USERNET

Introduzione alla Sicurezza nell'e-business

Versione 1.5 del 21/05/01 19.15

INDICE

"***L'escalation dei pirati e l'ingenuità dell'e-business: Una rete globale pronta all'attacco***

Le accuse degli esperti americani contro le società IT, poco impegnate nello sviluppo dei sistemi di sicurezza nonostante l'aumento della pirateria informatica, arrivano dopo una settimana di casi eclatanti. Gli hacker hanno violato il sito finanziario della Western Union , copiando dati e clonando carte di credito di migliaia di clienti. Poi sono penentrati nella home-page dell'Opec per solidarizzare con le proteste contro il caro carburante. Infine hanno violato il sito della Ikea , società internazionale specializzata nell'arredamento della casa.
Mentre gli esperti, dal Global Privacy Summit , rilevano il calo di fiducia per mancanza di privacy e di sicurezza nei navigatori e nei venditori on line, l'ultimo allarme viene lanciato dal Cert Coordination Center e pubblicato da ZDnet: gli hacker di tutto il mondo sarebbero organizzati in una rete globale, pronti a sferrare un attacco unico contro Internet. Una missione non impossibile, visto che almeno un sito su tre dell'e-commerce non adotta programmi fire-wall, barriere informatiche contro i pirati.
Anche la Casa Bianca ha ammesso la sua impotenza di fronte alle incursioni dei pirati informatici e, in accordo con le indicazioni del General Accounting Office , ha chiesto aiuto ai manager e agli esperti della sicurezza delle grandi compagnie private."

Il Sole 24 Ore - 20 settembre 2000

"***Privacy on line, cala la fiducia dei navigatori I colossi delle vendite in rete: non è vero***

Gli e-shoppers non si fidano più della rete. Secondo gli esperti riuniti al Global Privacy Summit di Washington , cresce la diffidenza dei navigatori nei confronti del commercio on line, preoccupati per la mancanza di privacy e di sicurezza come riferisce ZDnet .
Il rapporto del Privacy Council, elaborato insieme al provider Privista , prende in esame un campione di 800 consumatori on line. Il 61% dicono di essere spaventati dalla facilità con cui, in rete, si può accedere alle informazioni personali e riservate. L'84% dei navigatori vuole inoltre essere esattamente informato delle condizioni di utilizzo dei propri dati al momento dell'acquisto.
Dati opposti a quelli di AmericanGreetings.com , colosso delle vendite on line dopo Amazon.com con oltre 8 milioni di visitatori in agosto: i consumatori interessati alla propria privacy sarebbero addirittura in calo. Su 100mila navigatori, soltanto 9 leggono il regolamento sull'utilizzo dei dati personali da parte del sito.
"La privacy viene utilizzata come un prodotto commerciale" accusa Gary Clayton, del Privacy Council. Per Andrew Shen, dell'Electronic Privacy Information Center , il caso di Amazon è esemplare: "E' stato ammesso chiaramente che i dati vengono utilizzati e venduti". Una pratica comune, ma non esplicita. La stessa Federal Trade Commission ha messo in atto un piano di protezione per i dati personali in rete, anche se sono proprio i siti federali i primi a non rispettare le leggi sulla privacy .
In Italia il ministero dell'Industria, dall'Osservatorio sull'e-commerce , ha chiarito più severamente le regole del commercio elettronico. Ai consumatori devono essere fornite tutte le possibili informazioni relative al prodotto e all'utilizzo dei dati personali."

Il Sole 24 Ore - 14 settembre 2000

1 Introduzione

Il presente documento ha un carattere introduttivo e intende illustrare alcune peculiarità delle tematiche di Sicurezza dell'Informazione nelle organizzazioni che avviano iniziative di e-business. In seguito all'esposizione di alcune definizioni e premesse fondamentali, verranno descritti un approccio aziendale alla Sicurezza e un metodo per l'implementazione e il mantenimento della Sicurezza Infine verranno trattate le particolarità, sempre sul tema Sicurezza, del commercio elettronico (e-commerce).

La sicurezza diventa a tutti gli effetti un elemento abilitante per il commercio elettronico. La poca sicurezza di un sistema di commercializzazione elettronica può offuscare anche un prodotto/servizio qualitativamente superiore. Il trattamento dei dati è quindi un elemento di maggiore competitività che diventa parte integrante dell'offerta dell'azienda.
Il timore dei clienti a lasciare i propri dati per transazioni monetarie è ancora elevato e rallenta il futuro dell'e-commerce. Tutto ciò è causato dalle innumerevoli notizie di siti poco sicuri. In questa rete i potenziali clienti sono timorosi anche perché non esiste nessun tipo di garanzia che il sito contattato sia sicuro.

