Zvýšení bezpečnosti webhostingu

Ing. Petr Benedikt
Západočeská univerzita v Plzni
Centrum informatizace a výpočetní techniky
e-mail: ben@civ.zcu.cz

5. března 2013

Abstrakt

Předkládaný projekt se zabývá zvýšením bezpečnosti webhostingových serverů na Západočeské univerzitě v Plzni. Webhosting je nejexponovanější službou v organizaci, přes kterou bývá aktuálně vedeno největší množství útoků. Aktuální stav, který byl adekvátní situaci před několika lety, je již z hlediska bezpečnosti nedostačující. Cílem projektu je zajistit izolaci webhostingových projektů tak, aby zranitelnost jednoho nemohla ohrozit provoz ostatních služeb.

Projekt je zařazen do oblasti I, tématického okruhu A, písmeno c) (podporu nových postupů na odhalování, řešení a **prevenci bezpečnostních incidentů**, podporu bezpečnostních týmů CERT/CSIRT a budování jejich zázemí, sledování a vyhodnocování provozu sítě a služeb, a zapojení uživatele do budování bezpečnosti provozovaných sítí a služeb).

1 Současný stav řešeného problému

Západočeská univerzita v Plzni v současné době provozuje několik webhostingových serverů hostujících více než 400 webových projektů. Tato aktuálně provozovaná koncepce vznikla před více než 10 lety, kdy nároky na webhostingový server byly jiné než nyní.

V době vzniku webhostingových serverů se předpokládalo, že k webovým projektům bude přistupovat webmaster znalý použitých technologií a dokáže je bezpečně provozovat a udržovat. Postupem času s příchodem různých redakčních systémů se však okruh uživatelů webhostingových služeb rozšířil a začali vznikat různorodé webové projekty provozované na těchto redakčních systémech. Jejich správci často nemají příliš velkou znalost použitých programovacích metod, pouze dokaží provést instalaci a úpravu obsahu webu dle návodu a často opomenou bezpečnostní hledisko. Tímto způsobem se zvyšuje riziko bezpečnostních problémů, např. ponechání výchozího hesla do administrativní části redakčního systému, nevhodně nastavená přístupová práva k souborovému systému, neaktuálnost redakčního systému. Tyto a mnoho dalších příčin mohou vést ke kompromitaci

dat a v některých případech i celého webhostingu. V posledních měsících jsme také zaznamenali několik bezpečnostních incidentů na některých webových projektech a v jednom případě tento útok způsobil nedostupnost celého serveru. To znamenalo několika hodinový výpadek na těchto službách.

Webhosting je vysoce exponovaná služba, která často bývá terčem útoků, proto je nutné změnit stávající nedostatečný stav, který byl přiměřený situaci před několika lety.

2 Cíle řešení

Cílem projektu je nalezení vhodného řešení pro izolaci jednotlivých webhostingových projektů. Izolaci je potřeba provést z dvou různých hledisek - zajistit jak izolací výkonovou, tzn., že problém jednoho webhostingového projektu neohrozí stabilitu ostatních provozovaných služeb, tak i izolaci datového úložiště před možnou kompromitací dat ostatních projektů.

Dalším možným krokem je omezení konfiguračních možností jednotlivých webových projektů, které by vedlo k prevenci proti možným pochybením na straně správce webů.

3 Způsob řešení

V rámci projektu se prověří možností nástrojů pro izolaci programového vybavení. Z tohoto hlediska je potřeba nahlížet na problém ze dvou stran. Webové projekty bude potřeba izolovat jeden od druhého, aby nedocházelo ke kompromitaci dat ostatních projektů, a zároveň izolovat samotné projekty od systémových prostředků, aby nemohlo dojít k přetížení stroje, pokud bude ohrožen jeden z mnoha webových projektů. V rámci řešení bude provedena analýza možných aktuálních hrozeb a případné nastavení kanálu pro sledování vývoje těchto zranitelností.

Základní předpoklad bude využití volně šiřitelného software, proto oblast zkoumaných možností se bude orientovat na prostředky dostupné pro operační systém Linux.

Pro zvýšení bezpečnosti webového serveru je potřeba na problém nahlédnout z globálního hlediska. V podstatě se jedná o server s operačním systémem Linux a s aplikací Apache, která zajišťuje zprostředkování webového obsahu uživatelům. Abychom mohli řešit bezpečnost serveru, je potřeba nejprve rozumně zabezpečit operační systém a následně se zabývat zabezpečením na úrovni aplikace Apache. V rámci projektu absolvuje hlavní řešitel školení SEC506: Securing Linux/Unix od společnosti SANS, které je zaměřeno na komplexní zabezpečení celého stroje s OS Linux/Unix. Část školení se samozřejmě také zabývá zabezpečením webového serveru Apache.

Dalším úkolem bude provést analýzu dostupných virtualizačních metod, které jsou vhodné pro provoz webového serveru. Mezi uvažované metody virtualizace (či kontejnerování) patří např. chroot, LXC, OpenVZ apod.

Po provedení analýzy dostupných metod zvolíme nejvhodnější prostředky, které budou vhodné pro nasazení v prostředí organizace. Zvolené prostředky budeme následně prakticky

testovat na testovacím zařízení.

Po instalaci prostředí provedeme nasazení několika prázdných webových projektů, obsahující některé známé zranitelnosti, na nich pak provedeme vybrané testy popsané v bezpečnostní příručce vydané nadací OWASP, která se zabývá zranitelnostmi a prevencí zranitelností webových aplikací.

Na základě provedených testů různých konfigurací webového serveru zvolíme vhodnou konfiguraci, kterou aplikujeme do ostrého provozu a začneme rekonfigurovat stavající webhostingové servery na nové řešení.

