

Sicurezza informatica in azienda: solo un problema di costi?

Silvano Marioni, CISSP

Manno, Centro Galleria 2
14 ottobre 2005



www.ated.ch

Parliamo di sicurezza informatica

- Quali minacce possono interessarci
 - Cosa c'è di nuovo
- Dove si deve investire in sicurezza informatica
 - Settori a rischio
 - Cosa proteggere
 - Da cosa proteggersi
- Quanto si deve investire in sicurezza informatica
 - In che modo proteggersi

Cosa c'è di nuovo

- Consolidamento del mondo digitale
 - Documenti digitali, Posta elettronica, ecc
- Maggiore visibilità delle informazioni
 - Sistemi distribuiti, reti, Internet, accesso remoto
- Integrazione dei sistemi
 - ERP, business-to-business, ecc.
- Nuovi requisiti legislativi
- Sono diminuiti i problemi acuti ma sono aumentati i problemi cronici

14 ottobre 2005

Silvano Marioni, CISSP - www.marioni.org

3

Cosa c'è di nuovo

- Non è sufficiente proteggere i singoli oggetti ma bisogna difendere un sistema complesso
- È necessaria un'attenzione continua basata sul monitoraggio e la manutenzione
- La sicurezza informatica non è una soluzione definitiva, un prodotto, un risultato

14 ottobre 2005

Silvano Marioni, CISSP - www.marioni.org

4

Settori a rischio

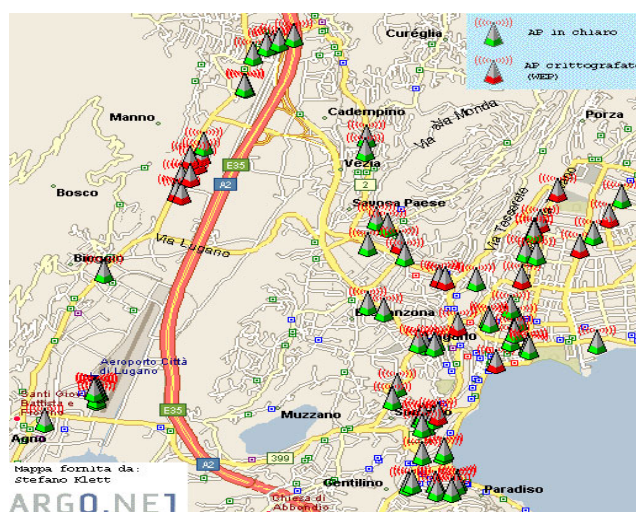
- Infrastrutture domestiche
 - A casa nostra, persone, famiglie, ...
- Infrastrutture aziendali
 - Aziende, fabbriche, banche, ...
- Infrastrutture pubbliche
 - Amministrazioni, enti pubblici, scuole, ...
- Infrastrutture critiche
 - Energia, sanità, trasporti, comunicazioni,

14 ottobre 2005

Silvano Marioni, CISSP - www.marioni.org

5

La tecnologia non basta



Reti wireless a Lugano

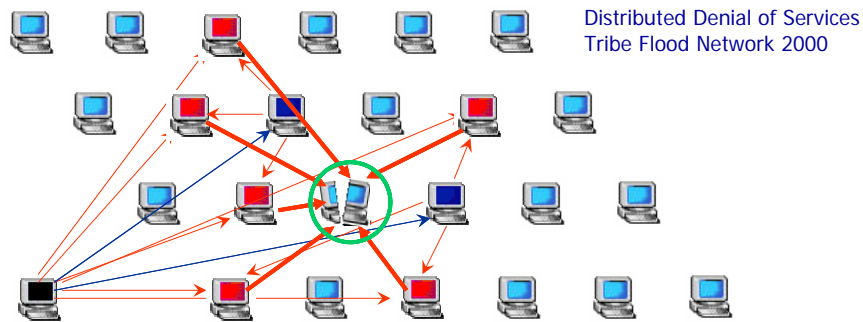
(dati 2004)

14 ottobre 2005

Silvano Marioni, CISSP - www.marioni.org

6

Non è più possibile ignorare



14 ottobre 2005

Silvano Marioni, CISSP - www.marioni.org

7

Cosa proteggere

- Sicurezza dei beni informatici dipende da:
 - Disponibilità
 - Quale sarebbe la produttività aziendale se i servizi informatici non fossero disponibili?
 - Integrità
 - Quali costi finanziari possono scaturire se le informazioni aziendali sono danneggiate?
 - Riservatezza
 - Ci sono informazioni riservate in azienda e come sono protette?