La garanzia della Sicurezza dell'Informazione coincide con l'assicurare, secondo il British Standard BS7799:1999 – Parte 1, i requisiti di:

- **RISERVATEZZA**: l'informazione deve essere accessibile solo a chi è autorizzato a conoscerla. Le informazioni riservate devono essere protette sia durante la trasmissione che durante la memorizzazione. I dati memorizzati devono essere protetti mediante crittografia o utilizzando un controllo d'accesso, mentre per le informazioni riservate trasmesse è necessaria la crittografia.
- **INTEGRITA'**: le informazioni devono essere trattate in modo che siano difese da manomissioni e modifiche non autorizzate. Solo il personale autorizzato può modificare la configurazione di un sistema o l'informazione trasmessa su una rete. Per garantire l'integrità dei dati è necessario che il sistema sia preparato ad individuare eventuali modifiche apportate ai dati durante la trasmissione, sia intenzionalmente in seguito ad un attacco, sia involontariamente in seguito ad un errore di trasmissione.
- **DISPONIBILITA'**: l'informazione deve essere sempre disponibile alle persone autorizzate quando necessario. Una varietà di attacchi possono comportare la perdita o la riduzione parziale della disponibilità di un sistema informatico; alcuni di questi attacchi sono evitabili tramite contromisure automatizzate come l'autenticazione e la crittografia, mentre altri richiedono speciali azioni fisiche per prevenire o ridurre la perdita di dati o di risorse in un sistema distribuito.

1.1 La Sicurezza nell'e-business come problema strategico e strutturale

Un'efficace soluzione di security management dovrebbe nascere come parte integrante della strategia di business di una organizzazione. Lo sviluppo e la gestione della Sicurezza devono essere infatti visti come elementi in grado di sostenere il core business aziendale.
La gestione della Sicurezza necessiterà dello sviluppo di linee guida atte alla creazione delle pratiche di Sicurezza necessarie per supportare la strategia di business. Queste linee guida, definite politica per la Sicurezza, indirizzano lo sviluppo di un sistema di gestione della Sicurezza (definito ISMS = Information Security Management System), che verrà monitorato per verificarne la vulnerabilità ad attacchi e utilizzi impropri. Il risultato finale sarà la garanzia di riservatezza, integrità e disponibilità dei dati, sia all'interno, sia all'esterno dell'organizzazione.

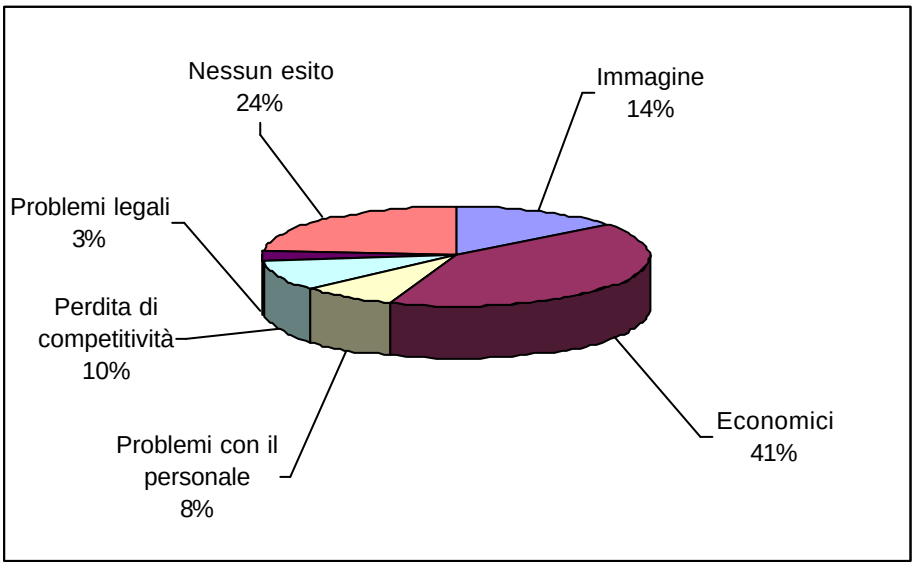
Nell'e-business, la Sicurezza dell'informazione deve essere considerata come un valore **strategico** e non come un costo. All'aumentare degli investimenti in e-business infatti aumenta inevitabilmente il grado di vulnerabilità[1] agli attacchi e, in un tale contesto, il costo maggiore consisterebbe nella NON-Sicurezza, ossia nella mancanza di politiche e misure di Sicurezza adeguate alle entità dei rischi esistenti.
Nella tabella seguente sono riportati i risultati di uno studio del CSI-FBI (Computer Security Institute – Federal Bureau Investigations) che riporta i costi dei cybercrimini negli USA:

Campione: 643 imprese – Cifre in mln di dollari.

