



## **BEZPEČNOSTNÍ AUDIT SERVERU BETA (VÝSLEDNÝ PROTOKOL)**

**pro společnost SIMPLE SAMPLE s.r.o.**

**zpracoval:**  
LOGIOS s.r.o.

V Podhájí 776/30, 400 01 Ústí nad Labem

web: <http://www.logios.cz/>

e-mail: [info@logios.cz](mailto:info@logios.cz)

datum: 31.1.2006

## 1. ÚVOD

### OBJEDNATEL

Objednatel auditu byla společnost SIMPLE SAMPLE s.r.o. Kontaktní osobou za objednatele byl Josef Stuchlík, manažer IT.

### AUDITOR

Auditorem byla společnost LOGIOS s.r.o.

### CÍL AUDITU

Cílem auditu bylo posoudit výkon a bezpečnost serveru BETA a prověřit procesy jeho správy a obnovy po havárii. V případě nalezení nedostatků bylo druhým cílem navrhnout opatření k odstranění závad.

### ROZSAH AUDITU

Audit se týkal serveru BETA s IP adresou 10.0.0.1, připojeného do vnitřní sítě v objektu firmy SIMPLE SAMPLE s.r.o. v pražské pobočce.

## 2. POPIS SYSTÉMU

Server BETA používá operační systém Linux, distribuce Red Hat Enterprise Linux ES verze 3.

Server funguje jako webový systém nasazený uvnitř firmy pro specializovanou CRM databázi vyvinutou třetí stranou a další intranetové aplikace. Rovněž se stará o zpracování elektronické pošty. Aktivně jej využívá cca 20-30 zaměstnanců společnosti.

Systém je firmou považován za středně důležitý.

Instalaci prováděla firma SIMPLE SAMPLE vlastními silami, instalace proběhla před cca 2 lety.

Systém používá neznačkový hardware mimo platnou dobu záruky.

Správce systému je Jaroslav Novák.

### 3. BEZPEČNOSTNÍ ZRANITELNOSTI

Audit identifikoval následující bezpečnostní zranitelnosti:

míra rizika	zranitelnost	vysvětlení a doporučená opatření
velmi vysoké	Snadno odhalitelná hesla uživatelů	U 28 uživatelů z celkových 33 se podařilo uhodnout hesla (84% celkového počtu). Test trval cca 20 sekund.  <b>Doporučení:</b> 1) ihned změnit hesla všech uživatelů 2) zavést a technicky vynucovat pravidla pro tvorbu kvalitních hesel  (V plné verzi dokumentu další doporučení ke tvorbě hesel a popis metod kontroly hesel pro pravidelný self-assessment)
...	...	...
vysoké	Chybí RAID pole	Server využívá jediný harddisk. Vzhledem k tomu, že chyba harddisku je patří mezi nejčastější hardwarová selhání, je provoz serveru na jediném harddisku velkým rizikem.  <b>Doporučení:</b> (v plné verzi dokumentu vysvětlení RAID polí a postup, jak server migrovat na RAID systém)
...	...	...
střední	Přihlášení na root účet přes SSH	Na server se lze přihlásit na účet root vzdáleně přes Internet. Povolené přihlášení na root přes SSH přináší minimálně dvě zranitelnosti: <ul style="list-style-type: none"> <li>• Umožňuje automatizovaným programům hádat hesla podle slovníku (velmi častý útok, na veřejně přístupných serverech někdy až několikrát do týdne!).</li> <li>• Podporuje špatné návyky rutinní práce s účtem administrátora i na úkolech, které privilegia správce nepotřebují.</li> </ul> <b>Doporučení:</b> (v plné verzi dokumentu postup, konfigurační soubory a další doporučení)
...	...	...
nízké	Chybné rozdělení disku	Systém je instalován na jediném diskovém oddílu („partition“). Zaplnění disku daty (vč. například auditních záznamů, tzv. „logů“) povede k pádu celého systému.  <b>Doporučení:</b> (v plné verzi dokumentu doporučení pro rozdělení disků a postup pro migraci)
...	...	...
velmi nízké	Chybí předem připravené CD pro obnovu systému	Odpovědné osoby nemají k dispozici CD s užitečnými programy pro případ výpadků. V případě problémů se serverem nebude možné se operativně pokusit obnovit provoz. Záchranné CD lze sice stáhnout z Internetu, ale dochází tím k časovým prodlevám a v případě výpadku internetového spojení nemusí být download vůbec funkční.  <b>Doporučení:</b> (v plné verzi dokumentu odkaz na vhodné nástroje).
...	...	...

## 4. VÝKONOVÁ ZLEPŠENÍ

Navrhujeme následující vylepšení výkonu:

priorita	popis	vysvětlení a doporučená opatření
<b>velmi vysoká</b>	Zlepšení odezvy souborového systému	Souborový systém použitý pro adresáře s provozními daty zaznamenává čas přístupu. Tím se zbytečně zatěžuje disk. <b>Doporučení:</b> vypněte zaznamenávání přístupu k souborům (V plné verzi dokumentu přesný postup.)
	...	...
<b>vysoké</b>	Nízká odezva webového serveru Apache	Pomocí benchmarku bylo zjištěno, že webový server Apache přestane efektivně zvládat obsluhu cca 10 simultánně přistupujících uživatelů. <b>Doporučení:</b> zvýšením parametru MinSpareServers a MaxSpareServer na hodnoty X, resp. Y se výkon serveru Apache zvýší. (V plné verzi dokumentu konkrétní postup a hodnoty a další doporučení k ladění webového serveru Apache.)
	...	...

## 5. PROCESNÍ ZLEPŠENÍ

Navrhujeme následující zlepšení postupů používaných ke správě systému:

(Pouze v plné verzi dokumentu.)

## 6. ZÁVĚR

Server BETA je poměrně dobře zabezpečen a s výjimkou špatně zvolených hesel neumožňuje bezprostřední neautorizovaný přístup.

V technické části navrhujeme některá dílčí výkonová opatření, která zvýší spolehlivost a výkon serveru.

Server je kvalifikovaně administrován. Server se zálohuje, ale při testovací obnově jsme zjistili, že některé klíčové části systému chybí a obnova provozu po havárii by byla časově náročná a obtížná, ne-li nemožná. V technické části jsou uvedena opatření, která doporučujeme urychleně provést, aby se zajistila plná funkčnost zálohování.