



Provvedimento del Garante per gli amministratori di sistema.

La soluzione basata su OneSign.



Il provvedimento in breve

Con il provvedimento del 27 novembre 2008 (pubblicato sulla Gazzetta Ufficiale lo scorso 24 dicembre) il Garante ha prescritto specifiche misure ed accorgimenti ai titolari dei trattamenti "effettuati con strumenti elettronici relativamente alle attribuzioni delle funzioni di amministratore di sistema."

Chi

Tale provvedimento non riguarda esclusivamente l'attività degli amministratori di sistema ma anche altre categorie di figure professionali quali gli amministratori di banche dati, reti e apparati di sicurezza e di sistemi di software complessi, le cui attività possono comunque in determinati casi comportare dei rischi per la protezione dei dati personali.

Il provvedimento riguarda organizzazioni sia pubbliche che private.

Adempimenti richiesti

Il provvedimento richiede sia adempimenti di tipo organizzativo che tecnici. In particolare, il punto F richiede che tutti gli accessi ai sistemi sottoposti al provvedimento debbano essere registrati e conservati e devono avere caratteristiche di completezza, inalterabilità e possibilità di verifica della loro integrità adeguate al raggiungimento dello scopo per cui sono richieste.

Quali sistemi

Oltre ai server dove girano applicazioni e database che contengono o gestiscono dati sottoposti al trattamento, anche l'accesso a banche dati, apparati di rete e di sicurezza e applicativi software complessi (come ERP o CRM) sono sottoposti al provvedimento nella misura in cui chi amministra questi sistemi possa accedere ai dati personali trattati.

Requisiti tecnici e di sicurezza

Nessuna specifica sugli aspetti tecnici o sui livelli di sicurezza necessari è descritto nel provvedimento, salvo i generici requisiti di completezza, inalterabilità e possibilità di verifica della loro integrità (dei log). Si lascia la discrezione al titolare dei trattamenti la scelta delle modalità di tracciamento degli accessi e di conservazione dei log in base al contesto specifico per raggiungere gli obiettivi del provvedimento.

Esclusioni

Sono esclusi dal provvedimento i sistemi utilizzati per adempimenti amministrativi contabili (come ad esempio gestione ordini, buste paga, presenze, corrispondenza ordinaria con clienti e fornitori, ecc.).

Scadenza

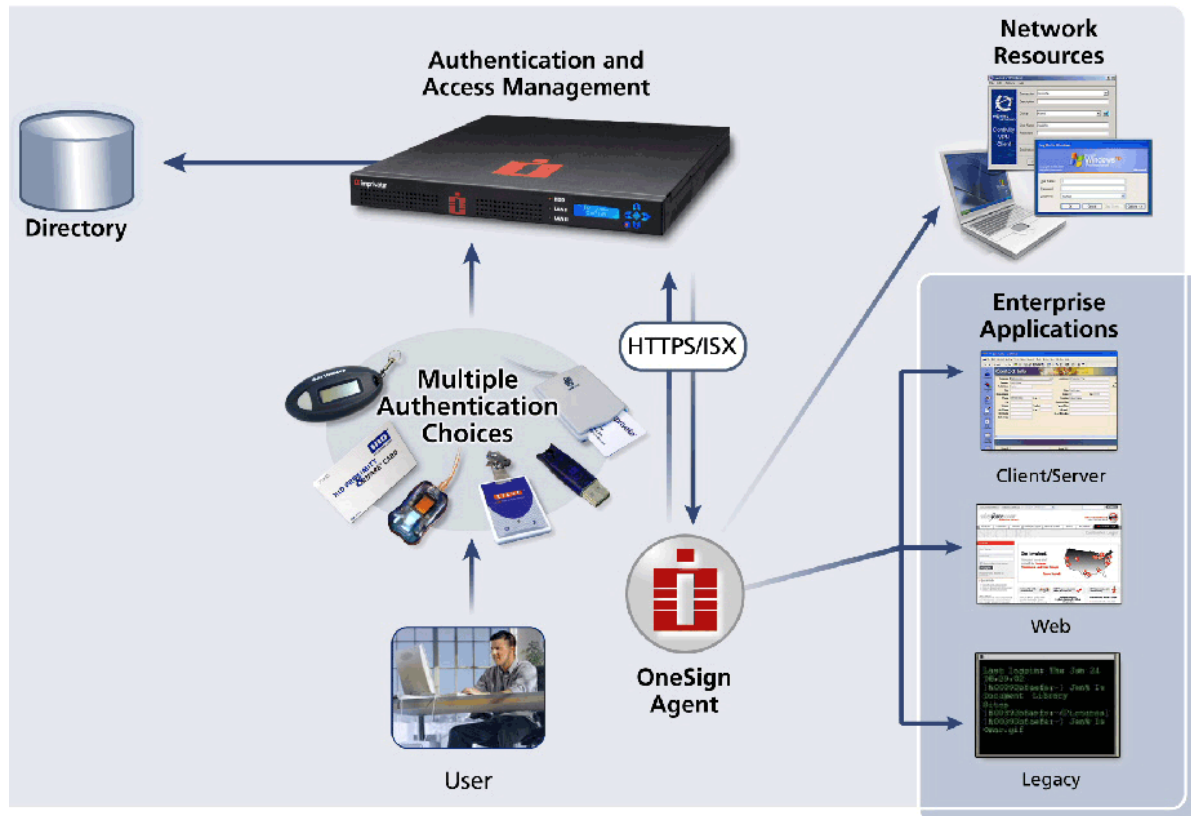
15 Dicembre 2009

Sanzioni

Le sanzioni previste vanno da 30.000 a 180.000 euro

La soluzione OneSign

OneSign è una soluzione non invasiva basata su appliance che non richiede modifiche a server, applicazioni o alla directory aziendale degli utenti.