	1997	**1998**	**1999**	**2000**
Furto di informazioni	20,04	33,54	42,49	66,70
Sabotaggio	4,28	2,14	4,42	27,14
Frodi Telecom	1,18	0,56	0,76	0,99
Intrusioni nei sistemi	2,91	1,63	2,88	7,10
Abuso della rete dall'interno	1,00	3,72	7,57	27,98
Frodi finanziarie	24,89	11,23	39,70	55,99
Blocco del servizio	n.d.	2,78	3,25	8,24
Virus	12,49	7,87	5,27	29,17
Accesso non autorizzato dall'interno	3,99	50,56	3,56	22,55
Intercettazioni attive	22,66	17,25	0,77	4,02
Furto di pc portatili	5,13	5,25	13,03	10,40
Altro	0,51	0,24	0,02	5,00
Totale perdite	**100,11**	**136,82**	**123,77**	**265,58**

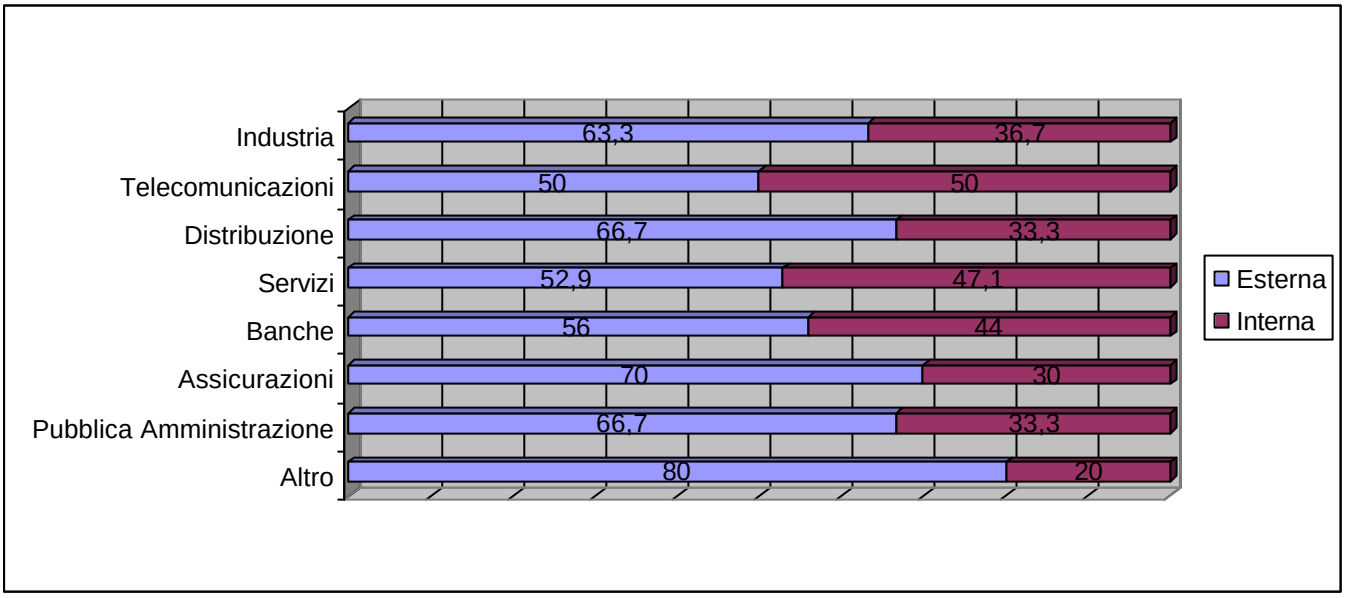
I danni causati dal cybercrime non sono solo economici, ma possono colpire l'immagine, il personale, gli aspetti legali fino ad arrivare alla perdita di competitività. Nel grafico è riportata in percentuale la tipologia dei danni (fonte OCI Osservatorio sui Crimini nell'ICT):

Tipologie di danni



Nell'e-business la Sicurezza è un fattore **strutturale** che si ripercuote sull'organizzazione aziendale nella sua globalità. È infatti indispensabile gestire in condizioni di Sicurezza l'intero sistema informativo aziendale salvaguardandone la riservatezza, l'integrità e la disponibilità. A tale fine devono essere impiegate tutte le risorse necessarie. Uno studio dell'OCI sull'origine degli attacchi rivela che in media il 36,8% degli attacchi provengono dall'interno dell'azienda a dimostrazione del basso livello organizzativo del sistema di sicurezza. Il grafico seguente dettaglia questo tema:

