Zvýšení bezpečnosti webhostingu

Závěrečná zpráva projektu 475/2013 Fondu rozvoje CESNET

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

19. února 2015

Závěrečná zpráva projektu Fondu rozvoje CESNET, z. s. p. o. pro rok 2013 vedeného pod číslem 475/2013. 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 Struktura dokumentu

Struktura tohoto dokumentu je v souladu s podklady pro závěrečné oponentní řízení Fondu rozvoje CESNET, z. s. p. o. rozčleněna následujícím způsobem.

- Způsob řešení
- Dosažené cíle
- Zdůvodnění změn v projektu
- Konkrétní výstupy
- Přínosy projektu
- Tisková zpráva
- Výkaz hospodaření s prostředky poskytnutými projektu z fondu

2 Způsob řešení

V rámci projektu se řešitel zůčastnil školení SANS SEC506: Securing Linux/Unix, které pomohlo rozšířit povědomí o potřebách pro zabezpečení linuxových serverů. Na základě těchto znalostí byly prozkoumány konfigurační možnosti linuxového serveru pro potřeby webhostingu. Z rozpočtu projektu byl pořízen server, na kterém byl zprovozněn operační systém Debian, a na něm bylo otestováno zvolené řešení.

3 Dosažené cíle

Díky školení SANS SEC506: Securing Linux/Unix prohloubil řešitel své znalosti v oblasti bezpečnosti linuxových strojů a získal certifikát GCUX (GIAC

Certified Unix Security Administrator). Tyto znalosti aplikoval při přípravě nové konfigurace webhostingového serveru.

Z důvodu vhodného napojení na ostatní systémy provozované v rámci infrastruktury ZČU v Plzni bylo vyžadováno zachování přístupu k distribuovanému souborovému systému AFS a podpora autentizace prostřednictvím systému WebAuth ze Stanfordské univerzity.

Hlavní body provedené v rámci řešení projektu lze shrnout do následujících bodů:

- Minimalizace operačního systému Debian
- Změna způsobu přístupu k distribuovanému souborovému systému AFS
- Kontrola zápisových práv do souborového systému a omezení spouštění skriptů z těchto míst
- Izolace jednotlivých webových projektů provozovaných na serveru
- Automatizace instalace bezpečnostních záplat použitého software
- Trvalé vynucení provozu zabezpečeným protokolem HTTPS
- Napojení na centrální logovací infrastrukturu
- Sledování zpráv týkající se bezpečnosti linuxových serverů

3.1 Minimalizace operačního systému Debian

Bylo využito stávajícího systému FAI pro instalaci opearčního systému Debian, které plně dostačuje požadavkům na bezpečnost připravovaného systému, a nebylo nutné do základní instalaci dělat další zásahy.

3.2 Změna způsobu přístupu k distribuovanému souborovému systému AFS

Pro přístup k AFS je využíváno systému Kerberos. Původní řešení spočívalo v namapování celé větvě souborového systému na serveru na základě IP adresy stroje. Toto řešení bylo nedostatečné, zde proto došlo ke změně.

Aktuálně má každý webový projekt generovánu vlastní Kerberos identitu, prostřednictvím které může přistupovat na souborový systém. Pro nastavení identity jednotlivým webům je nutné využít modulu *mod_waklog*.[1]

[1] http://www.modwaklog.org/

3.3 Kontrola zápisových práv do souborového systému a omezení spouštění skriptů z těchto míst

Webové projekty, které mají možnost vkládání souborů do souborového systému a nemají dostatečně ošetřené vstupy, mohou být zranitelné. Útočník může do složky nahrát skript se škodlivým kódem a z daného umístění jej pustit. Tomuto se snažíme zabránit vypnutím podpory PHP v těchto složkách. Pro tyto účely jsme připravili skript, který prohledává složky webových projektů na AFS a v případě nalezení zápisových práv ve složce zakáže spouštění skriptů v jazyce PHP.

3.4 Izolace jednotlivých webových projektů provozovaných na serveru

Pro izolaci jednotlivých webů jsme využili forkování instance webového serveru Apache. Tato možnost je dostupná jako součást instalace Apache. Pomocí skriptu */usr/share/doc/apache2.2-common/examples/setup-instance* je možné vytvářet nové instance programu Apache. Následně je také vhodné vytvořit vlastní úživatelský účet v systému Linux, pod kterým bude instance spuštěna. Tím se docílí izolace přístupu ke Kerberos identitě uložené lokálně na serveru.

Forkováním instancí Apache je nutné také vyřešit přístup k těmto webům, jelikož na serveru nemůže současně běžet více programů na stejném portu, tedy na portu 80 resp. 443. Z toho důvodu je nutné jednotlivé instance provozovat na odlišných portech a na základních portech je provozována hlavní instance Apache, která má funkci proxy serveru, který zprostředkuje přístup k lokálním portům.

3.5 Automatizace instalace bezpečnostních záplat použitého software

Tato změna se týká způsobu instalace bezpečnostních balíčků a je spíše volitelná, protože instalace nových balíků může mít vliv na provoz samotného webu.

Uvažovány byly nástroje pro automatickou instalaci balíků i nástroje pro pravidelné sledování změn instalovaných balíků s upozorněním v případě, že bude k dispozici aktualizace.