14 ottobre 2005

Silvano Marioni, CISSP - www.marioni.org

8

Da cosa proteggersi

Matrice dei rischi

	persone	processi	tecnologia	ambiente
interni	errori, uso illegale del software, frodi, spionaggio, negligenze	fughe di notizie, procedure incomplete, ruoli e responsabilità non chiari	guasti hardware, problemi software, accessi non autorizzati	incendio, animali nocivi,
esterni	ricatti, hacker, social engineering, accessi non autorizzati, phishing	problemi con fornitori e/o outsourcer, problemi legali o di regolamenti	cadute di corrente, problemi di telecomunicazione, virus, attacchi	allagamenti, terremoti, attentati

14 ottobre 2005

Silvano Marioni, CISSP - www.marioni.org

9

In che modo proteggersi

- Valutazione della sicurezza
 - Analisi del rischio e definizione delle contromisure
- Definizione del piano di sicurezza
 - Progetto del concetto globale di sicurezza

14 ottobre 2005

Silvano Marioni, CISSP - www.marioni.org

10

Valutazione della sicurezza

- Gli **obiettivi** principali della valutazione della sicurezza informatica sono:
 - Permettere alla direzione di capire se i processi di sicurezza informatica sono adeguati per proteggere le informazioni aziendali
 - Analizzare i processi di business e identificare i rischi di sicurezza per definire le protezioni con il miglior rapporto costo/efficacia.
 - Orientare l'azienda a gestire la sicurezza informatica in modo proattivo
 - Giustificare gli investimenti nel settore della sicurezza informatica

14 ottobre 2005

Silvano Marioni, CISSP - www.marioni.org

11

Valutazione della sicurezza

- La valutazione della sicurezza informatica permette di ottenere i seguenti **risultati**:
 - Fare un inventario delle risorse informative aziendali per definire la loro importanza e criticità
 - Identificare le applicazioni informatiche critiche e esaminare l'impatto per l'azienda nel caso di un loro mancato funzionamento
 - Analizzare i tipi di minacce e la probabilità di manifestazione in azienda
 - Esaminare le vulnerabilità comportamentali, organizzative e tecniche che riducono il livello di protezione aziendale

14 ottobre 2005

Silvano Marioni, CISSP - www.marioni.org

12

Piano di sicurezza

- Coinvolgimento della direzione
- Organizzazione della sicurezza
- Documenti di sicurezza
- Strumenti tecnici di protezione
- Formazione e informazione degli utenti
- Verifica della conformità

Coinvolgimento della direzione

- La sicurezza informatica non è solo un problema tecnico
- Non può essere delegata completamente agli informatici
- Aumentano le interazioni tra gli aspetti tecnici, giuridici e strategici

Organizzazione della sicurezza

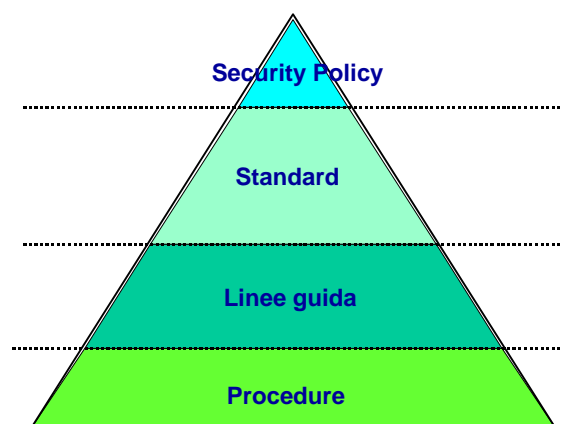
- **Classificazione delle informazioni**
 - Cosa proteggere
 - Schema di classificazione
 - Regole di classificazione
 - Ciclo di vita delle informazioni
- **Ruoli e responsabilità**
 - Proprietario dei dati
 - Custode dei dati
 - Utente
 - Revisore informatico

14 ottobre 2005

Silvano Marioni, CISSP - www.marioni.org

15

Documenti di sicurezza



14 ottobre 2005

Silvano Marioni, CISSP - www.marioni.org

16

Documenti di sicurezza - esempi

■ Security Policy

- « L'accesso alle informazioni aziendali è permesso ai soli utenti autorizzati »

■ Standard

- « Gli utenti devono avere un solo User ID e una password che va mantenuta segreta »

■ Linee guida

- « La lunghezza della password può variare tra 6 e 8 caratteri »

■ Procedure

- « Per i nuovi utenti lo User ID e la password sono definite dall'amministratore di rete. Dopo il primo collegamento l'utente è forzato a cambiare la password iniziale »

14 ottobre 2005

Silvano Marioni, CISSP - www.marioni.org

17

Strumenti tecnici di sicurezza

■ Protezione dei dati

- Autenticazione, cifratura, backup, ecc.

