

Sunday log watch #1

```
##### SLW Start #####
Processing Finished: Sat Oct 26 15:15:00 2008
Date Range Processed: lastweek
Period is: random
Logfiles for Host: all Internet
#####
```

----- News start -----

OpenSource můžeme chápat jako obrovskou celosvětovou laboratoř, která neustále vytváří a vylepšuje software. Vývojáři – tvůrci - spolu komunikují prostřednictvím Internetu - diskuzní fóra, mail, web. Zkusme sledovat aktivitu vývojářů z velké dálky a na velmi vysokém rozlišení, mohla by vypadat obdobně jako Braunův pohyb. Pravidel není mnoho. O úspěch se může pokusit každý kdo má zájem, znalosti a příslušné vybavení. Zdrojový kód je otevřen stačí se připojit k Internetu, stáhnout a přidat se kdykoliv, kdokoli – vládne chaos. Po chvíli pozorování zjistíme, že se v některých částech chaosu vytváří a vystupují pravidelné struktury – **Komerce**.

Pokoušení je příliš veliké. Některé projekty jsou příliš dobré a tak kvalitní, že se po nějaké době musí stát cílem investorů. V poslední době došlo ke komerčnímu uchopení výborného projektu **Bacula** (<http://www.bacula.org/>). Tvůrce Baculy Kern Sibbald na ní začal pracovat v roce 2000 a první veřejná verze byla uveřejněna pod licencí GPL v dubnu 2002 na portálu SourceForge. Tento rok v říjnu po 8 letech od začátku vývoje dochází ke vzniku

Švýcarské komerční společnosti Bacula Systems S.A.

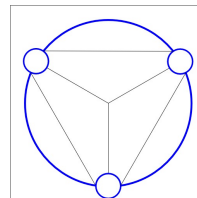
(<http://www.baculasystems.com/>). Finanční zdroje pocházejí přímo od zakladatelů, kteří tak mají sílu prosadit firemní prioritu - zůstat věrni ideám

OpenSource. Cílem nové společnosti je zastřešení vývoje, který nadále zůstává otevřený, poskytování placených služeb, enterprise podpora, konzultace, školení a certifikované binární soubory. Kern Sibbald je členem managementu – pozice „Chairman of the Board“ a „Chief Technical Officer“.



Co je Bacula?

Bacula je sada programů, která umožňuje systémovým administrátorům spravovat zálohování, obnovu a verifikaci dat přes počítačovou síť a to na počítačích různých druhů. Je možné ji samozřejmě používat i na jednom počítači. Celý proces zálohování probíhá poloautomaticky až automaticky,

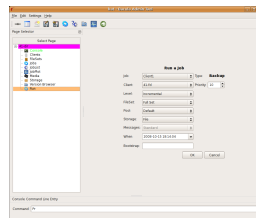


pravidelně v zadanou dobu, většinou v době nejnižšího vytížení systémů.

Záložní kopie dat jsou umístěny na vyhrazený hardware – pásková knihovna, hardisk, dvd. V případě potřeby (havarie, lidská chyba) může administrátor zkontrolovat integritu a strukturu dat. Použije informace uložené v záložní kopii dat.

----- **News end** -----

----- **Security start** -----



V těchto dnech může vážné nebezpečí představovat nová **zranitelnost** v systémech Microsoft windows. Pomocí chytré vytvořeného RPC požadavku může útočník bez jakékoliv autentizace spustit binární kód na vašem systému. <http://www.microsoft.com/technet/security/Bulletin/MS08-067.mspx>.

Zranitelnost (vulnerability) je chyba v procesu, designu, implementaci nebo programovém vybavení, která může být využita (exploit) k narušení bezpečnostní politiky. Tato chyba v systému umožňuje neoprávněné využívání zdrojů.

HIDS (Host-based IDS) je nástroj, který umožňuje monitorovat a odhalit podezřelou aktivitu na systému. Administrátoři HIDS často instalují na kritické systémy, které jsou exponované internetu například DMZ servery. Seznam těchto nástrojů:

OSSEC, Open Source Tripwire, SAMHAIN, OSIRIS, AIDE, Third Brigade Deep Security, Symantec Critical System Protection, IBM Proventia, Enterasys Dragon IDS/IPS, McAfee Total Protection for Endpoint, CA Host-Based Intrusion Prevention System r8, GfiEventsManager, Cisco Security Agent.

----- **Security end** -----

----- **Hack start** -----

Moderní operační systémy mají v sobě zabudovanou jednoduchou možnost kontroly svojí integrity. Chráněny bývají hlavně binární spustitelné soubory. Známa je kontrola pomocí příkazu **rpm -V jméno_balíčku** (`rpm -V httpd`). Příkaz **rpm -Va** začne prověřovat celý systém, výstup není příliš přehledný. Systémy s **dpkg** ukládají kontrolní součty do souborů. Například na Ubuntu jsou umístěny ve `/var/lib/dpkg/info/`. Kontrolu provedeme pomocí příkazu `md5sum`. Balíček `lsf` kontrolujeme příkazem `md5sum -c /var/lib/dpkg/info/lsf.md5sums`

----- **Hack end** -----

SLW End