Provenienza dei danni



 -

1.2 Definizioni

Risorsa aziendale = tutto ciò che ha un valore per l'azienda: sistemi applicazioni e servizi. **Minaccia**: una potenziale causa di danni alle risorse aziendali. **Vulnerabilità**: una debolezza in una risorsa o in un gruppo di risorse che può essere sfruttata per arrecare danni alle risorse. **Rischio per la Sicurezza**: la possibilità che una certa minaccia sfrutti le vulnerabilità delle risorse aziendali per arrecare danno alle risorse stesse.
Attacco alla Sicurezza = qualsiasi azione volta a compromettere la Sicurezza dell'informazione posseduta da un'azienda. **Risk assessment** = analisi dei rischi: il processo di identificazione dei rischi per la sicurezza e di individuazione delle loro magnitudo. **Tecnica di Sicurezza**: una procedura, una regola o un meccanismo in grado di ridurre i rischi di Sicurezza. **Servizio di Sicurezza** = servizio che garantisce la Sicurezza dei sistemi di elaborazione e di trasmissione dati di un'organizzazione. I servizi di Sicurezza, allo scopo di contenere gli attacchi, utilizzano una o più tecniche di Sicurezza. **Rischio residuo**: il rischio per la Sicurezza che rimane in seguito all'attuazione di tecniche di Sicurezza.
Risk Management = gestione dei rischi: il processo di identificazione e di applicazione di tecniche di Sicurezza all'interno di un'organizzazione (ai sistemi, alle applicazioni e ai servizi) proporzionali ai rischi identificati.
ISMS = Information Security Management System: il sistema di gestione della Sicurezza dell'informazione può comprendere l'intera organizzazione aziendale o parti di essa che riguardano le risorse, i sistemi, le applicazioni, i servizi, le reti e le tecnologie utilizzate per elaborare, memorizzare e comunicare l'informazione. Un ISMS può comprendere tutti i sistemi informativi aziendali, alcuni di essi o un sistema informativo specifico. Un'organizzazione può definire diversi ISMS per differenti parti o aspetti del suo business. Per ogni ISMS occorre effettuare i processi di Risk Assessment e di Risk Management. Gli ISMS aziendali sono oggetto di certificazione di Sicurezza secondo gli standard BS7799.

2 Il Sistema di Gestione per la Sicurezza dell'informazione (ISMS)

Un sistema di gestione per la sicurezza dell'informazione è l'insieme delle infrastrutture e delle procedure atte a garantire i requisiti sopra descritti di riservatezza, integrità e disponibilità dei dati. Definire un sistema di gestione è di fondamentale importanza nell'ambito della sicurezza in quanto non è sufficiente progettare una soluzione tecnica sicura, ma è altrettanto importante mantenerne la sicurezza nel tempo.
La complessità dei sistemi informativi delle società che si presentano nell'ambito dell'e-business renderebbe le stesse a rischio se non fossero preparate a seguire le evoluzioni interne ed esterne della sicurezza.
La perdita economica e di immagine causate da una cattiva gestione della sicurezza può essere molto grave. Questo obbliga le società che vogliono entrare nell'e-business ad impostare un sistema di gestione per la sicurezza prima di tutto valido dal punto di vista organizzativo.

[BS 7799 – 2]

