Il mestiere del security manager

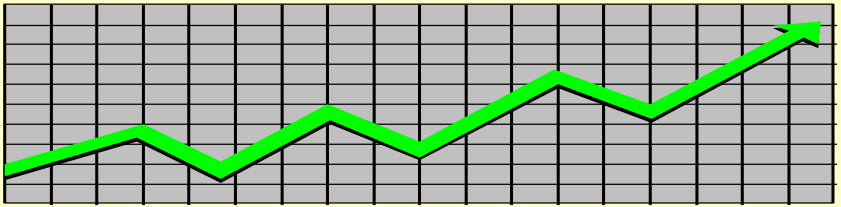
Giorgio Ledda
Senior Director Security
Oracle Corporation

CLUSIT
Associazione Italiana per la Sicurezza Informatica

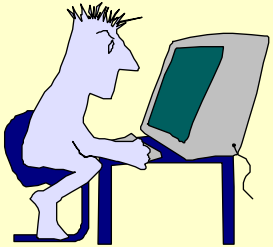
Argomenti della discussione

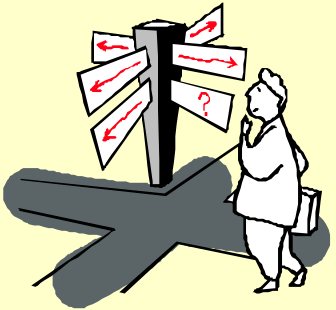
- Il mestiere del security manager.
- Perché la security?
- Una definizione di security.
- La security in Oracle.
- Alcuni elementi di successo dei programmi di security.

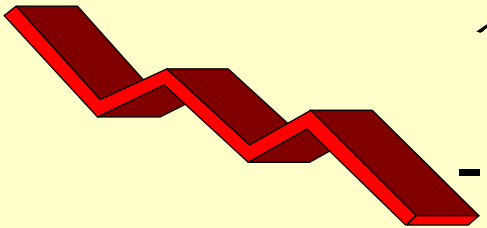
Il mestiere del security manager



+ $







- $

Perché Security?

.....Perché Security

La turbolenza sociale;
i mutamenti politici globali;
Il terrorismo globale;
L'esasperazione e speculazioni delle borse finanziarie;
il rapido sviluppo tecnologico;
i continui processi di ristrutturazione per ridurre costi;
la progressiva de-materializzazione delle risorse aziendali;
la globalizzazione;
I nuovi mercati emergenti;
l'intensificarsi dei rapporti internazionali;
il proliferare di norme/leggi a livello locale, nazionale e internazionale.

...verso una nuova cultura. Sul rischio di security.

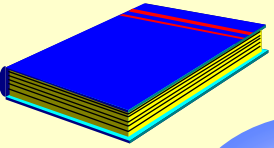
Una definizione di security: UNI 10459

business security: studio, sviluppo e attuazione delle **strategie**, delle **politiche** e dei piani operativi volti a prevenire, fronteggiare e superare eventi in prevalenza di natura dolosa e/o colposa, che **possono danneggiare le risorse materiali, immateriali, organizzative e umane** di cui l'azienda dispone o di cui necessita per garantire un'adeguata capacita' concorrenziale, nel breve, nel medio e nel lungo termine".

La security in Oracle

- **Oracle e' un leader del suo mercato**
  - Elevata attenzione da parte dei media
  - necessità di una chiara disciplina.
- **Modello organizzativo fortemente centralizzazione**
  - Diminuisce i costi ma può aumenta i rischi!
  - Sviluppo di prodotti in nuovi mercati
- **La situazione esterna**
  - Settembre 11, 2001
  - Nuove regole finanziarie per le società Americane SOX.
  - Aumento dei rischi da Cyber Crime
- **Condizioni**
  - Aumento di nuove leggi a livello governativo, aumenta la responsabilità legale di Oracle
- **Clienti**
  - Impongono requisiti contrattuali

Organizzazione della sicurezza in Oracle



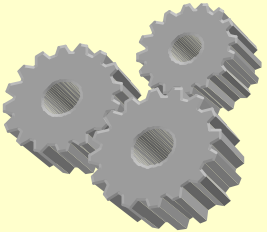
Ciclo della Security

Audits
Verifiche e
Migliorie

Strategie del
Business

Requisiti legali
e contrattuali

Investigare
Violazioni di
politiche
procedure e
leggi



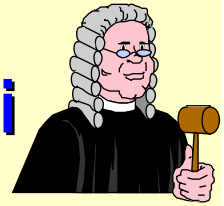
Minacce
Vulnerabilità
E Rischi

Educazione e
Formazione

Politiche Procedure
& Standard

Contromisure:
$ - budget
I responsabili
L'approvazione
-

Security e requisiti legali e contrattuali



- **Operare nel rispetto delle leggi e regolamenti dove la società opera. Rispetto degli obblighi contrattuali e dei requisiti prescritti per assicurare la protezione dei beni propri od terzi.**

ALCUNI ESEMPI:

- **Protezione dei dati personali**
- **Protezione dei documenti aziendali**
- **Protezione del copyright del software**
- **Proprietà Intellettuale**
- **Computer Crime/ Atti illeciti**
- **Insider Trading**
- **Applicazione di regole sul export di tecnologie informatiche.**
- **Spionaggio industriale**
- **Sicurezza imposta da enti governativi**

In caso di violazione vi sono significanti Sanzioni!

