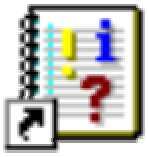
ultimo aggiornamento: **marzo 2011**

Cadmo INFOR Soluzioni di Informatica



Gestione Log di Sistema

Cosa sono i Log di Sistema (Access Log)

Per access log si intende la registrazione degli eventi generati dal sistema di autenticazione informatica all'atto dell'accesso o tentativo di accesso da parte di utente o da parte di un amministratore di sistema o all'atto della disconnessione nell'ambito di collegamenti interattivi a sistemi di elaborazione o a sistemi software.

Gli "*event records*" generati dai sistemi di autenticazione contengono i riferimenti allo "username" utilizzato, alla data e all'ora dell'evento, una descrizione dell'evento (sistema di elaborazione o software utilizzato, se si tratti di un evento di log-in, di log-out o di una condizione di errore, qualsiasi sia la linea di comunicazione o dispositivo terminale utilizzato).

Cosa si deve intendere per "amministratore di sistema"?

L'amministratore di sistema è la figura professionale dedicata alla gestione e alla manutenzione di impianti di elaborazione con cui vengano effettuati trattamenti di dati personali, compresi i sistemi di gestione delle basi di dati, i sistemi software complessi (ERP), le reti locali e gli apparati di sicurezza, nella misura in cui consentano di intervenire sui dati i personali.

Non rientrano invece nella definizione quei soggetti che solo occasionalmente intervengono sui sistemi di elaborazione e sui sistemi software (ad esempio per scopi di manutenzione a seguito di guasti o malfunzionamento).

La normativa

Con il provvedimento generale pubblicato in data 24 dicembre 2008, sulla Gazzetta Ufficiale n. 300, l'Autorità Garante per la privacy, ha dettato le misure che i titolari al trattamento debbono adottare, laddove affidino l'incarico di Amministratore IT (amministratore di sistema, rete o database) a proprio personale dipendente e/o ad aziende o consulenti esterni.

Le misure da adottare sono in vigore da in vigore dal 15 dicembre 2009.

Devono essere adottati sistemi idonei alla registrazione degli accessi logici (autenticazione informatica) ai sistemi di elaborazione e agli archivi elettronici da parte degli amministratori di sistema.

Le registrazioni (access log) devono avere caratteristiche di completezza, inalterabilità e possibilità di verifica della loro integrità adeguate al raggiungimento dello scopo di verifica per cui sono richieste.

Le registrazioni devono comprendere i riferimenti temporali e la descrizione dell'evento che le ha generate e devono essere conservate per un congruo periodo, non inferiore a sei mesi.

Tale registro (il c.d. File Access Log) dovrà:

- essere conservato per non meno di sei mesi
- contenere i dati relativi agli accessi logici degli amministratori IT
- avere caratteristiche di immodificabilità nel tempo
- la sua integrità dovrà poter essere verificabile.

L'Autorità Garante ha inteso creare un sistema di controllo sulle attività effettuate dagli amministratori IT relativamente alle strutture informatiche ed ai dati in esse contenute. In questo modo si è cercato di limitare il rischio di commissione di reati da parte del personale IT che, sfruttando la qualifica di operatore di sistema ed i relativi permessi (IT), poteva abusivamente permanere all'interno di sistemi informatici contro la volontà del titolare stesso, cancellare o alterare i dati in essi contenuti o, peggio, porre in essere attività lesive o dolose.

La creazione di un registro degli accessi rappresenta un primo, sufficiente deterrente per attività illecite commesse da detto personale allorché operante in qualità di amministratore IT.

Prima di procedere oltre occorre notare che l'acquisizione e la conservazione, pro normativa, del File Access Log, è funzione di due elementi:

- la bontà dei dati,
  ovvero l'effettiva rispondenza dei dati alle situazioni che li hanno generati,
  ovvero l'impossibilità che detti dati siano modificati in origine,
- la rispondenza del File Access Log alle caratteristiche di immodificabilità nel tempo.

I compiti dell'amministratore, i suoi ambiti di trattamento sono impartiti analiticamente dal titolare, il quale ha l'obbligo di verificare la persistenza dei requisiti essenziali e dell'adozione delle misure di sicurezza previste, con cadenza almeno annuale.

La designazione degli amministratori deve essere riportata sul DPS (documento programmatico sulla sicurezza), ove dovuto, o su atto autonomo da conservarsi presso la struttura del titolare e da esibire in caso di richiesta da parte dell'Autorità Garante.

Nel DPS aziendale, o nell'atto autonomo sostitutivo, gli amministratori sono indicati individualmente, unitamente alle funzioni ricoperte ed ai propri ambiti operativi consentiti. Costituisce eccezione il caso in cui l'incarico di amministratore IT sia affidato ad una ditta esterna (outsourcing): in tal caso sia l'onere di detenere elenco contenente gli estremi identificativi amministratori IT che l'istituzione di un File Access Log, potrà essere espletata direttamente dal Responsabile esterno ovvero dall'outsourcing.

Tutte le prescrizioni sicurezza sono disponibili sul sito http://www.webinfor.it

Funzionalità di ksLog

CADMO Infor ksLog può essere installato in due modalità diverse a seconda delle esigenze operative.

La prima modalità è specifica per server di rete, applicativi e di dominio, la seconda è disegnata per le postazioni di lavoro che rivestono particolare importanza all'interno dell'organizzazione e che non sono inserite in una rete con server di dominio.