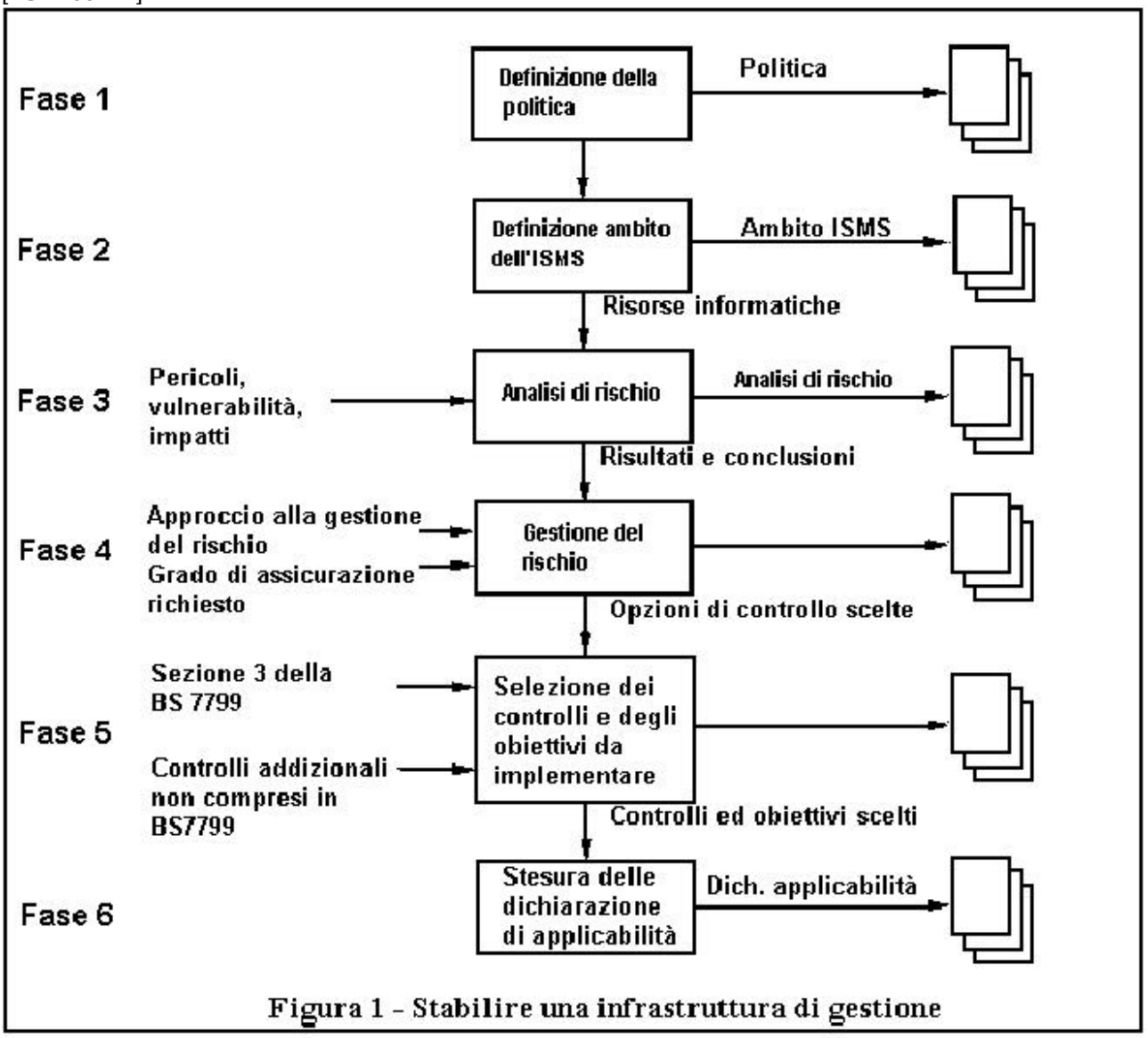


Figura 1 – Stabilire una infrastruttura di gestione

Per identificare e documentare le misure tecnico/organizzative (controlli) e i loro obiettivi devono essere intrapresi i seguenti passi (vd. Figura 1):

- Fase 1) Deve essere definita la politica di sicurezza informatica.
- Fase 2) Deve essere definito l'ambito del sistema di gestione della sicurezza informatica. Gli ambiti devono essere definiti in termini di caratteristiche dell'organizzazione, delle sue risorse, tecnologia e localizzazione.

Fase 3) Deve essere eseguita un'adeguata valutazione del rischio. La valutazione del rischio deve identificare i pericoli per le risorse, le vulnerabilità e gli impatti sull'organizzazione e deve determinare il grado di rischio.

Fase 4) Le aree di rischio da gestire devono essere identificate in base alla politica di sicurezza informatica dell'organizzazione e al grado di assicurazione richiesto.

Fase 5) Devono essere applicati controlli appropriati per l'implementazione da parte dell'organizzazione, e la loro selezione deve essere giustificata.

Fase 6) Deve essere preparata una dichiarazione di applicabilità. Devono essere documentati nella dichiarazione di applicabilità delle misure tecnico/organizzative selezionate i loro obiettivi e i motivi per la loro selezione.

3 L'approccio aziendale alla Sicurezza dell'informazione

L'approccio aziendale alla Sicurezza prevede l'integrazione tra vari aspetti **strategici**, **organizzativi**, **legali**, **tecnici** ed **economici**. Ciascuno di questi aspetti identifica attività specifiche di seguito elencate.

3.1 Aspetti strategici

- **Pianificazione di obiettivi aziendali.**

  La direzione deve definire gli obiettivi della società nell'ambito dell'e-business per consentire la definizione di piani di intervento sulla sicurezza.

  I piani devono essere tali da ottenere un livello di Sicurezza adeguato agli obiettivi stabiliti per le iniziative di e-business.

- **Definizione di budget aziendali.**

I budget aziendali devono essere proporzionali al livello di Sicurezza pianificato per gli obiettivi aziendali stabiliti.

- **Definizione della Politica per la Sicurezza dell'Informazione**

  È necessaria la formulazione di una Politica per la Sicurezza aziendale che indirizzi gli obiettivi, i comportamenti e i metodi per la Garanzia della Sicurezza dell'Informazione. Questa politica deve essere resa nota a tutta l'azienda.

3.2 Aspetti organizzativi

- **Costituzione di un Team per la Sicurezza che includa management e personale tecnico.**

  È necessaria la costituzione di un gruppo avente in carico lo sviluppo, la gestione e il mantenimento della Sicurezza delle informazioni e delle strutture aziendali.

- **Definizione di ruoli, ambiti e responsabilità**

  È necessaria la definizione dei ruoli, degli ambiti di azione e delle responsabilità dei singoli membri componenti il Team per la Sicurezza e di tutte le persone coinvolte operativamente nelle attività di e-business.