OneSign comprende diversi moduli:

- **Access Management:** per gestire e fare l'auditing dell'autenticazione primaria su sistemi Windows. Supporta anche diverse tipologie di Strong Authentication (Fingerprint, Token One Time Password, Proximity Card, Smart Card) senza richiedere server o software di gestione aggiuntivi.
- **Single Sign-On:** permette di gestire login e password per gli accessi ad applicativi, database e server remoti. L'agent si occupa di inserire le credenziali dell'utente. Abilitando la generazione di password casuali forti che nemmeno l'utente conosce, garantisce che tutti gli accessi avvengano tramite OneSign. Il sistema può anche essere integrato con sistemi di Provisioning tramite SPML. Tutte le operazioni sono registrate sul sistema di auditing centrale.
- **Auditing:** tutte le operazioni (dai login primari a Windows, agli accessi tramite Single Sign-On fino alle modifiche della password) vengono registrate in maniera sicura sull'appliance, dove vengono mantenute crittografate e non sono modificabili. Il tempo di ritenzione dei dati di auditing è configurabile e può essere di alcuni anni.
- **Integrazione sicurezza Fisica/Logica:** è possibile integrare OneSign con un sistema di sicurezza fisica di controllo degli accessi per disporre di policy di sicurezza integrate: l'utente non può accedere alla rete se non ha utilizzato il proprio badge per entrare in azienda.

OneSign e il provvedimento del Garante

Tutti gli accessi primari ai sistemi Windows sono controllati direttamente dall'agent al momento del login a Windows (con o senza Strong Authentication) ed i relativi log sono inviati all'appliance. L'agent può essere installato su Windows 2000, XP, Vista e Windows Server (inclusi Terminal Server e Citrix).

L'accesso agli altri sistemi sottoposti al provvedimento del Garante dovranno avvenire tramite una serie di applicazioni client (per esempio Putty per i server Unix o Oracle Enterprise Manager per il database Oracle) che saranno profilate per il Single Sign-On tramite un semplice strumento web (APG, Application Profile Generator) che non richiede la conoscenza di linguaggi di script.

Una volta profilate le applicazioni e acquisite le credenziali (dall'utente o tramite provisioning), l'agent, ad ogni richiesta di login, invierà le credenziali al posto dell'utente.

Il modulo di SSO si occuperà anche, al primo cambiamento di password, di generare una password casuale seguendo una policy definita in base all'applicazione. In questo modo l'amministratore di sistema non conosce più le credenziali di accesso ed è obbligato ad utilizzare il SSO per collegarsi a sistemi/database/applicazioni abilitati.

Anche in questo caso gli eventi relativi agli accessi e alle modifiche di password vengono salvati sull'appliance, rispettando i requisiti di completezza, non modificabilità e certificazione.

Ulteriori eventi possono essere catturati profilando altre schermate applicative (come ad esempio log-out, errori, transazioni pericolose ecc.) in base alle esigenze specifiche.

Il titolare del trattamento avrà dunque a disposizione gli strumenti e tutta la reportistica necessari per gli adempimenti richiesti.

Inoltre, l'utilizzo della Strong Authentication, associata alla reportistica, incrementa notevolmente il fattore sicurezza: la password da sola, infatti, difficilmente garantisce la reale identità della persona che ha avuto accesso ai sistemi o alle applicazioni da controllare, rendendo i semplici log uno strumento di parziale efficacia.

La correlazione forte fra utente primario e accesso agli altri sistemi permette infine di risolvere il problema degli account di gruppo (come ad esempio accessi root condivisi fra più utenti) o di gestire in modo sicuro l'accesso privilegiato di parte di terzi: grazie al SSO non sarà necessario dare le credenziali amministrative ai consulenti esterni in quanto sarà il sistema di SSO a provvedere.

Benefici

- Centralizzazione del controllo degli accessi
- Autenticazione centralizzata degli Amministratori, anche in modalità "forte"
- Accesso ai sistemi da parte degli Amministratori anche senza conoscere le credenziali
- Accesso da parte di operatori terzi (ad esempio Outsourcer) senza conoscere le credenziali
- Strong Authentication (senza altro software da installare/gestire)
- Logging degli accessi sicuro, completo ed inalterabile
- Report sugli accessi effettuati
- Soluzione ridondata di default per garantire l'Alta Disponibilità
- Gestione, solo tramite interfaccia web, molto semplice
- Tempi di implementazione rapidi

OneSign non solo aiuta a risolvere il problema dell'adeguamento al provvedimento del garante, ma è una piattaforma per aumentare la sicurezza interna, raggiungere la compliance anche ad altri regolamenti/leggi (Legge sulla Privacy, PCI, ecc) e migliorare l'efficienza degli utenti e dell'helpdesk riducendo i problemi legati alla gestione delle password (password reset, condivisione degli account, password scritte sui bigliettini, errori di login ecc.).