Security ed etica

- **Assicurare un adeguato livello di security e ‘ un dovere e senso civico di ogni organizzazione.**
- La sicurezza o la mancanza di sicurezza non e più un problema che ha le sue conseguenze e i sui **confini all’interno di un organizzazione**.
- Le organizzazioni vengono sempre più integrate e parte attiva del **contesto sociale globale.**
- Prodotto difettosi o non distribuiti, servizi non erogati, divulgazioni di informazioni strategiche, perdita di reputazione per varie ragioni interne possono avere un grande impatto sociale.con **conseguenze disastrose anche con perdite di vite umane ed economiche.**
- Esempio network , sistemi informativi ed INTERNET , ogni organizzazione deve adottare efficaci politiche di security in quanto **un danno al proprio sistema informatico può impattare e minacciare la sicurezza di altri.**

La Security NON opera unilateralmente!

L'organizzazione di security deve operare con il vertice dell'azienda e tutte le divisioni aziendali per definire attraverso l'analisi dei rischi una equa ed accettabile strategia e politica di security.

Alcuni elementi di successo della security

- La cultura
- Le politiche e le regole
- Ruoli e responsabilità
- La formazione
- Il controllo

La cultura della security

Mentre le procedure, le strategie, l'organizzazione e la formazione sono importanti, il fattore più critico per sviluppare una organizzazione consapevole dei rischi di security e la creazione di una valida cultura di security.

Le politica e le regole

- Le leggi
- Gli standard
- I contratti
- Le procedure
- Il buon senso ecc.

Tutto ciò va identificati, sviluppato, divulgato, spiegato e misurato.

Ruoli e responsabilità

- Organizzazione della sicurezza come per le altre discipline “Top down”, Chiare e definite responsabilità: Chi fa che cosa. “Corporate Governance”

- Definire con il vertice il concetto di security della propria organizzazione.

- Rendere i dipendenti importanti

La formazione

- Far sapere.
- Mantenere alto il livello di consapevolezza.
- Mantenere costante il livello di attenzione all security.
- Misurare il livello di consapevolezza.

Il controllo

Valutare e farsi valutare (Audits e certificazioni)

- Dai clienti interni.
- Dai clienti esterni.
- Da organizzazioni indipendenti (SAS70- ISO 17799 –ITSEC –ecc.)

Applicare le “Best practices”

La componente umana della security

Le persone sono spesso l'elemento vulnerabile di un sistema di security e trainante per il suo successo.

- Vengono valutate in fase di assunzione.
- Vanno educati ed incoraggiati alla protezione.

- Vanno identificate tecnologie, automatismi e metodologie che prevengano e rieducano fattori umani negativi al fine della security.
- Sviluppare procedure chiare e facilmente raggiungibili da tutta la forza lavoro.
- Le persone devono sapere che l'organizzazione controlla il buon funzionamento del programma di security aziendale e che violazioni delle procedure non sono tollerate.

Un Esempio di criticità

- Esigenze delle imprese di espandere attività di produzione e ricerca verso mercati più competitivi Come India e Cina creano nove opportunità come pure nuovi elementi di rischio che richiedono nuove strategie di security. Da qui alcune nuove esigenze:
- **Il concetto di rischio mutabile.**
- **La valutazione integrata dei rischi.**
- **Il concetto di Continuità del Business.**

Alcuni elementi di un programma di security

- COMITATO STRATEGICO DI SECURITY.
- RISCHI & VULNERABILITÀ.
- POLITICHE & PROCEDURE.
- FORMAZIONE ALLA SECURITY.
- REQUISITI LEGALI.
- GESTIONE DEGLI INCIDENTI, EMERGENZE E CRISI.
- SECURITY AUDIT.
- VALUTARE; INVESTIGARE ogni violazione.
- CONTROMISURE ADEGUATE rispetto al rischio.

.....Valutare, imparare, migliorare.

Conclusione

- Dall' 11 settembre 2001..ma non solo, si e' aperta una nuova era dove ogni rischio e' sempre più globale e condiviso tra continenti ed organizzazione diverse.

dove il concetto di ***"questo a noi non succede ne e' mai successo"*** e' ormai tramutato e dove l'elemento security in tutte le sue forme porterà a nuove regole e comportamenti atti a cambiare le definizione di rischio, prevenzione, protezione e modi di operare. In alcuni casi anche in modo paranoico.....

"Il mestiere del security manager" può aiutare!

Grazie per l'attenzione.