- **Definizione di adeguati programmi di formazione sia a livello tecnologico che a livello metodologico.**

  Formazione del personale aziendale e diffusione della cultura di Sicurezza

  È necessario pianificare percorsi formativi per il personale aziendale sulle problematiche legate alla Sicurezza e all'utilizzo dei sistemi informativi in condizioni di Sicurezza. È altresì indispensabile rendere accessibili le informazioni, le politiche e la documentazione tecnica relativa alla Sicurezza a tutto il personale, in modo da diffondere la cultura di Sicurezza in azienda.

  Formazione del personale tecnico addetto alla Sicurezza delle infrastrutture

  Il personale responsabile della Sicurezza dei sistemi e delle reti deve essere tecnicamente preparato e deve mantenersi aggiornato attraverso la partecipazione a convegni e corsi sullo stato dell'arte delle tematiche di Sicurezza.

- **Classificazione delle risorse.**

  Dati, sistemi e reti devono essere classificati in termini di riservatezza, integrità e disponibilità. L'organizzazione deve quindi documentare politiche e procedure per identificare una metodologia per l'assegnazione delle classi.

  È necessario identificare quale informazione è disponibile e quale parte di essa richiede opportuni livelli di protezione (conformità alle politiche di sicurezza).

- **Documentazione delle procedure per la Sicurezza dell'Informazione.**

  Devono essere descritte le procedure organizzative di attuazione degli indirizzi contenuti nella Politica per la Sicurezza. In particolare devono essere descritti i metodi per :

  - ✓ **Analisi dei rischi per le informazioni**
  - ✓ **Sicurezza fisica delle risorse HW/SW**
  - ✓ **Gestione della Configurazione HW**
  - ✓ **Gestione della Configurazione SW**
  - ✓ **Controllo anti-virus**
  - ✓ **Backup**
  - ✓ **Disaster Recovery**
  - ✓ **Utilizzo sicuro dei sistemi informativi**
  - ✓ **Utilizzo sicuro di Internet**
  - ✓ **Utilizzo sicuro della Posta Elettronica**
  - ✓ **Sicurezza dei sistemi operativi**
  - ✓ **Sicurezza dei server Web**
  - ✓ **Incident Management**
  - ✓ **Monitoraggio**

- **Applicazione delle procedure per la Sicurezza.**
  In seguito alla definizione delle politiche e delle procedure di Sicurezza sopra elencate, è necessaria la loro diffusione all'interno dell'organizzazione aziendale sia sotto forma di documentazione, che sotto forma di strumenti e metodi.

- **Verifica del rispetto delle procedure per la Sicurezza.**
  Sono necessari audit periodici allo scopo di verificare la validità e l'adeguatezza delle politiche. Tali audit assicurano la conformità dei sistemi alle rispettive politiche, mantenendo le risorse allineate alle mutate condizioni contestuali.

3.3 Aspetti legali

- **Conformità a leggi e normative esistenti nazionali e internazionali.**
  È necessario valutare la conformità delle politiche di Sicurezza alle leggi e alle normative esistenti nazionali e internazionali (es: DL 675/96). È altresì essenziale che l'implementazione (o l'assenza) di tecniche di Sicurezza in ogni sistema informativo non violi le leggi, i diritti civili o i contratti commerciali vigenti (es: DPR 513 10 novembre 1997).

3.4 Aspetti tecnici

Gli aspetti tecnici consistono nell'implementazione della Sicurezza fisica e logica dei sistemi informativi aziendali, secondo il seguente schema:

- **Sicurezza delle infrastrutture IT**

  Controllo degli accessi
  È necessario predisporre sistemi per il controllo dei permessi di accesso alle informazioni.

  Autenticazione
  È necessario implementare sistemi di autenticazione degli accessi, utilizzando tecnologie proporzionate alla classificazione di Sicurezza assegnata ai dati, ai sistemi o alle reti.

  Crittografia
  È necessario utilizzare opportune tecniche crittografiche per l'accesso autenticato alle informazioni e la trasmissione dati tramite i servizi intranet, extranet e internet. L'accesso alle informazioni e la trasmissione dati devono avvenire in modo sicuro sia dall'interno dell'azienda (accessi locali) che dall'esterno (accessi remoti).

  Antivirus e Backup
  È necessario predisporre sistemi antivirus e di backup per garantire la Sicurezza dei dati memorizzati nei sistemi nei confronti di attacchi portati da software pirata (virus) e da altri eventi accidentali che potrebbero comportarne la perdita.

- **Gestione delle vulnerabilità**

  Individuazione delle vulnerabilità
  È opportuno utilizzare strumenti software per condurre periodiche verifiche della Sicurezza delle reti e dei sistemi, alla ricerca di vulnerabilità.

  Analisi delle vulnerabilità
  È opportuno adottare sistemi utili a valutare i risultati della Vulnerability Detection, considerando i rischi delle vulnerabilità che sono state determinate.

