



Management Pack 196 (MP196)



MANAGEMENT SOLUTION

Cos'è

E' un Management Pack per Microsoft System Center Operations Manager che fornisce un insieme di regole e report utili a determinare la conformità del proprio sistema informatico con l'allegato B della Legge 196/03 "Codice in materia di protezione dei dati personali".

Che problema risolve

La legge 196/03 "Codice in materia di protezione dei dati personali" impone a chiunque tratti dati personali di realizzare opportune norme per la tutela della riservatezza degli stessi. Alcuni dei principi generali della legge sono esplicitati operativamente nel suo allegato B, prescrivendo controlli su credenziali, password, antivirus e così via. Per tutti gli elementi che possono essere verificati automaticamente, Progel srl ha sviluppato un Management Pack per System Center Operations Manager che permette di controllare costantemente la conformità del proprio sistema informatico con quanto imposto dalla legge.

Inoltre aggiunge una serie di regole per l'audit della gestione degli account utente, l'audit dell'attività di logon ai server (interattivo o via terminal server), e l'audit dell'accesso ai file.

Principali funzionalità

Le regole contenute nel Management Pack controllano che:

- l'esistenza di account inutilizzati in Active Directory ed eventualmente li disabilitano (Art.7 All. B);
- che tutti gli account presenti in Active Directory abbiano cambiato la loro password nel limite temporale prescritto (Art.5 All. B);
- che le policy sulle password rispettino i criteri di complessità necessari (Art.5 All. B).
- che la creazione di un account rispetti i criteri minimi necessari, ad esempio che sia forzato un cambio password da parte dell'utente al primo logon o che non sia abilitata l'impostazione che evita la scadenza della password (Art.2. All. B).

- che l'antivirus abbia pattern aggiornati (al momento il controllo è disponibile per TrendMicro OfficeScan 7.x e eTrust InoculateIT 7.x) e che sia funzionante simulando l'infezione di un virus tramite il pattern EICAR (www.eicar.com) (Art. 16 All. B)
- che le patch di sicurezza rilasciate prima di una soglia definita dall'utente (di default 40 giorni) siano state applicate ai server (Art. 17 All. B) - perché questo controllo abbia successo occorre che il server sia gestito tramite SMS 2003 e "Inventory Tool for Microsoft Updates".

Per ogni situazione problematica viene generato un alert e in base alle esigenze specifiche può essere attivato un meccanismo di notifica.

Il management pack è completato dalle seguenti funzionalità:

- Collezione degli eventi di accesso a file sensibili
- Collezione degli eventi di logon locali ai server
- Verifica delle policy di auditing e notifica su ogni scostamento delle stesse
- Collezione degli eventi di gestione degli account e gruppi utente e report sugli stessi

Le regole di gestione sono completate da una serie di report di compliance che coprono le seguenti necessità:

- Elenco degli account inutilizzati da disabilitare o disabilitati in automatico
- Elenco degli account che non hanno cambiato la propria password nel limite di tempo indicato
- Eccezioni nelle politiche di qualità della password (ad esempio lunghezza)
- Eccezioni nelle politiche di auditing
- Eccezioni nella creazione degli account utente
- Elenco delle operazioni amministrative compiute dagli operatori sugli account
- Elenco degli accessi a file sensibili e da parte di chi

Il controllo è applicabile a tutti i sistemi operativi attualmente supportati da Microsoft.



Advanced Infrastructure Solutions
Information Worker Solutions
Learning Solutions