CAMBIAMENTO/MIGLIORAMENTO
Migliorare i risultati di gestione in situazioni di incertezza

Sicurezza e Identity & Access Governance

Andrea Foschi

Bologna, 6 settembre 2016

Agenda

1 L’importanza dell’informazione

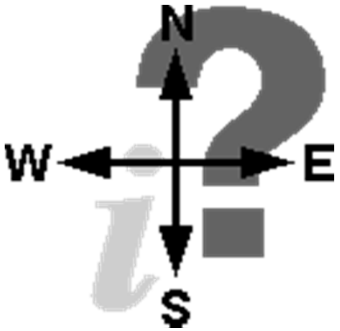
2 Sicurezza e sistemi IAG

2 Compliance

3 Obiettivi di un sistema IAG

L'importanza e l'aumento dell'informazione

L'informazione è oggi un elemento "cruciale" per poter svolgere qualsiasi tipo di attività; tutte le Organizzazioni trattano oramai un numero di informazioni che è aumentato in modo esponenziale nel tempo … forse fin troppe.



E' pertanto cresciuta la consapevolezza di quanto l'informazione (*parte degli Asset "intangibili" di ogni Organizzazione*) siano un **valore strategico**

La distruzione o la divulgazione non consentita di una informazione di business produce sempre e comunque un danno all'azienda.

L'importanza e l'aumento dell'informazione

Garantire la sicurezza delle proprie informazioni significa quindi garantire il proprio patrimonio da potenziali danni … anche se a riguardo le imprese maggiormente sensibili sono proprio quelle che hanno subito rilevanti perdite di dati e, di conseguenza, gravi perdite economiche.

Questo accade perché le imprese spesso tendono a sottovalutare i rischi connessi ad una non corretta gestione e tutela delle informazioni.

Il tema della "Security" non passa solo dal governare e tutelare il proprio Sistema Informativo bensì dal:

- *conoscere l'intera "mappa" delle informazioni aziendali (cartacee, informatiche, vocali, audio, video, ecc…)*
- *comprendere il valore delle diverse tipologie di dati gestiti*
- *prevedere opportune azioni a tutela degli stessi in base ad una corretta analisi dei rischi*

Il governo degli accessi

Ma in questo scenario in cui l'informazione (in modo particolare quella digitale) è sempre più un asset di valore per l'azienda qual è una delle contromisure più importati a tutela della protezione delle informazioni ?

Il governo dell'identità e degli accessi

Pensare di garantire la sicurezza delle informazioni senza un adeguato governo dell'identità e degli accessi è come pensare di fare ordine pubblico in un mondo privo di documenti di identità, di porte e di serrature.

I sistemi IAG non solo sono propedeutici alla maggioranza delle contromisure implementabili sulla sicurezza ma sono elemento indispensabile per molteplici aspetti di compliance normativa.

Le normative e gli standard

262/05

Disposizioni per la tutela del risparmio e la disciplina dei mercati finanziari

- Focus su applicazioni significative per la predisposizione del bilancio;
- Focus sulla separazione dei compiti (SOD)

ISO 27001

- Definizione politiche di sicurezza
- Sicurezza Logica e Fisica
- Continuità dei servizi

231/01

Responsabilità di Impresa, Codice Etico e Responsabilità delle persone Giuridiche

- Focus sugli aspetti di frodi

D. lgs. 196/03 (Privacy)

Protezione dei dati personali e sensibili

- Focus su applicazioni che custodiscono dati sensibili
- Focus sulla figura degli amministratori di sistema (allegato B)

Cosa richiedono le normative ?

…e anche un sistema di governo sicuro....?

- ✓ Aderenza al principio del «Minimo Privilegio»
- ✓ Assegnazione abilitazioni attraverso procedure coerenti, ripetibili e tracciabili e non per «copia account»
- ✓ Disattivazione o cancellazione degli account in coerenza al ciclo di vita dell'identità
- ✓ Revisioni periodica delle abilitazioni
- ✓ Controllo e limitazione della presenza di account orfani, applicativi, di servizio sui sistemi
- ✓ Identificazione di utenti o gruppi che attraverso gli accessi concessi possono svolgere attività in conflitto tra loro (SOD)

Obiettivi di un sistema IAG

- dare evidenza a tutti gli attori interessati, di quelle che sono le abilitazioni in essere su tutto il panorama applicativo dell'organizzazione;
- Implementare e monitorare processi di ricertificazione degli accessi da parte dei certificatori autorizzati (Business Owner);
- Implementare la gestione del ciclo di vita delle identità (user LifeCicle)
- Fornire reportistica as-is e storica degli accessi in ottemperanza alle normative vigenti e/o specifici requisiti indicati da eventuali organismi di controllo (auditor interni, Odv, ecc);
- Implementare processi per la gestione e la tracciatura delle richieste di abilitazioni (change request);
- Implementare la modellazione di ruoli (role mining);
- Fornire strumenti per la definizione di regole SOD e di valutazione del rischio relativo all'attività di assegnazione autorizzazioni.

Riferimenti

Andrea Foschi
afoschi@soluzioniaziendali.net

Soluzioni srl

Via Andrea Ercolani, 9 40026 Imola
info@soluzioniaziendali.net www.soluzioniaziendali.net