Zajištění bezpečného provozu systému WebLIS

M. Novotný

Tento článek má za cíl posloužit jako vodítko pro bezpečnou instalaci trojvrstvé ASP aplikace WebLIS zajišťující webový přístup do systému OpenLIMS firmy Stapro s.r.o. založeného na technologiích firmy Microsoft (ASP.NET, MS Internet Information Server, MS SQL). Předpokládáme, že uživatel bude využívat webový přístup jak z lokální sítě tak z Internetu.

1. Bezpečnostní rizika

Jádrem informačního systému OpenLIMS je databáze obsahující výsledky laboratorních vyšetření spojené s jednoznačnými identifikačními údaji konkrétních fyzických osob. Z pohledu Zákona 101/2000 Sb. o ochraně osobních údajů ve znění pozdějších předpisů se tedy jedná o citlivé osobní údaje, jež je nutno zpracovávat v souladu s ustanoveními tohoto zákona, a jejichž porušením se zpracovatel (zdrav. zařízení) ocitá v nebezpečí uvalení finančních sankcí či dokonce trestního postihu fyzických osob. Zejména je dle ustanovení §13 nutno "… přijmout taková opatření, aby nemohlo dojít k neoprávněnému nebo nahodilému přístupu k osobním údajům, k jejich změně, zničení či ztrátě, neoprávněným přenosům, k jejich jinému neoprávněnému zpracování, jakož i k jinému zneužití osobních údajů. Tato povinnost platí i po ukončení zpracování osobních údajů."

I přes všeobecnou známost výše zmíněného zákona stále dochází k deliktnímu jednání a nutnosti sankcionovat i zdravotnická zařízení (viz např. seminare.idg.cz/seminare.nsf/www/security-invex-2008-loga/$File/02_UOOU.ppt). Kromě sankcí je samozřejmě v sázce i pověst a klientela příslušného zařízení.

Webový přístup je dnes běžnou technologií pro přístup uživatele k celé řadě, ne-li většině existujících informačních systémů. Přesto nebo snad právě proto bývá tato technologie často jedním z nejslabších článků systému. Co konkrétně hrozí?

a) Infiltrace webového prohlížeče nebo operačního systému přídavným modulem typu trojský kůň, který je schopen zachytávat a rozkrýt útočníkovi autentizační dialog ještě dříve, než dojde k jeho zašifrování vrstvou SSL. Jde o aktivní útok modifikací výpočetního prostředí klienta, jež může být umožněn předchozí infiltrací např. pomocí SPAM zprávy.

b) Možnost dešifrování zašifrovaného HTTP provozu mezi webovým prohlížečem a ASP aplikací na základě útoku „man-in-the-middle". Jde o pasivní útok podmíněný předchozím přesměrováním URL nebo HTTPS provozu na útočnický systém. Tento útok je veden na výpočetní prostředí klienta.

c) Napadení vlastního webového serveru na úrovni http pomocí útoku typu „buffer overflow" a získání možnosti umístit na server a spustit nežádoucí kód umožňující další infiltraci webového serveru. Jde o aktivní útok na webový server.

d) Modifikace webových stránek a jejich infiltrace nežádoucím kódem typu spyware nebo trojský kůň útokem typu „cross-site scripting", jež si následně legální uživatelé systému WebLIS mohou zanést do svých klientských operačních systémů. Jde o aktivní kombinovaný útok na server i na výpočetní prostředí klienta.

Zvláště tento a minulý rok prokázal, že útoky na soukromí a krádež elektronické identity osob je vedena přes webové prohlížeče, jejichž bezpečné použití není vždy v silách jejich uživatelů.

2. Základní bezpečnostní pravidla pro webový server

- **Server, na němž poběží IIS musí být logicky a komunikačně oddělen od serveru, na němž je provozována databáze OpenLIMS.**

  Díky vysoké zranitelnosti MS IIS je třeba provést řadu konfiguračních opatření jak na vlastním webovém serveru IIS, tak na OS MS Windows. Ta by mohla kolidovat s požadavky aplikace OpenLIMS. V případě zdařilého útoku na IIS nejsou přímo ohrožena data aplikace OpenLIMS. Požadavek na logické oddělení umožňuje provoz IIS na virtuálním stroji. Fyzické oddělení na samostatném HW serveru je samozřejmě též možné.

- **IIS musí být vystaven do Internetu přes stavový firewall a musí být provozován v demilitarizované zóně.**

  Toto opatření umožňuje eliminovat DoS útoky a poskytuje řiditelnou komunikační bezpečnost mezi IIS a databázovým serverem OpenLIMS.

