Bezpieczeństwo e-commerce

praca dyplomowa inżynierska

Bezpieczeństwo w dziedzinie handlu elektronicznego jest bardzo ważnym zagadnieniem, które często jest bagatelizowane i większość małych i średnich firm o nim zapomina lub nie traktuje go z należytą powagą. Osoby, które uważaj ą, iż skoro ich firma nie jest duża i nie ma popularnej strony, to już samo to stanowi wystarczającą ochronę – nic bardziej mylnego. To, czy firma posiada dwóch pracowników i jeden serwer internetowy czy jest to duży serwer w dużej firmie tak samo mogą stać się obiektem ataku. Anonimowość nie jest absolutnie żadnym zabezpieczeniem. Dla hakera jest najważniejsze to, iż włamie się do kolejnego systemu, a co za tym idzie – zdobędzie kolejne trofeum.

Uruchamiając serwis, w którym będziemy przechowywać dane o klientach jest jeszcze lepszym i ważniejszym powodem aby zabezpieczyć serwer. Niewątpliwie bardzo ważne jest zabezpieczenie systemu wspomagające pracę agencji reklamowych, gdyż oprócz danych klientów na kradzież lub zniszczenie narażone są również prace, które zostały wykonane dla kontrahentów. Często są to rzeczy oryginalne i nietuzinkowe, a ich utrata mogłaby wiązać się z poważnymi konsekwencjami.

Oczywiście najbezpieczniejszy komputer to taki, który nie ma użytkowników i nie jest podłączony do Siecie. Ponieważ taki komputer nie znajduje praktycznego wykorzystania w większości zastosowań, trzeba na coś pozwolić: komputer w przypadku serwisu on-line potrzebuje administratora i musi być podłączony do sieci.

Dobrym rozwiązaniem jest udostępnienie możliwości przesyłanie plików poprzez serwer FTP[1]. Jest niewiele możliwości na zawieszenie serwera mając do niego dostęp tylko poprzez FTP.

Nie ma wglądu do innych danych niż tylko te udostępnione. Usługa FTP może być tak skonfigurowana, aby możliwe było wyłącznie zapisanie, ale pliki nie będą mogły zostać odczytane, co znacznie ogranicza możliwość manipulacji danymi.

Takie metody oczywiście pomagaj ą ustrzec się przed włamaniem do systemu, jednak nie są one absolutnie pewne. Jest przy tego rodzaju rozwiązaniach kilka problemów, które niestety nie mogą być rozwiązane tak długo, jak komputer jest podłączony do sieci. Zalecane jest zatem skorzystanie z rozwiązania typu „firewall”. Przy korzystaniu z tego typu rozwiązań istnieje jednak niebezpieczeństwo, iż będą one na tyle kosztowne, iż inwestycja może być ekonomicznie nieopłacalna. Koszty wdrożenia i utrzymywania takiego rozwiązania zaczynaj ą się od zera i nie mają górnej granicy. Wszystko zależy od tego, jakie decyzje zostaną podjęte przy wdrożeniu zabezpieczeń. Czy wybór padnie na doradztwo eksperta z dziedziny bezpieczeństwa czy będą to profesjonalne zabezpieczenia, które wdroży i nadzór nad nim będzie sprawował specjalizujący się w tym usługodawca czy też firma chce kupić gotowy produkt lub usługę lub czy chce sama zbudować swoje rozwiązanie typu firewall. Aby wybrać najlepsze rozwiązanie należy poradzić się eksperta lub posiadać szczegółową wiedzę odnośnie bezpieczeństwa i protokołów.

Najczęściej jednak w przypadku małych i średnich firm korzysta się z gotowych, niedrogich rozwiązań w postaci aplikacji, którą konfiguruje się na serwerze, routera z funkcjonalnością firewall lub osobnego urządzenia firewall.

Istnieją dwa różne rodzaje firewall: serwer pośredniczący (ang. proxy) i filtr pakietowy. Najczęściej stosuje się oba rozwiązania jednocześnie, gdyż tak jest po prostu bezpieczniej.