4 Prezentace výsledků

Odborné materiály, získané poznatky, použitá řešení a výsledky související s řešením projektu budou zájemcům dostupné v elektronické formě prostřednictvím webových stránek CIV, ZČU v Plzni.

Výsledky analýzy, testování prostředků pro izolaci prostředí webhostingových projektů a prostředků zvolených při implementaci budeme prezentovat v rámci semináře pořádaného CIV při ZČU v Plzni a také na semináři CESNET pro správce systémů.

Výsledky tedy mohou být k užitku všem členům sdružení.

5 Charakteristika řešitelského týmu

Ing. Petr Benedikt (hlavní řešitel)

je absolventem Fakulty elektrotechnické Západočeské univerzity v Plzni v oboru Sdělovací a zabezpečovací technika. V letech 2010 - 2012 pracoval při studiích jako člen týmu HELPS - technická podpora pro zaměstnance při CIV, ZČU. Od roku 2012 pracuje v oddělení Internet a síťové služby Laboratoře počítačových systémů při CIV, ZČU jako správce systému.

E-mail: ben@civ.zcu.cz, tel.: +420 377 632 870.

Ing. Michal Švamberg (spoluřešitel)

je absolventem Fakulty Aplikovaných věd Západočeské univerzity v Plzni v oboru Distribuované systémy. Od roku 2002 pracuje v Laboratoři počítačových systémů (LPS) Centra informatizace a výpočetní techniky (CIV), kde se účastnil návrhu a budování kolejních sítí Západočeské univerzity. Dále se zabývá správou operačního systému Linux a jeho integrací do distribuovaného výpočetního prostředí `Orion`. Spravuje také FibreChannel infrastrukturu, distribuovaný souborový systém AFS a XEN virtuální stroje. Na ZČU působí jako instruktor v certifikačních programech CCNA a CCNP[1]. Pro CESNET z.s.p.o. se podílí

[1] Jedná se o kurzy z Cisco Networking Academy Program, více viz `http://www.netacad.cz/`.

na správě výpočetních clusterů jako řešitel výzkumného záměru – projekt MetaCentrum národní gridové a superpočítačové infrastruktury.

E-mail: svamberg@civ.zcu.cz, tel.: +420 377 632 833.

6 Navrhovaná doba trvání projektu

Navrhovaná doba řešení projektu je 12 měsíců.

7 Finanční rozvaha

Pro projekt jsou požadovány náklady na testovací server, prostředky pro absolvování školení SEC506: Securing Linux/Unix od společnosti SANS a náklady na mzdy pracovníků.

Předpokládaná cena testovacího serveru je 75 000,- Kč bez DPH, tj. 90 750,- Kč s DPH. Cena testovacího serveru byla stanovena na základě již proběhlých výběrových řízení s ohledem na požadované potřeby tohoto projektu. Koncová konfigurace vzejde z výběrového řízení pořádaného ZČU. Server a náklady spojené s jeho pořízením bude hrazeno z finančních zdrojů řešitelské organizace.

Cena školení SEC506 je stanovena na 3 412€ a poplatek za certifikaci v rámci kurzu je 499€. Při uvažovaném kurzu měny 1€ = 25,4 Kč ke dni 20.2.2013 je cena školení odhadována na 86 665,- Kč a náklady na certifikaci 12 675,- Kč. Tato cena zahrnuje pouze poplatky za absolvování školení, nejsou zde zahrnuty náklady spojené s dopravou, ubytováním a stravného. Náklady s tímto spojené byly stanoveny na 32 789,- Kč, tj. 6 500,- Kč na dopravu, 18 288,- Kč na ubytování, při uvažované ceně 720€ za 6 nocí v hotelovém pokoji v místě konání, a 8 001,- Kč na stravné, určené z hodnoty 45€ na stravné na den a délce konání školení 7 dní. Cena školení bude hrazena z fondu rozvoje, náklady na certifikaci a ubytování/dopravu/stravné budou hrazeny řešitelskou organizací.

Ve finančních prostředcích projektu jsou také zahrnuty příspěvky na mzdy řešitelů. Částka 75 000,- Kč na mzdy (včetně sociálního a zdravotního pojištění) odpovídá 30 člověkodní práce, které budou využity na instalaci HW, instalaci a testování vybraného programového vybavení, programátorské úpravy a testování bezpečnosti instalovaného řešení. Z uvedené částky je 55 556,- Kč vyhrazeno na mzdy a 19 444,- Kč na sociální a zdravotní pojištění. Prostředky na mzdy budou hrazeny z fondu rozvoje.

Režie, tj. 15% z celkové části neinvestičních zdrojů bude hrazeno z fondu rozvoje.

Celková částka na pokrytí nákladů spojených s řešením projektu byla stanovena podle propozic uvedených v tabulce 1. Míra spoluúčasti ve financování řešitelskou organizací je 37,80%.

Případné vícenáklady spojené s řešením projektu jdou na vrub řešitelské organizace.

Položka	**cena**	**hradí**	**CESNET**	**ZČU**
Server	75 000,- Kč	ZČU		75 000,- Kč
Mzdy	75 000,- Kč	CESNET	75 000,- Kč	
Školení SEC506	86 665,- Kč	CESNET	86 665,- Kč	
Certifikát GCUX	12 675,- Kč	ZČU		12 675,- Kč
Výlohy na školení	32 789,- Kč	ZČU		32 789,- Kč
Režie 15%	36 552,- Kč	CESNET	36 552,- Kč	
Celkem			198 217,- Kč	120 464,- Kč

Tabulka 1: Náklady spojené s řešením projektu