Legal Logger NEO GDPR

soluzione per registrare i log degli eventi di sistema e monitorare gli accessi ai dati personali. Ottimizzato per essere inserito nel processo di conformità al GDPR.

Legal Logger NEO GDPR è la soluzione per registrare i log degli eventi di sistema e monitorare gli accessi ai dati personali. Ottimizzato per essere inserito nel processo di conformità al GDPR.

Legal Logger NEO GDPR è un appliance e si integra perfettamente in qualsiasi rete informatica aziendale. La raccolta dei log avviene installando un agente sulle macchine e gli apparati da monitorare: la compatibilità è garantita su tutti i sistemi Microsoft Windows, MAC Os, Linux, Unix.

Legal Logger NEO GDPR aiuta gli Amministratori di Sistema e gli IT manager a controllare gli accessi ai sistemi e ad analizzare gli eventi dei dispositivi monitorati. Gli esperti Privacy e i Data Protection Officer (DPO) possono utilizzare la soluzione per perfezionare la fase di audit GDPR (ispezione sistematica, documentata e indipendente) e garantire la tracciabilità delle operazioni svolte dai vari utenti presenti nel network.

1. Descrizione del prodotto

Legal Logger è un sistema di centralizzazione dei log basato su applicazione Client/Server, dove il client è costituito da un agente che viene installato sul sistema da tenere sotto controllo, e il server è costituito da un'appliance con sistema operativo realtime che colleziona i log, li classifica, li esporta in un formato standard (XML) e li marca con una marca temporale digitale.

Il sistema non impedisce in alcun modo l'accesso ai dati ma si limita a tenerne traccia.

2. Come funziona il Legal Logger

L'agente di Legal Logger è in grado di essere installato su qualsiasi piattaforma Win32, ed il nostro server è in grado di accettare qualsiasi sistema *nix che generi log in formato syslog.

A titolo esemplificativo, per controllare l'accesso alle cartelle e files di un File Server Windows 2K8/2k12 o Win7/Win10 è necessario abilitare l'auditing dei criteri di controllo (group policy).

3. Procedura di funzionamento

3.1. Entità Coinvolte:

- Ente certificatore per il rilascio della Marca Temporale.
- Server Centrale con funzione di CA per il rilascio di certificati verso i singoli appliance.
- Server centrale con funzione di archivio Informatico con procedure di backup.
- Appliance presso il Cliente.
- Agente installato sui server/Client.

3.2. Descrizione tecnica:

3.2.1. Appliance

L'appliance è costituito da un dispositivo Embedded di adeguate capacità computazionali con

1. Disco flash da 64 GB (di cui 256 MB occupati dal sistema).
2. Dual core cpu 64 bit
3. 4GB RAM

Tipologia Appliance: Fisica o Virtuale.
Entrambe le versioni necessitano della presenza di un Serve di Dominio.
L'appliance virtuale necessita la creazione di una macchina virtuale (VMware o Hyper-V) su un server interno all'infrastruttura IT. Le caratteristiche della macchina virtuale sono: 2 processori, 4 GB di RAM e 64 GB di disco.

3.2.2. Server

Il server installato e residente presso due Server Farm in cluster geografico con accesso loggato e controllato eroga il servizio di:

- C.A. (Certification Autority)
- SSL Vpn (RSA 2048 bit)
- Archiviazione su file system Criptato DSA 1024 (il livello di encription più basso è dovuto alle migliori performance del sistema)
- Browsing Web dei Log Archiviati (con accesso tramite certificato X.509 personale)
- Marcatura temporale tramite interfacciamento con server dell'ente certificatore (viene rilasciata una marca temporale per ogni file di log).
- Backup di sicurezza dei log dei clienti

I server hanno sede sul territorio europeo.

3.3.4 Funzionalità di Log Management:

1. Registra i log di tutti gli apparati che consentono il forwarding di eventi:
a) Log a sistemi operativi Windows, MAC Os, Unix, Linux, AS400 e superiori;
b) Log a database;
c) Log a file (lettura, modifica, creazione, cancellazione)
d) Log a e-mail (Microsoft Exchange, Lotus Notes);
2. Effettua un dump giornaliero (in formato xml) del registro dei log con:
a) Salvataggio su risorsa locale;
b) Salvataggio in cloud (fino a 180 giorni);
3. Notifiche push e-mail (indirizzi e-mail personalizzabili) near real time (entro 15 minuti) per accessi ripetuti negati;
4. Pseudonimizzazione del registro dei log attraverso tokenizzazione a livello di campo;
5. Monitoraggio ogni 5 minuti dello stato di funzionamento della soluzione con invio e-mail in caso di anomalie (indirizzi e-mail personalizzabili);
6. Invio giornaliero di un report sintetico del registro dei log della giornata precedente;
7. Marcatura temporale giornaliera del registro degli eventi rilasciata da Infocert;
8. Conservazione del registro degli eventi giornaliero in Cloud;

4. Visualizzazione di log

5. Servizi canone
1) Marcatura temporale giornaliera del registro degli eventi;
2) Conservazione del registro degli eventi giornaliero in Cloud;
3) Assistenza tecnica;
4) In caso di guasto, sostituzione dell'appliance in modalità advance replacement.