Serwer proxy jest komputerem, który chroni granicę pomiędzy zewnętrznym Internetem, a wewnętrzną siecią lokalną. Serwer pośredniczący sam nawiązuje wszystkie połączenia z siecią

zewnętrzną i wyłącznie poprzez niego dochodzi do kontaktu z zewnątrz.

W tym momencie bezpieczeństwo jest związane z tym serwerem, gdyż tylko on narażony jest na atak hakera. Oczywiście pokonanie serwera proxy oznacza wolny dostęp do sieci lokalnej.

Z powyższego powodu stosuje się filtry pakietowe. Filtrację zapewnia komputer, który analizuje ruch wszystkich pakietów danych, ażeby upewnić się, że są one dozwolone w sieci lokalnej.

Bardzo dobrym zabezpieczeniem jest tzw. „honeypot”. Jest to pułapka składająca się z „komputera, danych i wyodrębnionego obszaru sieci lokalnej które udają prawdziwą sieć, lecz są odizolowane i odpowiednio zabezpieczone. Wszystko to z zewnątrz wygląda jakby zawierało informacje lub zasób który mógłby być potencjalnym celem cyberprzestępcy.

---

[1] FTP – File Transfer Protocool – protokół umożliwiający przesyłanie danych (teksty, dane audio-wideo, obrazy) z tzw. serwera FTP do własnego komputera poprzez Internet bądź w kierunku odwrotnym.

XSL

praca dyplomowa inżynierska

Język XSL (Extensible Stylesheet Language) stanowi uzupełnienie XML. W założeniu ma on służyć do formatowania dokumentów w XML (podobnie jak CSS dla HTML). Może być on również używany do przekształcania dokumentów XML na dokumenty HTML. XSL nie tylko umożliwia definiowanie wyglądu, ale także selekcj ę, dokonywanie operacji oraz sortowanie danych. XSL definiuje szablon końcowy oraz określa w jaki sposób elementy źródłowe mają być przekształcone i w jaki sposób umieszczone w dokumencie HTML. Aktualnie ogólnodostępne przeglądarki nie potrafią interpretować opisu formatowania wyrażonego w XSL. Za to doskonale radzą sobie z prezentacją dokumentów HTML. Zatem dokumenty XSL przetwarzane zostają do postaci HTML.

Wg najnowszego podziału, wyróżnia się cztery części języka:

- XSLT (XSL Transformations) – zawiera zestaw instrukcji umożliwiających przekształcenie dokumentu XML'owego w nowy dokument,
- XPATH – zawiera język do adresowania części dokumentu XML.
- XSL (Extensible Stylesheet Language) – dawny XSL-FO, słownik opisujący formatowanie,
- XQuery (XML Query Language) – język zapytań.

> *„Prezentacja dokumentu z użyciem XSL polega na transformacji drzewa hierarchii znaczników dokumentu wejściowego na drzewo tzw. formatting objects, którym przypisano określone sposoby prezentacji. Przeglądarka służąca do prezentacji powinna zrozumieć język owych obiektów formatujących."*[18]

Proces transformacji dokumentu:

1. parsowanie oryginalnego dokumentu XML’owego,
2. parsowanie dokumentu XSLT – poprawny dokument XML’a, zawiera opis transformacji jaką należy wykonać na oryginalnym dokumencie XML’a,
3. utworzenie wynikowego dokumentu XML, który zawiera znaczniki z XMLF,
4. interpretacja znaczników opisujących sposób formatowania i prezentacji dokumentów.