  Azioni correttive
  È opportuno adottare sistemi utili ad intraprendere azioni correttive volte alla risoluzione delle problematiche evidenziate dalla Vulnerability Analysis.

- **Gestione delle minacce**

  Rilevazione delle intrusioni e reazioni

È necessario utilizzare strumenti (quali Auditing e Logging) per il monitoraggio delle reti e degli host critici, allo scopo di identificare segnali di attacchi o intrusioni e di intraprendere immediate azioni correttive.

Individuazione degli utilizzi non autorizzati (abusi)
È necessario che i sistemi siano protetti da utilizzi scorretti o volutamente negligenti da parte degli utenti.

Monitoraggio delle minacce
Un gran numero di minacce e di attacchi alla Sicurezza dei sistemi informativi sono riportati quotidianamente su siti Internet che provvedono alla generazione di Security Alert.

Risposta attiva
È necessario che i sistemi di Intrusion Detection siano in grado di intervenire automaticamente al presentarsi di segnali di pericolo, intraprendendo, ove necessario, azioni di difesa.

- **Automazione della gestione dei rischi**

Supporto alle decisioni aziendali
Sono necessari sistemi in grado di supportare opportune reazioni e azioni correttive immediate da parte di manager e amministratori al fine di proteggere le risorse esposte online.

Supporto alla gestione delle risorse
Sono necessari sistemi in grado di raccogliere informazioni di Sicurezza da molteplici sorgenti all'interno dell'organizzazione, di memorizzarle, di analizzarle e di correlarle allo scopo di permettere decisioni efficaci e precise sul miglioramento o sulla ridefinizione.

Supporto alla verifica di attuazione delle politiche di sicurezza aziendali
Sono necessari sistemi in grado di fornire informazioni utili al monitoraggio dell'effettiva attuazione delle varie politiche di Sicurezza aziendali.

3.5 Aspetti economici

- **Analisi dei costi.**
  È necessario effettuare un'analisi dei costi delle soluzioni di Sicurezza da adottare, tenendo presente che, come già evidenziato, il costo maggiore per un'azienda fortemente orientata alla rete e all'e-business consiste nella NON-Sicurezza.

- **Valutazione di impatto.**
  È necessario valutare l'impatto sul business aziendale delle misure di Sicurezza da adottare. Ad esempio, l'introduzione di misure e tecniche di Sicurezza avanzate (firewall, VPN, certificati digitali) potrebbe comportare la modifica di alcune procedure aziendali (ad esempio l'accesso remoto alle informazioni o l'invio di posta elettronica autenticata e riservata) con conseguente impatto economico dovuto all'aumento del numero di operazioni da svolgere da parte del personale durante la normale attività lavorativa di tutti i giorni.

- **Analisi dei rischi.**
  L'analisi dei rischi (risk assessment) deve evidenziare anche le ripercussioni economiche di eventuali attacchi alla Sicurezza delle risorse aziendali.

4 Sicurezza nel commercio elettronico (e-commerce)

L'e-business e, in particolare, l'e-commerce possono comportare l'utilizzo di scambio dati in formato elettronico (EDI, Electronic Data Interchange), posta elettronica e transazioni on-line attraverso reti pubbliche come Internet. Il commercio elettronico è quindi vulnerabile a una serie di minacce alla Sicurezza delle reti che possono portare ad attività fraudolenta, dispute contrattuali e rivelazione o modifica dell'informazione.
Al fine di proteggere il commercio elettronico da tali minacce devono essere adottate e implementate opportune tecniche e misure di Sicurezza.

Tra i vari metodi, oramai consolidati, per la garanzia della sicurezza dell'informazione ricordiamo:

- **AUTENTICAZIONE**: assicura che la fonte di un messaggio o di un documento elettronico sia identificata correttamente, con la garanzia che l'identità non sia falsa. La tecnica di autenticazione dipende dal sistema utilizzato. Nel caso di un singolo messaggio, la tecnica di autenticazione assicura che esso provenga effettivamente dalla sorgente autorizzata, mentre nel caso di interazione tra due o più host, l'autenticazione assicura che le entità coinvolte nell'interazione siano effettivamente chi dichiarano di essere.
- **NON-RIPUDIO**: richiede che né il mittente, né il destinatario di un messaggio possano negarne la trasmissione. Pertanto, quando un messaggio è inviato, il ricevente deve essere in grado di provare che il messaggio è stato effettivamente inviato dal mittente; quando il messaggio è ricevuto, il mittente deve poter provare che il messaggio è stato effettivamente ricevuto dal destinatario.
- **CONTROLLO DI ACCESSO**: è la facoltà di monitorare e limitare l'accesso da parte di un utente ad un host locale o ad un server remoto. Per ottenere questo controllo l'identità che prova ad accedere al server o alla stazione locale deve essere autenticata o identificata prima di ottenere i diritti di accesso alle risorse di rete.

