Keywords: garante privacy, ads, administrator, log amministratore, amministratore di sistema, open source, freeware, syslog, eventlog

Implementare un Syslog/Eventlog server "free" in ambiente Windows

Materiali occorrenti:

Materiale	Descrizione	Dove trovarlo
Un server	Un vecchio PC con XP Professional e un po' di disco	http://www.tubenet.it
Un software "collettore"	Un software di raccolta degli eventi dalle macchine della rete Da installare sul server	**Snare BackLog** **http://www.intersectalliance.com/projects/index.html**
Un "agente" software	Un software "agente" da montare sulle macchine da controllare. Differente per ciascun sistema operativo	**Snare Agent for Windows** **http://www.intersectalliance.com/projects/index.html**
Un Backup di tipo crittato/temporizzato	Per eseguire una copia sicura dei dati di log e renderla immodificabile e trasportabile	http://www.educ.umu.se/~cobian/cobianbackup.htm http://www.truecrypt.org

Come procedere:

Id.	Azione	Note
1	Installare il software collettore sul server definendo la cartella di "log" su un disco capiente	Prendere nota dell'IP della macchina. Ci servirà per impostare la trasmissione dai client. In caso di A.D. Non inserire il PC nel dominio. Lasciarlo come macchina a parte.
2	Installare sui client da controllare il software agente, abilitando il filtro sui log di interesse.	Dopo l'installazione andare nella maschera WEB dell'Agente Snare e selezionare il solo log dell'utente Amministratore.
3	Fare in modo che il software trasmetta i pacchetti di dati al software collettore installato sul server.	Dalla maschera WEB dell'agente impostare l'IP del collettore e la trasmissione in modalità DYNAMIC
4	Aprendo il software Backlog sul server si dovrebbero vedere i pacchetti generati.	Importante impostare i criteri di suddivisione dei log per giorno, per macchina, per tipologia di evento. Fare riferimento al manuale.
5	Sul server impostare un backup crittato e temporizzato (Cobian, opzione timer) Oppure (truecrypt) creare un disco crittato ed impostare un task periodico di backup della cartella di log nel medesimo	La password del disco/backup crittato dovrà essere assegnata dal **titolare** ed essere ignota all'**amministratore**.
6	Fare impostare al titolare la password di accesso al PC. Sia quella di amministratore che quella dell'utente utilizzatore	**L'amministratore non deve conoscere queste password.**
7	Trascrivere tutte le password in busta chiusa e sigillarle	

Bibliografia:
http://diegotech.wordpress.com/2009/11/18/how-to-deploy-a-free-log-server-for-windows/