3.6 Trvalé vynucení provozu zabezpečeným protokolem HTTPS

Jeden z aspektů bezpečnosti webových projektů spočívá také v zajištění bezpečnosti dat při přenosu mezi serverem a uživatelem. Z toho důvodu jsme také zavedli politiku využití pouze HTTPS přenosu. S tím jsou také spojeny změny v podpoře šifrovacích metod. V návaznosti na nedávné zprávy o zranitelnosti v šifrovacím protokolu SSL tzv. Poodle útokem jsme přestali podporovat SSLv3 a primárně využíváme TLSv1.

3.7 Napojení na centrální logovací infrastrukturu

Infrastruktura pro centrální logování je na ZČU již vybudovánu. Nový server byl do této infrastruktury zapojen. Podrobnosti tohoto připojení nejsou obsahem této práce.

3.8 Sledování zpráv týkající se bezpečnosti linuxových serverů

Pro zvýšení povědomí o aktuálních bezpečnostních hrozbách využívají správci webhostingových serverů na ZČU několik zdrojů.

Hlavní zdrojem informací je bezpečnostní skupina na oddělení CIV, která upozorňuje pracovníky ZČU použitím interních kanálů na možná bezpečnostní rizika.

Dále správci sledují zprávy z mailing listů distribuce Debian a odebírají zprávy z newsletteru SANS Newsbites.

4 Zdůvodnění změn v projektu

V průběhu řešení byla schválena změna v rozpočtu z důvodu zrušení původně plánovaného školení od firmy SANS. Školení bylo následně absolvováno prostřednictvím e-learningového kurzu, nebyly proto nutné výdaje za zahraniční cestovné. Tím bylo nutné přehodnotit stávající stav rozpočtu, aby byly splněny požadavky na finanční spoluúčast.

Dále bylo schváleno prodloužení projektu z původních 12 měsíců na 18 měsíců. O prodloužení bylo žádáno kvůli zdržení výběrového řízení pro nákup serverů, které znemožnilo včasné testování řešení.

5 Konkrétní výstupy

Výsledky projektu jsou využívány ve výpočetním prostředí Západočeské univerzity. Projekt umožnil získat poznatky vedoucí ke zlepšení provozovaných služeb webhostingových serverů.

Technická dokumentace s podrobným popisem změn je k dispozici na webových stránkách řešitelské organizace na adrese [1]. V technické dokumentaci jsou popsány provedené změny a přiloženy ukázky z konfiguračních souborů. Kompletní balík konfiguračních souborů bude zájemcům z řad členů sdružení CESNET k dispozici na vyžádání.

Popis nového řešení bude prezentován pro zaměstance a lokální správce na ZČU v rámci semináře CIV pořádaného v březnu 2015. Informace o pořádané akci a materiály k semináři budou dostupné na adrese [2].

6 Přínosy projektu

Projekt přispěl ke zlepšení bezpečnosti webhostingových serverů. V rámci projektu byl také zakoupen nový stroj, který bude sloužit pro poskytování webhostingových služeb.

7 Tisková zpráva

Díky finanční podpoře Fondu rozvoje sdružení CESNET, z. s. p. o. byla upravena koncepce webhostingových serverů na ZČU v Plzni. Projekt umožnil získat nové poznatky v bezpečnosti webových serverů a tyto poznatky aplikovat a připravit konfigurační změny pro zvýšení bezpečnosti webhostingových serverů.

8 Výkaz hospodaření

Na projektu se podílely dva subjekty, a to Fond rozvoje CESNET a ZČU. Z prostředků fondu rozvoje bylo hrazeno plánovaných 94 tisíc za školení a certifikaci SANS. Z prostředků fondu rozvoje se ještě očekává vyplacení 75 tisíc na odměny řešitelům, které budou vyplaceny po obhájení projektu. Západočeská univerzita v Plzni hradila jako spoluúčast nositele dlouhodobý hmotný majetek v podobě serveru v celkové hodnotě 88 tisíc a režijní náklady ve výši 30 tisíc. Celkové náklady na školení a certifikaci SANS převýšili předpokládanou hodnotu o 18 tisíc a cena stroje převýšila předpokládanou

cenu o 13 tisíc. Tuto částku zaplatil nositel a v závěrečné rekapitulaci není započtena do jeho spoluúčasti.

Položka	**cena**	**hrazeno z**
1x server	88 000,- Kč	ZČU
školení a certifikát SANS	94 000,- Kč	CESNET
odměny řešitelům	75 000,- Kč	CESNET
režie a cestovné	30 163,- Kč	ZČU
Celkem	274 163,- Kč	

Tabulka 1: Náklady spojené s řešením projektu

Celkové náklady Fondu rozvoje CESNET byly 169 000,- Kč a náklady na straně ZČU byly 105 163,- Kč. Spoluúčast ZČU na projektu byla 38,4%.

Odkazy

[1] Stránka s elektronickými zdroji projektu
`http://support.zcu.cz/index.php/LPS:Webhosting`
[2] Seminář CIV
`http://seminar.civ.zcu.cz`

V Plzni dne 19. února 2015

Ing. Petr BENEDIKT
hlavní řešitel projektu