Audit degli accessi alle risorse elaborative

Raffaella D'Alessandro

Security and Privacy Services

Roma 10 Giugno 2008

Log Management

Cosa sono log, log retention e log management?

Perchè c'è l'esigenza di gestire i log?

Log Management: la gestione del ciclo di vita del log

La Sicurezza nel Processo di Log Management

Implicazioni connesse con il Log Management

I fattori di successo per Log Management e Log Retention

Cosa sono log, log retention e log management?

Log: Una registrazione a cui l'organizzazione riconosce ufficialmente uno scopo legato ad una legge o ad un regolamento , o unvalore di business/mission, o una esigenza tecnica o di sicurezza.

Log retention: Si riferisce alla conservazione di una registrazione per uno specifico periodo di tempo, in funzione di particolari esigenze di legge/regolamenti, di business, di natura tecnica o di sicurezza.

Log management: E' il processo per il controllo sistematico del ciclo di vita dei log.

Perchè c'è l'esigenza di gestire i log?

Ragioni di Business/Mission

Normativa del Settore della specifica PA
Normativa Interna dell'Amministrazione (Circolari, Delibere, altro)
Miglioramento dei servizi al pubblico

Conformità con leggi e regolamenti

Leggi nazionali e internazionali (Codice privacy, Copyright Sw, ..)
Regolamenti Pubblica Amministrazione (CAD, Indirizzi CNIPA, SPC,..)
Perseguibilità reati informatici

Ragioni tecniche

Incident & problem Management
Performance & Test
Consistenza dati

Ragioni di Sicurezza delle Informazioni

Verifica rispetto politiche di sicurezza delle Informazioni
Gestione delle violazioni di sicurezza e dei security incident
Auditabilità delle attività condotte in ambito ICT

Attenzione ad armonizzare limitazioni e conflitti imposti dalle leggi

Il ciclo di vita del Log

Generazione

Local Registration | Local Archive | Local Retrieval * | Local Destruction

Trasmissione verso sito Centrale

Central Registration | Central Archive | Central Retrieval * | Central Destruction

Trasmissione verso siti esterni

External Archive | External Retrieval * | External Destruction

* Accesso diretto, normalizzazione, aggregazione, correlazione, analisi, stampa, reporting, monitoring

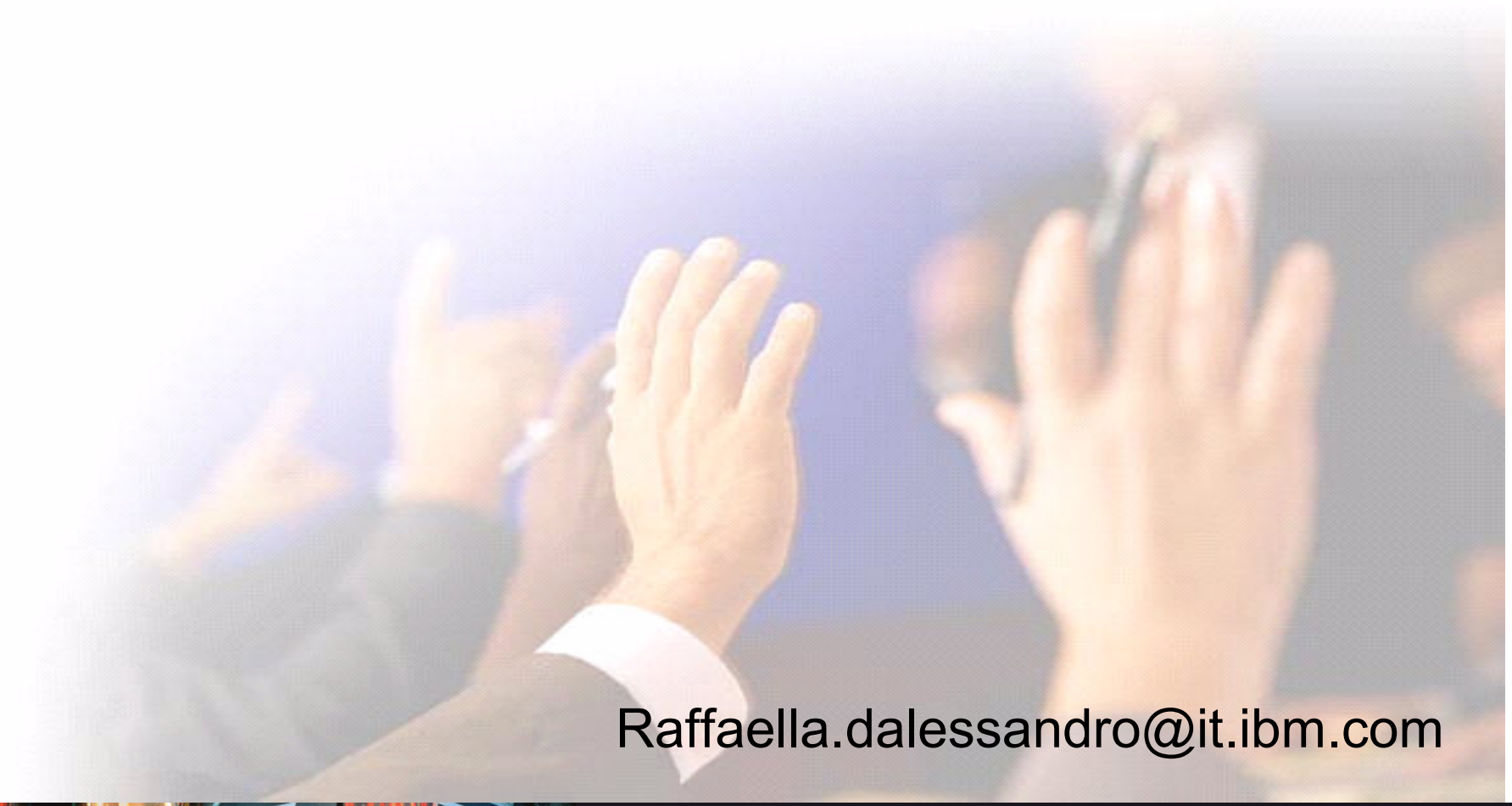
Le esigenze di sicurezza per ogni fase del ciclo di vita dei log

I requisiti di Riservatezza, Integrità, Disponibilità ed Autenticità dei log devono essere garantiti durante **tutte** le fasi del ciclo di vita del log

Le minacce da contrastare includono:

- Accesso non autorizzato anche solo in lettura
- Cancellazione o modifica non autorizzata
- Interruzione non autorizzata della registrazione e della raccolta del log
- Modifica non autorizzata del clock sinchronization
- Sovrascrittura
- Distruzione non autorizzata
- Esportazione e trasmissione non autorizzata
- Conservazione oltre i limiti temporali autorizzati

Domande e risposte



Raffaella.dalessandro@it.ibm.com