■ Messa a punto dei programmi di sistema

- Hardening, patch, change management, ecc.

■ Difesa perimetrale

- Firewall, reverse proxy, ecc.

■ Protezione dal software dannoso

- Antivirus, antispyware, firma dei programmi, ecc.

■ Verifica delle vulnerabilità

14 ottobre 2005

Silvano Marioni, CISSP - www.marioni.org

18

Formazione e informazione

- La **formazione** è importante per chi deve compiere delle scelte di tipo strategico, progettuale o tecnologico
 - Per riconoscere i rischi informatici e decidere le modalità di gestione del rischio
 - Per comprendere i principali aspetti tecnici e organizzativi della gestione della sicurezza
 - Per progettare le soluzioni di sicurezza in modo efficace e efficiente

14 ottobre 2005

Silvano Marioni, CISSP - www.marioni.org

19

Formazione e informazione

- L'**informazione** è importante per tutti gli utenti che utilizzano un sistema informatico
 - Per proteggere le informazioni aziendali da attacchi e malversazioni
 - Per avere garanzie della sicurezza utilizzando Internet e la posta elettronica
 - Per creare la consapevolezza dei nuovi rischi informatici

14 ottobre 2005

Silvano Marioni, CISSP - www.marioni.org

20

Verifica della conformità

- Revisione e IT governance
 - Per avere l'assicurazione che la sicurezza dei processi aziendali sia conforme a quanto stabilito dai regolamenti interni e dalla legislazione esistente

14 ottobre 2005

Silvano Marioni, CISSP - www.marioni.org

21

I pilastri della sicurezza

La tecnologia

È una componente importante per facilitare e automatizzare la protezione dei beni



14 ottobre 2005

Silvano Marioni, CISSP - www.marioni.org

22

I pilastri della sicurezza

Le persone

Sono l'elemento fondamentale per la sicurezza, per la capacità di comprendere, valutare e decidere in situazioni nuove o impreviste



14 ottobre 2005

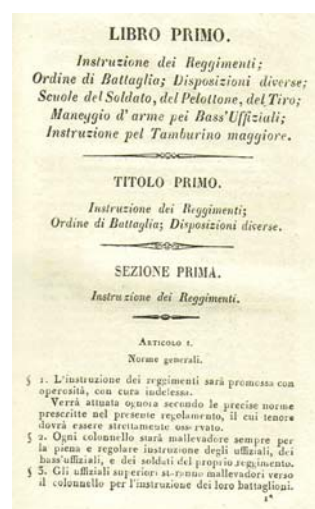
Silvano Marioni, CISSP - www.marioni.org

23

I pilastri della sicurezza

Le regole

Sono l'elemento essenziale per comunicare quali sono gli obiettivi e come bisogna comportarsi nei diversi momenti e nelle diverse situazioni

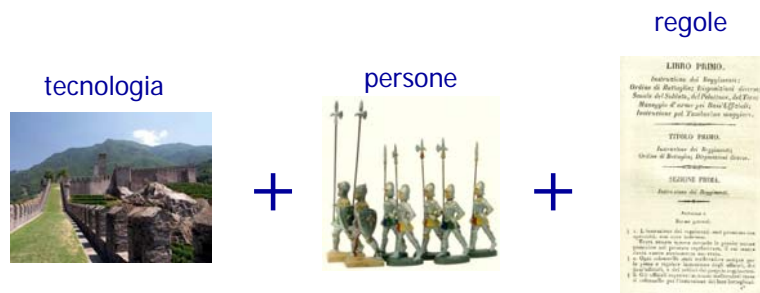


14 ottobre 2005

Silvano Marioni, CISSP - www.marioni.org

24

La protezione efficace



14 ottobre 2005

Silvano Marioni, CISSP - www.marioni.org

25

In conclusione

- La sicurezza non è solo un problema per specialisti
- La cultura della sicurezza deve essere diffusa in tutta l'azienda
- Deve essere condivisa tra persone con attività professionali e competenze diverse, per garantire una maggiore protezione delle risorse dell'azienda
- È fondamentale sia la formazione che l'informazione

14 ottobre 2005

Silvano Marioni, CISSP - www.marioni.org

26

Domande?



Grazie per l'attenzione

14 ottobre 2005

Silvano Marioni, CISSP - www.marioni.org

27