Service Pack 2 wymusi zmiany podczas pisania kodu HTML

WWW w Oknach

Wkrótce pojawi się oficjalne wydanie uaktualnienia dla Windows XP. Zmiany, które tam wprowadzono, są ważne nie tylko dla użytkowników systemu Microsoftu, ale również dla każdego projektanta stron WWW.

Magdalena Pięta

Bezpieczeństwo jest w Sieci sprawą dużej wagi. Mimo to wielu użytkowników nie potrafi zapewnić go sobie w sposób dostateczny, choćby instalując i poprawnie konfigurując tzw. zaporę ogniową. Producenci oprogramowania próbują więc często robić to za nich. Zwiększanie bezpieczeństwa systemu operacyjnego (patrz: 20) i aplikacji na nim działających odbywa się najczęściej poprzez instalowanie uaktualnień i łatek na system, dostarczanych przez producenta. W przypadku systemów operacyjnych z rodziny Windows Microsoft regularnie wydaje tzw. Service Packi. Druga edycja tego uaktualnienia dla Windows XP zmienia domyślne ustawienia IE i OE na bardziej bezpieczne i wprowadza blokady tam, gdzie ich wcześniej nie było. Zawiera również kilka dodatków pozwalających w łatwy i szybki sposób zmodyfikować te opcje dla otwieranych w przeglądarce pojedynczych lub też wszystkich stron internetowych (czy wiadomości pocztowych HTML).

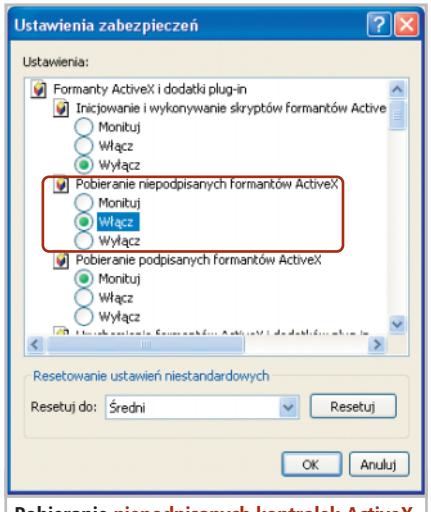
Kontrola nad ActiveX

Jeśli nasza witryna internetowa wykorzystuje kontrolki ActiveX, musimy pamiętać o tym, że Internet Explorer z SP2 może je zablokować. Stanie się tak, gdy zastosujemy w naszej witrynie odesłanie do innej strony, która będzie usiłowała wywołać kontrolkę ActiveX. Blokowany będzie także taki kod, którego rezultatem jest natychmiastowa instalacja tejże kontrolki. Uaktualnienie zainstalowanego w systemie komponentu ActiveX może odbyć się tylko wtedy, gdy spełnione są warunki:

- globalny unikatowy identyfikator (ang. globally unique identifier – GUID) jest taki sam jak GUID istniejącego kodu,
- uaktualniane i zainstalowane kontrolki są podpisane z użyciem Microsoft Authenticode z certyfikatem dostarczonym przez tego samego wystawcę i wydanym do tego samego obiektu.

Internet Explorer blokuje także instalację wszelkich kontrolek, które nie są podpisane. Sygnatury muszą być oczywiście aktualne i znajdować się w odpowiednich plikach CAB (CABinet file) lub DLL (Dynamic Link Library). Można jednak zezwolić na uruchamianie takich kontrolek, zmieniając ustawienia IE w menu **Narzędzia | Opcje internetowe**. Na karcie **Zabezpieczenia** wybieramy **Poziom niestandardowy** i ustawiamy **Pobieranie niepodpisanych formatów ActiveX** na **Włącz**.

Gdy użytkownik będzie chciał wydrukować stronę z kontrolkami ActiveX, które zostały zablokowane przez Windows XP z Service Packiem 2, to nie uda mu się to. Domyślne ustawienie mechanizmu Local Machine Zone Lockdown blokuje drukowanie takich stron, w podglądzie wydruku pojawia się jednak informacja, że została zablokowana kontrolka ActiveX. Jedyną możliwością wydrukowania tego rodzaju witryny jest wyłączenie przez użytkownika w Rejestrze **Local Machine Zone Lockdown**.