- **Komunikace klienta s IIS musí být zabezpečena protokolem SSL/TLS.**

  Toto je standardní požadavek na zajištění autenticity a důvěrnosti komunikačního toku přes síť Internet. V tomto ohledu nečiníme rozdíl mezi komunikací ve vnitřní síti a komunikací přes

Internet. Microsoft IIS umožňuje zabezpečit komunikaci mezi www serverem a klientským prohlížečem pomocí protokolu SSL. Je proto nutné vygenerovat žádost o vydání certifikátu, tu poslat certifikační autoritě (CA). Vygenerovaný certifikát naimportovat na server, nastavit port pro použití SSL na serveru (v případě, že je standardní port 443 již použit) a nainstalovat do www prohlížečů kořenový certifikát dané CA (pouze v případě, že ho prohlížeče nemají nainstalován). Doporučujeme využít pro tento účel komerční (popř. i akreditovanou) CA, jejíž provoz je v souladu s RFC popř. ETSI standardy. V ČR může jít např. o I.CA, Českou poštu, eIdentity a.j.

3. Bezpečné nastavení IIS

1) Nainstalovat a pravidelně spouštět MBSA (Microsoft Base Line Security Analyzer) – stahovat nové opravy OS a jeho komponent.
2) Aktivní IIS Lockdown, nakonfigurovaný URLscan.
3) Deaktivace nepotřebných služeb (SMTP, FTP, Telnet, WebDAV apod.)
4) Konfigurace MS firewallu na serveru z hlediska příchozí komunikace pouze pro PING a HTTPS.
5) Bezpečné nastavení uživatelských účtů (smazat zbytečné lokální účty, účet uživatele Administrator přejmenovat a zvolit silné heslo).
6) Odebrána práva vzdáleného přihlášení k OS pro skupinu „Everyone".
7) Zakázán anonymní přístup.
8) Obsah webových stránek ASP aplikace je umístěn na nesystémovém NTFS svazku.
9) Přístupová práva k systémovému svazku a kořenu webového serveru jsou u skupiny „Everyone" odebrána.
10) Zakázáno MS sdílení adresářů s výjimkou systémových sdílení.

4. Nastavení prohlížeče (stanice)

Na stanici (v prohlížeči) nutno mít importován kořenový certifikát příslušné CA (viz výše) a v okně URL zadat místo http https popř. za odkazem dvojtečku a port (pokud byl změněn z 443). Např.: https://www.domena.cz:888 se připojí pomocí šifrovaného protokolu https na port 888 www serveru v doméně domena.cz. Bezpečné používání prohlížeče pro účely aplikace WebLIS zahrnuje minimálně:

1) Průběžnou instalaci bezpečnostních oprav prohlížeče.
2) Zachovávat rezervovanost vůči webovým stránkám a portálům pochybného či nemorálního obsahu, neboť ty jsou s velikou pravděpodobností (a úspěšností) zdrojem webové infiltrace.
3) Nastavení automatické kontroly validity serverových certifikátů předávaných v rámci navazování HTTPS spojení vč. vysvětlujícího upozornění pro uživatele v případě nesrovnalostí.
4) Zapnut mechanismus kontroly validity webových míst (Phishing filter) a kontrolu přesměrování formuláře s vloženými údaji na jiné webové místo.
5) Zapnuto upozornění uživatele při pokusu o instalaci rozšíření (plug-in) webového prohlížeče.
6) Zapnuto upozornění při pokusu o spuštění aktivního obsahu webové stránky.
7) Automaticky blokovat spouštění aktivního obsahu, u něhož nebyl rozpoznán platný digitální podpis.
8) Mít na klientském OS aktivní a aktualizovaný kvalitní (certifikovaný) antivirový prostředek schopný kontroly HTML kódu.
9) Využívat systém kvalitní antispamové ochrany resp. nikdy neklikat na odkaz v e-mail zprávě, u níž si nemůže příjemce být jist (z kontextu) jejím autorem.
10) V případě nejistoty ohledně chování webového prohlížeče požádat kompetentní osobu o poučení.

Závěrem bych rád uvedl, že zajištění reálné informační bezpečnosti v prostředí sítě internet a aplikací založených na webovém přístupu je alespoň z 80 % (z pohledu množství zranitelností) závislé na bezpečném chování uživatelů, zbytek úkolu pak leží na technologickém a organizačním zabezpečení serverové strany. Proto je velmi důležité informovat uživatele a správce systémů o možných rizicích provozu takové aplikace a apelovat na zodpovědné chování včetně sebevzdělávání v oblasti používání soudobých prostředků IT.