Dla XSLT istnieje wiele implementacji kompilatorów, które pozwalają na praktyczne skorzystanie z możliwości jakie oferuje XML+XSLT. Transformacje opisywane przez XSLT są zapisywane jako poprawny dokument XML, który może zawierać zarówno elementy należące do specyfikacji języka XSL, jak i elementy użytkownika. Transformacja wyrażona w XSLT zawiera zbiór reguł opisujących przekształcenie jednego drzewa XML w nowe. Reguły te wyrażane są przy pomocy wzorców, które składają się z części pozwalającej na sprawdzenie czy dana reguła powinna zostać zastosowana do bieżącego elementu drzewa XML i z zawartości wzorca czyli tego co ma się pojawić w wynikowym drzewie po napotkaniu pasującego elementu drzewa. Elementy dokumentu XML są kolejno dopasowywane do wzorców i w ten sposób, poruszając się w głąb źródłowego drzewa, tworzone jest drzewo dokumentu wynikowego.

XSLFO jest skomplikowanym językiem o dużych możliwościach, zawierającym ponad 50 różnych „obiektów formatujących”. Obiekty te można formatować wykorzystując ponad 200 różnych właściwości, takich jak: kroje, odmiany i wielkości pisma, odstępy, kolory itp.

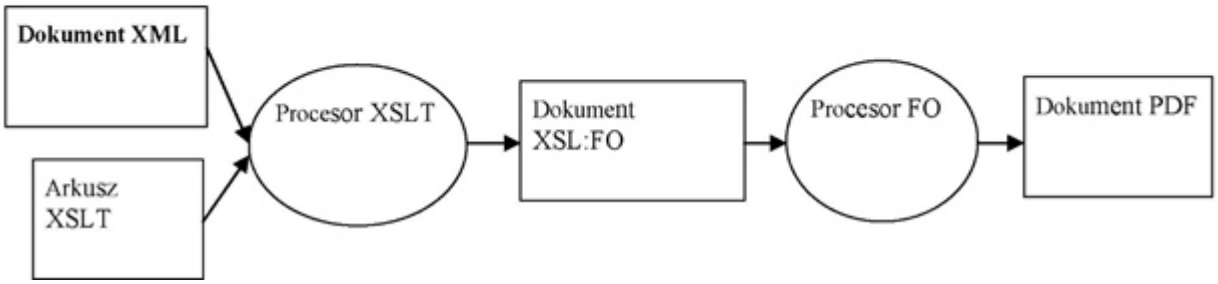
W dokumencie XSLFO elementy i atrybuty nie opisują struktury dokumentu, a wyłącznie jego postać graficzną. Różni go to od arkuszy stylów CSS, w których polecenia formatujące są (zwykle) oddzielone od dokumentu, którego dotyczą. XSLFO pod tym względem przypomina raczej tradycyjne systemy przetwarzania tekstu takie jak TeX. Dokument XSLFO winien być generowany automatycznie na podstawie danych zapisanych w

innym formacie (np. „strukturalnego” dokumentu XML lub informacji z relacyjnej bazy danych), a po wykorzystaniu usunięty. Format XSLFO nie jest przeznaczony ani do przechowywania informacji, ani do jej wymiany.

W typowym scenariuszu dokument XSLFO jest tworzony za pomocą odpowiedniego arkusza stylu XSLT. W poniższym przykładowym fragmencie arkusza XSLT element para wyjściowego dokumentu jest transformowany do elementu fo:block:

Rysunek 11. Typowy scenariusz przetwarzania dokumentu XSLFO

```
<template match="para">
 <fo:block space-after.optimum="0pt" hyphenate="true" >
<xsl:apply-templates/> </fo:block>
</xsl:template>
```



Cały dokument XSLFO zawarty jest wewnątrz elementufo:root, który składa się z:

- jeden elementfo:layout-master-set zawierający szablony określające wygląd poszczególnych stron oraz sekwencji stron,
- zero lub więcej elementów fo:declarations,
- jeden lub więcej elementówfo:page-sequance zawierających treść formatowanego dokumentu wraz z opisem jego sformatowania i podziału na strony.

Treść formatowanego dokumentu znajduje się wyłącznie wewnątrz elementów fo:page-sequence, podczas gdy elementfo:layout-master-set zawiera definicje szablonów.

[18] „JęzykXSL”, Tomasz Traczyk, IAilS, Politechnika Warszawska, ia.pw.edu.pl/~ttraczyk/pdf/ploug2000_art.pdf