Pobieranie niepodpisanych kontrolek ActiveX to zagrożenie dla naszego komputera.

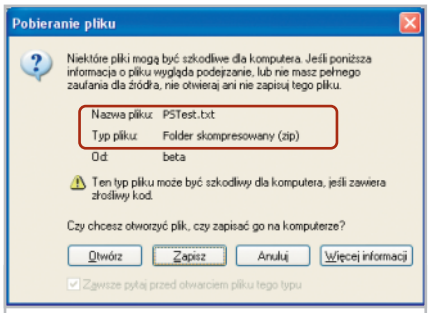
Podpisuj pliki

Jeśli odwiedzającym naszą witrynę internetową umożliwiamy pobieranie z niej plików, musimy zwracać uwagę na kilka detali. Pierwszy to kopiowanie zbiorów na komputer, zainicjowane przez kod na stronie WWW, bez udziału użytkownika. Zmiany w SP2 spowodują, że akcja taka zostanie domyślnie zablokowana. Dodatkowo pliki wykonywalne powinny być podpisane, ponieważ podczas downloadu sprawdzane są informacje dotyczące publikującego. Wyświetlane będą one użytkownikowi, który może w takiej sytuacji bardziej świadomie podjąć decyzję o ewentualnym pobraniu i uruchomieniu zbioru.

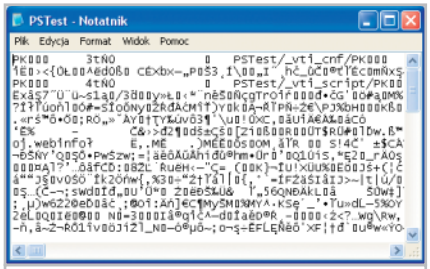
Druga sprawa, na którą należy zwrócić uwagę, to pliki, których typ nie odpowiada opisowi ich zawartości Content-Type (Typ pliku) i/lub rozszerzeniu. Takie niezgodności muszą zostać usunięte. Jeśli na przykład typ jednego ze zbiorów w witrynie będzie oznaczony plain/text, taki plik nie zostanie wyświetlony jako HTML.

Ostatnią kwestią, o której należy pamiętać, jest to, czy używamy obrazków w formularzach pobierania plików. Gdy wymagane jest kliknięcie stosownego przycisku, aby zainicjować download – grafikę komponentów należy uaktualnić (Download dialog UI) ręcznie w kodzie HTML.

Informacja o tym, że pobieranie pliku zostało zablokowane, pojawia się użytkownikowi na



Pobieranie plików, których rozszerzenie nie odpowiada ich rzeczywistemu typowi, będzie w SP2 zablokowane.



Pobrany plik z rozszerzeniem TXT jest w rzeczywistości w formacie ZIP. Otwarcie go w skojarzonej z typem tekstowym aplikacji może mieć trudne do przewidzenia skutki.

Zmiany w SP2

Największe zmiany w Service Packu 2 dla Windows XP dotyczą bezpieczeństwa wbudowanej w system przeglądarki Microsoftu, a tym samym korzystania z Internetu. Jeśli zatem chcemy, by nasza witryna internetowa była poprawnie wyświetlana na ekranach komputerów z Okienkami, musimy zapoznać się ze zmianami dotyczącymi:

- ➔ używania kontrolek ActiveX,
- ➔ udostępniania użytkownikom możliwości pobierania plików,
- ➔ otwierania okienek pop-up,
- ➔ ograniczania możliwości otwierania kolejnych okien przeglądarki.

Z punktu widzenia użytkownika najbardziej widoczną zmianą będzie chyba pojawienie się paska informacji o obiektach (ang. Information Bar). W zależności od tego, jakiego komponentu będzie on dotyczył, użytkownik będzie miał do dyspozycji menu pozwalające m.in. na zaakceptowanie, odrzucenie obiektu czy zmianę ustawień Internet Explorera.