Alcune considerazioni sulla Sicurezza nell'e-commerce sono [BSI 7799-1]:

1. ***Autenticazione***: quale livello di fiducia devono richiedere l'acquirente e il venditore sulle identità reciproche?

2. ***Autorizzazione***: chi è autorizzato a stabilire i prezzi, a divulgare o a firmare documenti commerciali importanti? Come fanno i partner commerciali a saperlo?

3. ***Processi di contratto e di offerta***: quali sono i requisiti di riservatezza, di integrità e di prova dell'invio e della ricezione di documenti fondamentali e di non ripudio dei contratti sottoscritti?

4. ***Informazioni sui prezzi***: quale livello di fiducia può essere posto sull'integrità della lista dei prezzi pubblicata e sulla riservatezza di accordi di vendita a prezzo ribassato?

5. ***Transazioni di ordini***: come vengono garantite la confidenzialità e l'integrità di ordini, di pagamenti, di dettagli relativi agli indirizzi di consegna e di ricevute di consegna?

6. ***Controlli***: quale grado di controllo è appropriato per verificare le informazioni per il pagamento fornite dal cliente?

7. ***Accordi***: quale forma di pagamento è più adeguata per evitare le frodi?

8. ***Ordini****:* quale protezione è richiesta per salvaguardare la riservatezza e l'integrità degli ordini e per evitare la perdita e la duplicazione delle transazioni?

9. ***Responsabilità****:* chi si fa carico del rischio di transazioni fraudolente?

Molte di queste questioni possono essere risolte mediante l'utilizzo di opportune tecniche crittografiche, tenendo anche in considerazione la conformità ai requisiti legali delle transazioni commerciali (come ad esempio la normativa per l'esportazione delle chiavi crittografiche).

Gli accordi di e-commerce tra partner commerciali devono essere supportati da un contratto scritto che impegni entrambe le parti sui termini di accordi concordati, compresi i dettagli relativi alle autorizzazioni precedentemente esposti. Potrebbero essere anche necessari ulteriori accordi relativi ai livelli di servizio e di valore aggiunto dei fornitori delle connessioni di rete.
I sistemi pubblici di commercio elettronico devono rendere noti ai clienti i propri termini commerciali.
È altresì necessario dare risalto alla capacità di reazione agli attacchi da parte degli host utilizzati per il commercio elettronico e alle implicazioni per la Sicurezza di ogni interconnessione di rete richiesta per la sua implementazione.

5 Conclusioni

Come si è visto, la Sicurezza e' un fattore strutturale e complesso che si ripercuote sull'organizzazione aziendale nella sua globalità e che richiede la definizione di politiche, procedure e linee guida oltre all'implementazione di adeguati sistemi e tecniche di Sicurezza e alla realizzazione di opportuni percorsi formativi per il personale aziendale.

In un'azienda di e-business la Sicurezza dell'informazione deve essere considerata come un valore strategico e non solo come un costo; in un'azienda fortemente orientata alla rete e al commercio elettronico il costo maggiore consisterebbe infatti nella NON-Sicurezza, ossia nella mancanza di politiche e misure di Sicurezza adeguate alle entità dei rischi esistenti.

Diventa quindi fondamentale riuscire ad avere un riscontro oggettivo del "livello" di Sicurezza e di affidabilità dei propri sistemi informativi. Tale riscontro oggettivo deve essere basato su standard internazionali autorevoli e universalmente riconosciuti e occorre che l'ISMS (Information Security Management System) aziendale sia valutato da un ente indipendente. Una certificazione autorevole e universalmente riconosciuta del proprio ISMS è importante per:

- **l'azienda stessa**: è interesse primario dell'azienda sapere se il proprio business è supportato da strumenti e risorse adeguate;
- **i partner commerciali**: la supply chain ha la forza dell'anello più debole; è quindi indispensabile che tutte le entità coinvolte siano adeguatamente affidabili;
- **i clienti**: un'azienda solida e certificata offre un livello di fiducia maggiore, sia per le transazioni on-line che per ogni altro aspetto commerciale.

USERNET – **U**nione per la **S**icurezza **E** la **R**iservatezza dei **NET**works – organizzazione apolitica e senza finalità di lucro che non svolge attività commerciale, propone un modello di riferimento basato su tre elementi fondamentali:

- la gestione organizzativa e qualitativa;
- il rispetto dei requisiti di legge per gli aspetti contrattuali e per la gestione dei dati (Privacy);
- la Sicurezza delle transazioni.

Il modello di Usernet si basa su riferimenti normativi internazionali (BS7799) e offre la possibilità di valutare, sulla base di criteri oggettivi, la Sicurezza e l'affidabilità dei sistemi informativi aziendali.

