



Registrazione degli Accessi degli Amministratori di sistema

Gli amministratori di sistema sono figure essenziali per la sicurezza delle banche dati e la corretta gestione delle reti telematiche. Sono esperti chiamati a svolgere delicate funzioni che comportano la concreta capacità di accedere a tutti i dati che transitano sulle reti aziendali ed istituzionali. Ad essi viene affidato spesso anche il compito di vigilare sul corretto utilizzo dei sistemi informatici di un'azienda o di una pubblica amministrazione. Per questo il Garante sulla Privacy ha prescritto l'adozione di specifiche misure tecniche ed organizzative da parte di enti, amministrazioni e società private che agevolino la verifica sull'attività dell'amministratore di sistema da parte di chi ha la titolarità delle banche dati e dei sistemi informatici.

Regi.A è una soluzione che permette di ottemperare a queste richieste del Garante relativamente agli amministratori di sistema (provvedimento del 27-11-08, pubblicato sulla G.U. n. 300 del 24-12-08). Le misure e le cautele devono essere messe in atto sia da parte delle aziende private che dei soggetti pubblici, compresi gli uffici giudiziari, le forze di polizia e i servizi di sicurezza.

Cosa richiede il Garante

Dal punto 4.5: *"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 allo scopo di verifica per cui sono richieste."