Pasku informacji (Information Bar). Kliknięcie go spowoduje wyświetlenie menu, w którym mamy do wyboru dwie opcje:

Download Software
What's the Risk?

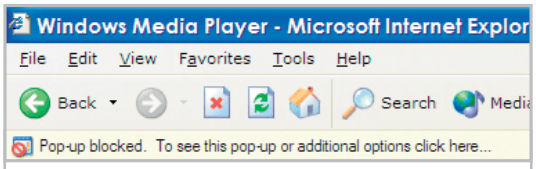
Pierwsza, jak łatwo się domyślić, umożliwi pobranie pliku, druga spowoduje wyświetlenie informacji dotyczących pochodzenia zbioru i związanego z tym ryzyka.

Niechciane okna

SP2 dla Windows XP sprawia, że blokowanie okienek pop-up jest domyślnie włączone. Pod Paskiem adresu przeglądarki IE pojawia się mały Pasek informacji (Information Bar), który poinformuje użytkownika, że okienko pop-up zostało zablokowane. Kliknięcie tego paska spowoduje otwarcie menu:

Show Last Pop-up
Allow Pop-ups for this Site
Allow Pop-ups
Show Information Bar for Blocked Pop-ups (Checked)
Pop-up Window Options...

Jeśli podczas tworzenia witryny internetowej, używamy metody **window.createPopup()**, musimy uwzględnić to, że SP2 dla Windows XP ogranicza jej wywołanie do jednego okienka na stronę. Internet Explorer będzie także usiłował zablokować automatyczne otwieranie okienek ze skryptu z wyjątkiem tych wykorzystujących metodę **createPopup()** i elementy DHTML, które zostają nałożone na zawartość strony.

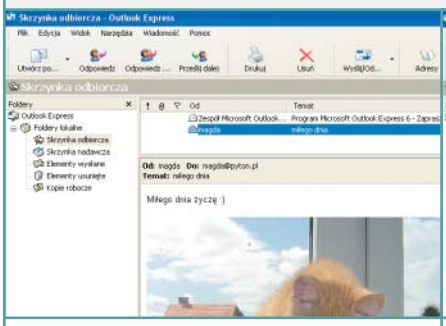


Internet Explorer, dostępny po zainstalowaniu Service Packa 2 dla Windows XP, domyślnie blokuje okienka pop-up.

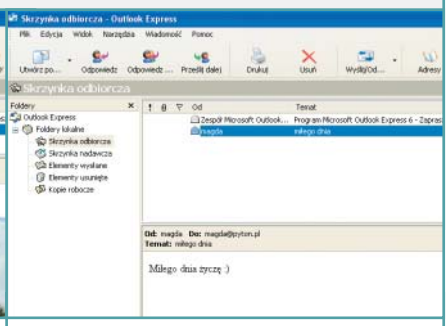
Dzięki Security Center użytkownik komputera z Windows XP SP2 może w jednym miejscu sprawdzić stan bezpieczeństwa systemu.

Service Pack 2 a Outlook Express

SP2 dla Windows XP wprowadza zmiany zwiększające bezpieczeństwo również w popularnym kliencie pocztowym, jakim jest Outlook Express. Program zapewnia teraz między innymi ochronę przed potencjalnie niebezpieczną zawartością plików otrzymywanych za pośrednictwem e-maila. Najczęściej w tych przesyłkach mamy do czynienia ze spamem pochodzącym od różnych firm, rozsyłanym w celach marketingowych. Wiadomości w formacie HTML zawierają często odnośniki do zbiorów graficznych umieszczonych gdzieś na serwerze w Sieci. Obrazki takie mogą czasami być wielkości jednego piksela, przez co są niewidoczne dla odbiorcy. Nie chodzi bowiem o to, żeby je ktokolwiek zobaczył. Dotychczas OE po otwarciu takiej wiadomości kontaktował się z serwerem i pobierał obrazek. Dla tego, kto wysłał taką wiadomość, jest to cenna informacja, że konto jest aktywne i ktoś z niego korzysta. Po zainstalowaniu SP2 OE, zamiast pobrać automatycznie plik, wyświetli na pasku informację o tym, że w wiadomości umieszczono odnośniki do danych znajdujących się na zewnętrznych serwerach.



