCJA: Iwona Jeleń, i.jelen@publiczni.pl, tel. 022 487 83 76 • SKŁAD: Marek Wiśniewski
ISSN 1898-2549 • FOTOGRAFIA NA OKŁADCE: digitouch
DZIAŁ REKLAMY: Kornelia Jeleń, k.jelen@publiczni.pl, tel. 022 428 38 35

WYDAWCA: Publiczni.pl Sp. z o. o.,
ul. Rogalińska 1/40, 01-206 Warszawa,
tel./faks: 022 631 00 63
publiczni@publiczni.pl



publiczni.pl
SERWIS NOWOCZESNYCH URZĘDNIKÓW

Copyright by Publiczni.pl
Publikacja jest chroniona przepisami prawa autorskiego. Wykonanie kserokopii lub powielanie inną metodą oraz rozpowszechnianie bez zgody wydawcy w całości lub części jest zabronione i podlega odpowiedzialności karnej. Materiałów niezamówionych nie zwracamy, zachowując sobie prawo do skrótów i zmian tytułów. Nie ponosimy odpowiedzialności za treść reklam zamieszczonych na łamach.



Michał Piszczek

Bezpieczna strona internetowa

Jak zapewnić bezawaryjne działanie stron www urzędu

Bezpieczeństwo strony internetowej to obecnie kluczowa sprawa – z administracyjnej (gminnej, samorządowej, wojewódzkiej) witryny korzystają mieszkańcy danej gminy, turyści i dziennikarze, inwestorzy. Dlatego musi być ona spójna, aktualna i odpowiednio zabezpieczona.

Atak hakerów, niezależnie czy jest przypadkowy, czy celowy, zawsze może wywrzącić krzywdę w postaci podmiany zawartości strony, bądź usunięcia ważnych danych. Może to doprowadzić do ośmieszenia gminy bądź jej władarzy, pogorszenia jej wizerunku, a także późniejszego, żmudnego odtwarzania witryny. Z tego względu jednym z podstawowych elementów, o jakie należy zadbać podczas budowy i wdrażania strony internetowej,

jest bezpieczeństwo. Aby strona była rzeczywiście dobrze zabezpieczona, należy zwrócić uwagę na kilka aspektów – zarówno w zakresie technologicznym, jak i w zakresie tak często niedocenianego, czynnika ludzkiego.

Dostawcy

Pierwszym ważnym krokiem, rozpoczynającym proces zabezpieczenia przyszłej strony internetowej jest odpowiedni dobór

zaufanych dostawców. Niezależnie od tego czy w planach jest uruchomienie niewielkiego BIP-u, czy też rozbudowanego systemu zarządzania danymi, galeriami, dokumentami i aktualizacjami, to właśnie odpowiednio przygotowany kod może decydować o „skutecznych zaporach” lub „otwartych drzwiach”. Wybierając dostawcę warto sięgnąć po referencje wcześniejszych klientów, zapytać o przebieg wdrożeń oraz o współpracę po wdrożeniu. Szczególnie ten ostatni punkt ma duże znaczenie, ponieważ wsparcie w okresie użytkowania strony daje pewność stabilności i stałej dostępności witryny. Wzmacnia też poczucie bezpieczeństwa osób zarządzających stroną.

Jeżeli zamawiający dysponuje odpowiednim czasem i środkami, warto zwrócić się do zewnętrznego specjalisty ze zleceniem

zbadań jakości i poziomu bezpieczeństwa projektów już zrealizowanych przez potencjalnego dostawcę. Taki obiektywny audyt z pewnością będzie dużo bardziej wiarygodny od otrzymanej oferty handlowej.

Hosting

Kolejnym elementem istotnym dla zapewnienia bezpieczeństwa jest hosting. Wybierając dostawcę tego typu usług należy zwrócić uwagę nie tylko na cenę, ale przede wszystkim na to ile lat firma istnieje na rynku, jak często wykonywane są kopie zapasowe danych przechowywanych na serwerach (*backup*), a także jakie są procedury dostępu do tych kopii z naszej strony. Nie sprawdzając tego typu danych, klient naraża się na niebezpieczeństwo utraty części danych w przypadku awarii serwera (jeśli *backup* jest zbyt rzadko przeprowadzany) lub braku dostępu do kopii zapasowych w przypadku własnego błędu (jeśli firma hostingowa robi *backup* tylko na własne potrzeby). Warto dokładnie zapoznać się ze wszystkimi procedurami oraz czasem reakcji działu pomocy technicznej (*helpdesk*). Jeśli strona będzie zawierać „wrażliwe” informacje, przechowywane w intranecie, warto rozważyć hosting na własnym, dedykowanym serwerze.

