


ASPETTI ORGANIZZATIVI DELLA INFORMATION SECURITY AZIENDALE

CORRADO GIUSTOZZI

master universitario di secondo livello
Master in Gestione della Sicurezza
 Informatica per l'Impresa e la Pubblica Amministrazione

29 maggio 2010 Sapienza Università di Roma 1

Gli argomenti che tratteremo

- La “funzione sicurezza” in azienda
- Il concetto di business security
- I modelli organizzativi della sicurezza
- Casi di studio

29 maggio 2010 Sapienza Università di Roma 2

Una “nuova” funzione aziendale

- L'azienda moderna non si identifica solo coi suoi *asset* fisici, anzi il suo vero valore è nelle *informazioni* che gestisce
- Accanto alla responsabilità della “sicurezza industriale” (fisica), deve quindi esservi quella della *sicurezza delle informazioni*
- La sicurezza delle informazioni è qualcosa di più della sicurezza informatica, così come un sistema informativo è qualcosa di più di un sistema informatico

29 maggio 2010 Sapienza Università di Roma 3

Funzione sicurezza: i compiti (1/2)

- Protezione e prevenzione contro l'uso illecito o fraudolento:
 - accessi illegali al Sistema Informativo
 - estrazione o modifica di informazioni
 - sfruttamento abusivo di risorse
- Protezione e prevenzione contro il falso e la frode:
 - autenticazione dei soggetti, dei dati, dei documenti
 - certezza della legittimità delle operazioni
- Protezione e prevenzione contro incidenti, naturali o dolosi:
 - business continuity
 - disaster recovery

29 maggio 2010 Sapienza Università di Roma 4

Funzione sicurezza: i compiti (2/2)

- Protezione e prevenzione contro comportamenti illeciti o indesiderati:
 - attività improprie da parte del personale interno o esterno
 - adempimenti/adeguamenti normativi e legali (*compliance*)
- Mantenimento della *readiness*:
 - formazione e sensibilizzazione del personale
 - intelligence & awareness
- Gestione degli incidenti:
 - crisis management
- Audit e controllo:
 - controllo e garanzia dei processi di business (*governance*)
 - interpretazione e ricostruzione dei fatti (*forensic*)

29 maggio 2010 Sapienza Università di Roma 5

Da cosa ci si deve difendere

- Minacce esterne:
 - terzi estranei, curiosi od ostili
 - competitor sleali
 - organizzazioni criminali
 - hacker, cyberterroristi, tecnovandali, attivisti, ...
- Minacce interne:
 - errore, incuria, disattenzione, approssimazione, ...
 - dipendenti infedeli, insoddisfatti, vendicativi, ...
 - dipendenti curiosi, smanettoni, “furbi”, ...
 - personale esterno (consulenti, clienti, fornitori, ...)
- Minacce “pervasive”:
 - virus, worm, spam, *phishing*, ...

29 maggio 2010 Sapienza Università di Roma 6

I moderni rischi "inside"

- Attività che sono dei veri e propri reati e sono percepite come tali:
 - possesso e/o diffusione di materiale pedopornografico
- Attività che sono dei reati, ma non vengono sempre percepite come tali:
 - "scarico" di musica e film abusivi
- Utilizzo improprio delle risorse informatiche:
 - posta privata, chat, navigazione, ...
- Veri e propri illeciti verso i colleghi o l'azienda:
 - sniffing, lettura della email, sottrazione di credenziali, ...
- Attività ostili verso terzi esterni

29 maggio 2010

Sapienza Università di Roma

7

Protezione non è solo tecnologia

- Il "cordone sanitario" non è tutto!
 - firewall, antivirus, IDS, sono necessari ma non sufficienti
 - occorre un approccio integrato e multidisciplinare
- La sicurezza delle informazioni riguarda:
 - tecnologie
 - processi
 - persone
- La sicurezza delle informazioni si fa a livello:
 - fisico
 - logico
 - organizzativo

29 maggio 2010

Sapienza Università di Roma

8

Il concetto di *business security*

- La moderna tutela del business va affrontata in ottica globale e trasversale su tutte le funzioni aziendali e su tutti gli asset da proteggere
- Il concetto di business security comprende:
 - tutela del patrimonio aziendale
 - tutela dell'immagine aziendale
 - sicurezza fisica e logica (security)
 - tutela del know-how e del patrimonio informativo
 - tutela della privacy
 - informazione e formazione del personale
 - audit e controllo
 - awareness, readiness, intelligence
 - gestione degli incidenti e delle crisi

29 maggio 2010

Sapienza Università di Roma

9

Obiettivi di business security

- Conformità ai requisiti legali e normativi:
- Prevenzione della criminalità e degli illeciti
- Prevenzione di:
 - incidenti fortuiti e dolosi
 - frodi, truffe
 - atti di sabotaggio e vandalismo
 - atti di terrorismo
- Tutela dell'immagine e del patrimonio aziendale
- Supporto alle azioni di audit e controllo
- Formazione ed awareness del personale
- Partecipazione a tavoli istituzionali

29 maggio 2010

Sapienza Università di Roma

10

La funzione business security

- Dovrebbe fondarsi su di un'unità con competenze multidisciplinari, con funzione di indirizzo e coordinamento, e mandato di:
 - sviluppare linee guida ed indirizzi metodologici generali per la tutela del business aziendale
 - analizzare i problemi "dall'alto" con visione trasversale sui processi e sulle strutture aziendali
 - svolgere il compito di armonizzazione e condivisione delle esigenze delle singole strutture aziendali
 - elaborare e diffondere soluzioni omogenee, condivise e replicabili, alle problematiche individuate
 - redigere specifici regolamenti attuativi, di concerto con le strutture interessate

29 maggio 2010

Sapienza Università di Roma

11

Ruolo aziendale

- La funzione business security deve indirizzare problematiche di tipo:
 - organizzativo
 - legale
 - amministrativo
 - tecnologico
- Deve dunque potersi interfacciare con le strutture:
 - delle risorse umane
 - legali e amministrative
 - di audit e controllo
 - tecniche e di servizio
 - di produzione
 - di vigilanza

29 maggio 2010

Sapienza Università di Roma

12

Dove collocare la sicurezza?

- La sicurezza aziendale non deve essere:
 - nell'ufficio legale
 - nell'ufficio informatica
 - nell'ufficio risorse umane
 - nell'ufficio X...
- ...ma a riporto/staff del Top Management
- La business security consiste nel coordinare...
 - le funzioni tecniche
 - le funzioni legali
 - le funzioni organizzative
 - le funzioni di audit
- ...mediante una struttura trasversale di C³

29 maggio 2010

Sapienza Università di Roma

13

FINE

**ASPETTI ORGANIZZATIVI DELLA
INFORMATION SECURITY AZIENDALE**

master universitario di secondo livello
Master in Gestione della Sicurezza
Informatica per l'Impresa e la Pubblica Amministrazione



29 maggio 2010 Sapienza Università di Roma 14