Wiadomość ze zdjęciem pobieranym bezpośrednio z zewnętrznego serwera to zagrożenie dla naszej prywatności.



Wiadomość wyświetlona w trybie tekstowym – zdjęcie nie zostało pobrane, nie wysłano też żadnych danych do zewnętrznego serwera.

Jeśli chcemy, żeby użytkownik otrzymał informację o tym, że okienko zostało zablokowane, musimy sprawdzać wartość **window.open()**. Funkcja, która zwraca obiekt okienka, zwraca **null**, w przypadku gdy zostanie ono zablokowane. Sprawdzanie **window.open()** pozwoli uniknąć błędów skryptu, kiedy okienko nie będzie wyświetlone. Istnieją dwa sposoby rozwiązania problemu. Jeśli użytkownik korzysta z przeglądarki IE 5.0 (lub nowszej) z włączonym JavaScriptem, można użyć konstrukcji **try/catch**, w innym wypadku należy obsłużyć błąd w funkcji otwierającej okno.

Jeżeli nasza witryna uruchamia okienka poprzez inne obiekty (na przykład animacje Macromedia Flash), Internet Explorer także zablokuje możliwość otwarcia pop-upów. Niestety, musimy się z tym pogodzić, bo nie ma tu żadnej możliwości obejścia tego mechanizmu.

Oprócz tego nie należy używać metody **setTimeOut()** wewnątrz zdarzeń **click**, ponieważ okienko pop-up nie zostanie uruchomione. Nie powinno się też automatycznie zamykać wyskakującego okna, gdy zostało ono zablokowane przez nowego Internet Explorera. Użytkownik nie będzie mógł wtedy kliknąć Paska informacji (Information Bar) i zaakceptować obiektu (okienka, kontrolki, pliku itp.)

Poczta ekspresowa

Service Pack 2 dla Windows XP wprowadza też zmianę domyślnego trybu pracy klienta poczty – Outlooka Expressa (zarówno dla wiadomości otrzymywanych, jak i dla wysyłanych) z HTML-a na zwykły tekst (ang. plain text mode). Tryb HTML powoduje, że przesłane wiadomości są często efektowne graficznie, lecz mogą zawierać skrypty, które są wykonywane po otwarciu wiadomości. Jest to zagrożenie dla bezpieczeństwa użytkownika, gdyż takie skrypty są potencjalnym źródłem złośliwego kodu. Przełączenie OE w tryb tekstowy sprawi, że skrypty się nie wykonają. Ma to jednak pewne skutki uboczne, np. nie można formatować tekstu w tworzonej odpowiedzi takiej wiadomości. Przełączenie do trybu HTML jest jednak bardzo proste dzięki nowej opcji **Message in HTML** w menu **View**. Używanie tego ustawienia zaleca się jednak tylko wtedy, gdy wiadomo, że przesyłka pochodzi z zaufanego źródła.

Zaawansowanych użytkowników, którzy w wielu przypadkach sami umieją określić ryzyko związane z jakąś akcją, ochrona na siłę, jaką wprowadza Service Pack 2 dla Windows XP, może denerwować, ponieważ w wielu przypadkach nakłada na system zbyt duże ograniczenia. Przeciętny użytkownik komputera często nie zdaje sobie jednak sprawy z zagrożeń pochodzących z Internetu. Chroniony przez dostawcę swojego systemu operacyjnego czy innego oprogramowania może się czuć trochę bardziej bezpieczny. ■

Więcej informacji

Zmiany w Service Packu 2 dla Widows XP
http://www.microsoft.com/technet/prodtechnol/winxppro/maintain/sp2brows.mspx
http://www.microsoft.com/technet/prodtechnol/winxppro/maintain/sp2email.mspx