Po wybraniu wykonawcy należy dokładnie zapoznać się z treścią umów (słusznym krokiem jest konsultacja z prawnikiem). Zwróćmy uwagę na kwestie odpowiedzialności za uaktualnienia systemu, oraz czas ich realizacji. Jest to szczególnie ważne, jeśli system w dużym stopniu opiera się o kod *Open Source*, w którym na bieżąco są odkrywane i publicznie pokazywane niedoskonałości. Tylko stały monitoring i udostępnianie odpowiednich „łatek” (najlepiej instalowanych automatycznie) pozwala na bezpieczne funkcjonowanie witryny opartej o taki kod.

Administratorzy

Często słyszymy stwierdzenie, że najsłabszym ogniwem bezpieczeństwa jest człowiek. Trudno się z tym nie zgodzić także w kontekście strony internetowej, a zwłaszcza samodzielnie administrowanych systemów CMS. Z tego względu jednym z najważniejszych etapów wdrożenia witryny jest szkolenie pracowników, którzy będą administrowali stroną, niezależnie od poziomu nadanych im później uprawnień. Ważna jest ich umiejętność obsługi sys-

temu, wiedza o formatowaniu wkładanych artykułów, umieszczaniu grafik.

Równocześnie to właśnie szkolenie powinno uświadomić pracownikom jak ważne jest odpowiednie przechowywanie haseł, wylogowywanie się z systemu po zakończonej pracy oraz niepodawanie nikomu danych dostępowych telefonicznie ani e-mailem.

Obok dbałości o odpowiedni dobór dostawców i przeszkolenie personelu, niezwykle ważne jest odpowiednie technologiczne zabezpieczenie samego systemu CMS. W przypadku systemu VelaCMS, jednego z najbezpieczniejszych na rynku (od pierwszego wdrożenia systemu u klienta, nigdy nie odkryto i nie opublikowano żadnych informacji o słabych elementach tego systemu, które pozwoliłyby na udany atak z zewnątrz), zastosowano tzw. kaskadowy system uprawnień, czyli określenie do jakich danych ma dostęp konkretny użytkownik. Dzięki temu najszerze możliwości administracyjne, pozwalające np. na usunięcie kategorii, czy uszkodzenie systemu, znajdują się w rękach bardzo wąskiej, odpowiednio

wyszkolonej grupy osób. Umieszczanie artykułów, czy zarządzanie grafikami można przekazać większej ilości pracowników, nie ponosząc niemal żadnego ryzyka.

Wyciek danych

Ważnym i skutecznym zabezpieczeniem jest również definiowanie adresów i klas adresów IP, z których dany użytkownik (lub wszyscy użytkownicy) mogą się logować do systemu. Dzięki temu, nawet w sytuacji, gdy któryś pracownik udostępni niepowołanej osobie swój login i hasło, to hacker nie będzie w stanie go wykorzystać. Dodatkowo, próbując wejść do systemu, pozostawi identyfikowalny ślad, dzięki czemu sprawny administrator będzie mógł odpowiednio zareagować:

- zmieniając feralny login i hasło,
- blokując IP, z którego nastąpił atak.

W przypadku wycieku danych (pojedynczego loginu i hasła), szybka reakcja w postaci blokady dostępu będzie skuteczna, o ile hasła są przechowywane w bezpiecz-