Modalità Server

Se installato su un server sempre attivo e connesso alla rete Internet ksLog fornisce le seguenti funzionalità:

- salvataggio locale giornaliero dei log di sistema
- invio giornaliero a server remoto per l'archiviazione
- consultazione dei log salvati in locale
- consultazione dei log salvati in remoto tramite CADMO Infor Sicurezza On Line
- salvataggio su supporto USB dei log salvati in locale
- eventuale eliminazione dei log salvati in locale

Modalità Personal Computer

Se installato su un personal computer ksLog fornisce le seguenti funzionalità:

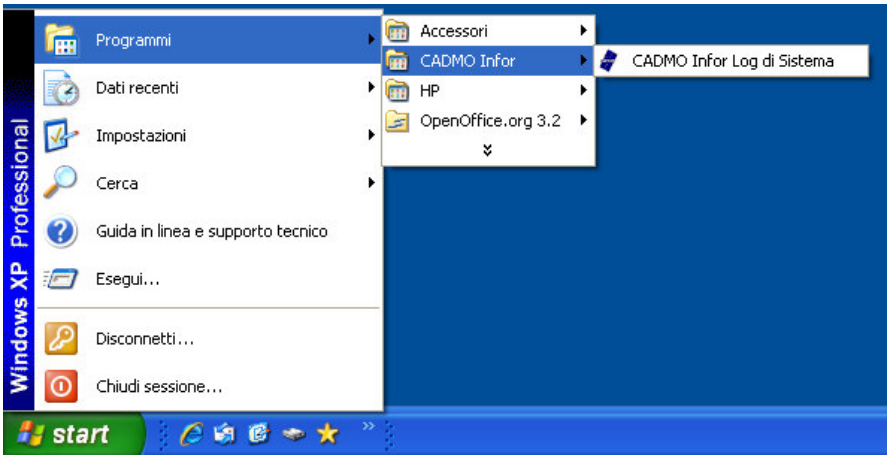
- salvataggio locale ad ogni accensione dei log di sistema settimanali
- consultazione dei log salvati in locale
- salvataggio su supporto USB dei log salvati in locale
- eventuale eliminazione dei log salvati in locale

Utilizzo di ksLog

Una volta installato ksLog è possibile eseguire sul server o sul personale computer tramite l'interfaccia utente le seguenti operazioni:

- consultazione dei log salvati in locale
- salvataggio su supporto USB dei log salvati in locale
- eventuale eliminazione dei log salvati in locale

Per avviare l'interfaccia utente dare clic sul pulsante "Start" di Windows, selezionare la voce "Programmi" e poi la voce "CADMO Infor". Selezionare poi l'icona "CADMO Infor Log di Sistema" come mostrato nella figura 1.



[Figura 1- Avvio dell' interfaccia utente di ksLog]

La finestra principale di ksLog si presenta come nella figura 2 sotto riportata.

[Figura 2- La finestra principale di ksLog]

Nel seguito vengono illustrate le funzioni principali di ksLog richiamabili dalla finestra principale che permettono di gestire i log di sistema sul server o computer locale.

- **Vedi log di sistema salvati in locale**

  Permette di visualizzare i files compressi in cui vengono memorizzati i log di sistema salvati periodicamente

- **Salva ora log di sistema in locale**

  Permette di eseguire subito il salvataggio dei log di sistema invece di attendere la pianificazione automatica (vedi il punto configurazione)

- **Vedi contenuto supporto USB**

  Permette di visualizzare il contenuto del supporto USB collegata al computer.

  Se è la prima volta che il supporto USB viene utilizzato con ksLog viene chiesta conferma per eseguire la prima inizializzazione del supporto.

  Alla prima inizializzazione verrà richiesta di indicare la lettera di unità assegnata dal sistema al supporto USB collegato al computer. Accertarsi di indicare la corretta lettera di unità prima di procedere.

- **Salva log locali su supporto USB**

  Permette di selezionare un periodo temporale per salvare sul supporto USB in unico file di archivio tutti i files compressi che memorizzano i log di sistema individuati dal filtro temporale.

  I filtri temporali disponibili sono:

  - Primo semestre, Secondo semestre
  - Primo trimestre, Secondo trimestre, Terzo trimestre, Quarto trimestre
  - Intero Anno Corrente
  - Intero Anno Precedente,

  Al momento del salvataggio verrà richiesto di indicare il nome desiderato da assegnare al file di archivio.

- **Configurazione**

  Permette di visualizzare le impostazioni di funzionamento di ksLog configurate al momento dell'installazione e se necessario di effettuare eventuali modifiche alla configurazione.

  Si raccomanda di eseguire eventuali modifiche solo sotto la guida di personale tecnico CADMO Infor.

- **Elimina log locali**

  Permette di visualizzare di eliminare i files compressi in cui vengono memorizzati i log salvati in locale. Viene richiesta conferma. È importante avere prima eseguito la funzione di **Salvataggio su supporto USB** descritta sopra.

Installazione e configurazione di ksLog

L'installazione e la configurazione di ksLog devono essere effettuate utilizzando un account locale con poteri amministrativi.

La configurazione richiede l'identificazione del Server o del Personal Computer utilizzando le convenzioni e le numerazioni utilizzate anche in CADMO Infor Sicurezza On Line.

L'installazione e la configurazione di ksLog verranno effettuate sui Server e sulle postazioni di lavoro individuate in collaborazione con il Cliente e deve essere eseguita dal personale tecnico CADMO Infor