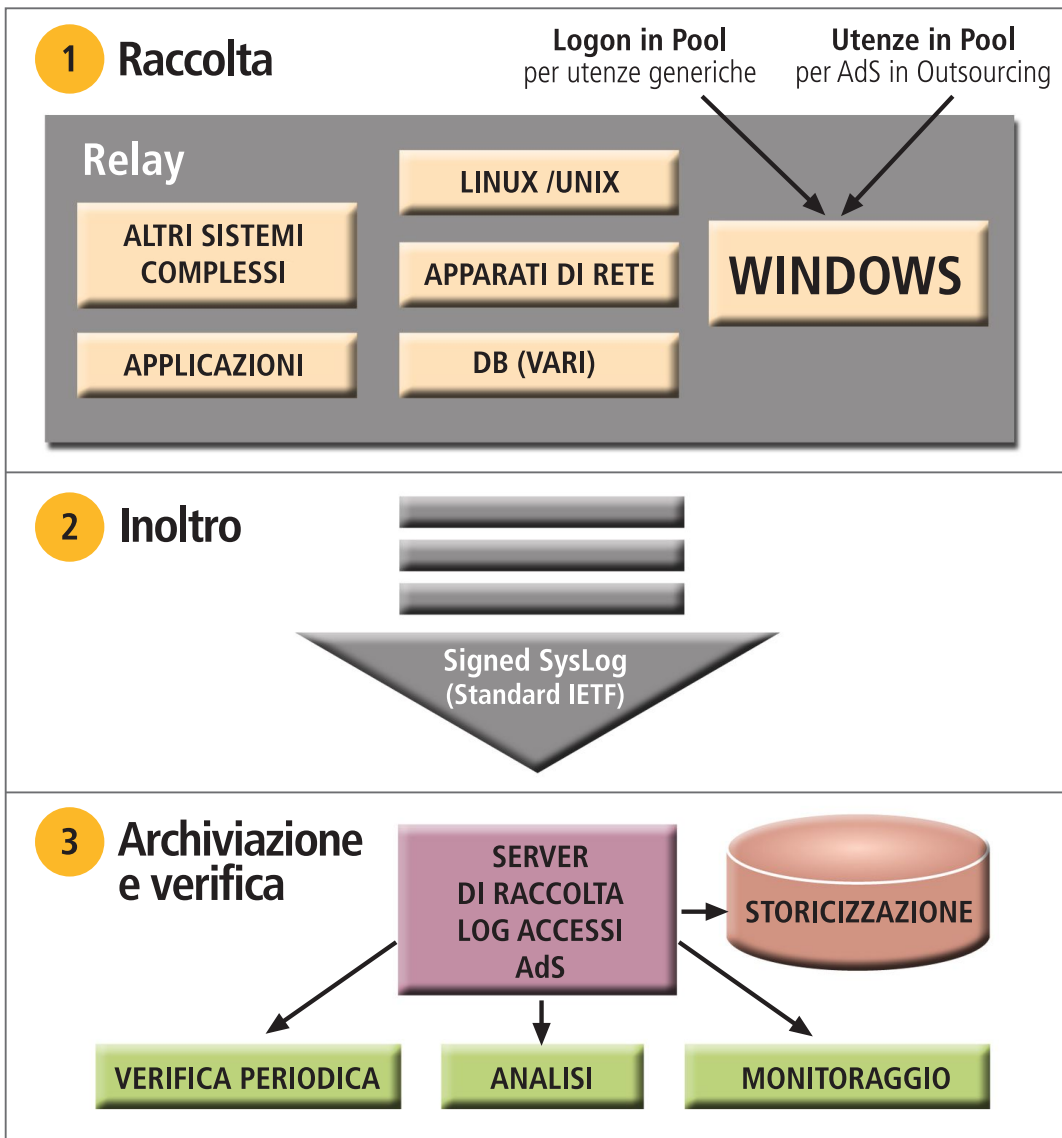
Cosa prevede la soluzione

La soluzione è costituita da:

- Componenti per la registrazione degli accessi e l'inoltro degli eventi secondo le specifiche richieste (Relay).
- Componenti per l'analisi in tempo reale degli eventi raccolti centralmente per ricerche e verifiche richieste dal Garante (**Monitor di Regi.A**)



Monitor di Regi.A



Relay

Per ogni sistema interessato dalla registrazione dei log è previsto un Relay. Con l'utilizzo di questi relay, **Regi.A** è in grado potenzialmente di gestire i log di tutti i sistemi. I Relay registrano gli eventi e li inoltrano al server di raccolta in formato signed syslog.

Sistema di raccolta e veicolazione dei log

È stato scelto lo standard internazionale syslog, nella forma definita da IETF come syslog-signed, che garantisce compatibilità e omogeneità di formato.

Sistemi supportati

Windows 2000, XP, Vista, Win2003, sistemi Linux e Unix (Ubuntu, Fedora, RedHat, Os/x, Suse e altri) e apparati di rete compatibili con syslog standard - HP, Cisco, Fortinet, ecc.

Caratteristiche e vantaggi

- Filtro alla fonte**
 Riduce drasticamente i costi di archiviazione e semplifica le ricerche
- Completamento dei dati alla fonte**
 Identifica con precisione gli accessi amministrativi
- Abilitazione automatica degli audit amministrativi**
 Controllo anti-elusione (solo Windows)
- Certificazione alla fonte**
 Gli eventi sono firmati alla fonte, resi inalterabili ed identificabili univocamente
- Bufferizzazione**
 Riduce al minimo il traffico di rete e gestisce le indisponibilità della rete o dei server di raccolta (off-line)
- Collegamento tra accessi, utenze e amministratori**
 Collega le attività alle utenze che le hanno generate e all'amministratore
- Integrazione dei dati**
 Integrazione dei dati degli amministratori di più sistemi, compresi gli outsourcers
- Formato standard ed aperto**
 Syslog-signed, standard IETF per garantire l'interoperabilità con i migliori software di mercato

MODULI AGGIUNTIVI

Relay per altri sistemi	El.A.S. Elenco Amministratori di Sistema	LogIPo Logon in Pool	UtIPo Utenze in Pool
Database Sistemi custom Applicativi	Gestione centralizzata dell'elenco degli amministratori di tutti i sistemi (Domini, DBA, Apparati, Applicazioni, ecc)	Gestione di credenziali amministrative generiche, non assegnate ad un singolo amministratore, ma utilizzate da più individui identificabili con credenziali di dominio Windows.	Gestione di utenze esterne e/o con privilegi amministrativi temporanei in ambiente Windows.