Akademia Humanistyczno-Ekonomiczna w Łodzi

WSHE 17001 M **Uczelnia z pasją**

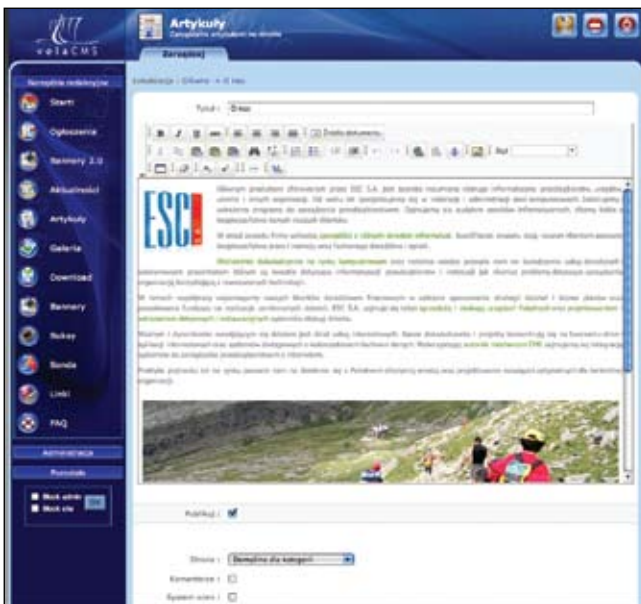
osiągnęła status Akademii

- Dziennikarstwo i komunikacja społeczna
- Realizacja obrazu filmowego, telewizyjnego i fotografia
- Kulturoznawstwo
- Filologia polska
- Pielęgniarstwo
- **Administracja**
- Pedagogika
- Zarządzanie
- Informatyka
- Politologia
- Transport
- Filologia
- Grafika

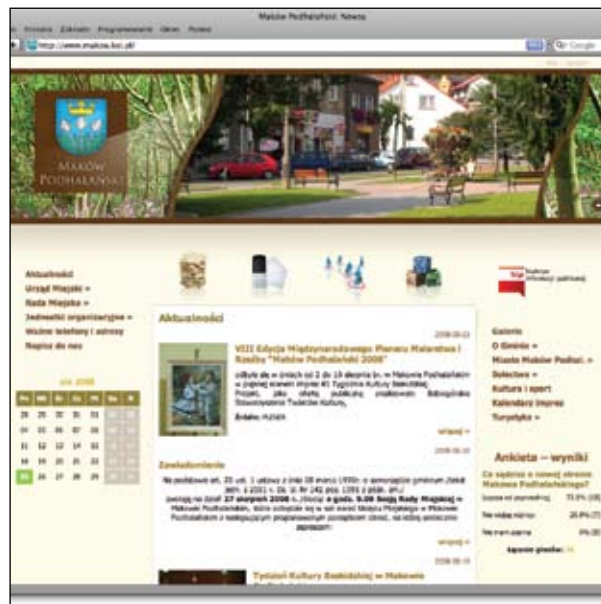


www.wshe.lodz.pl
infolinia: 0800 080 888

Akademia Humanistyczno-Ekonomiczna w Łodzi



Panel do zarządzania artykułami w systemie VelaCMS



Strona internetowa Makowa Podhalańskiego zarządzana w systemie VelaCMS

ny sposób, w postaci jednostronnych *hash* (MD5 i SHA1). Wówczas nawet bezpośredni dostęp do bazy danych nie pozwala na poznanie i użycie hasła. Natomiast jeżeli hasła są przechowywane w systemie w postaci otwartego tekstu, to blokada pojedynczej pary login-hasło jest przerwaniem ataku na krótką chwilę – hacker po kilku sekundach użyje następnej pary, którą uzyskał z bazy danych. Administratorowi pozostaje wówczas reset wszystkich par login-hasło i ponowne ustawienie ich. W przypadku wielu użytkowników to długi i żmudny proces.

Stały monitoring bezpieczeństwa systemu i prób ataku zapewnia logowanie wszystkich istotnych zdarzeń w systemie na wielu różnych warstwach:

- komponent „dziennik”, czyli logowanie działań użytkowników,
- logowanie dostępu na poziomie serwera www,
- logowanie prób włamań metodami *brute force*, fuzowania zmiennych przesyłanych metodami POST GET PUSH, itp.

Szeroki obraz, który otrzyma z tych danych administrator, pozwoli mu przede wszystkim na szybką i skuteczną reakcję uniemożliwiającą powodzenie ataku. Osoba zarządzająca stroną internetową będzie także w stanie na bieżąco monitorować działania użytkowników – zarówno te dozwolone, jak i te wykraczające poza nadane uprawnienia (np. wszelkie próby wejścia w niedozwolone komponenty).



Panel do zarządzania zdjęciami na stronie internetowej w systemie VelaCMS

Bezpieczeństwo rządowej strony internetowej zawsze było istotne, ale obecnie, w czasie niezwykle szybkiego przepływu informacji, ma szczególne znaczenie. Niezależnie od tego, czy na stronie internetowej są tylko krótkie informacje, opis urzędu i dane kontaktowe, czy też rozbudowane, często aktualizowane treści, atak jest zawsze negatywnie odbierany. Tym samym budowany latami wizerunek, może zostać mocno nadszarpnięty w ciągu kilku godzin przez niefrasobliwe podejście do

zabezpieczeń informatycznych i odpowiedniego poziomu wiedzy pracowników. ■

Michał Piszczek



Kierownik działu programistów ESC S.A. Odpowiada za zabezpieczenia systemu VelaCMS