

Infosecurity 2002

**Sistema di Gestione
della Sicurezza Informatica**

**IL VALORE DELLA CERTIFICAZIONE
SECONDO LA NORMA
BS 7799 - ISO 17799**

Luigi PAVANI

ICT Services Department Manager
RINA SpA



Tendenze

Fonte: IDC

- **Le Organizzazioni aumenteranno il livello di decentramento delle sedi fisiche e la soglia di difesa degli asset aziendali**
- **Diminuzione di viaggi per spostamento e aumento di utilizzo di mezzi di comunicazione via telefono, rete, web e video**
- **Maggiore attenzione e richiesta a livello individuale di sicurezza vs privacy e disponibilità ad accettare inconvenienti a fronte di più sicurezza**
- **Governo/Istituzioni Pubbliche ed aziende lavoreranno di più insieme sui temi della sicurezza per salvaguardare le infrastrutture critiche a livello paese**



Priorità per la sicurezza informatica

Fonte: IDC

OLD

- Sicurezza Fisica e Infosecurity separate
- Centro di costo opzionale
- Downtime
- Restrict Access
- Servers, PCs, Reti
- Business Unit Driven
- Internal Focus

NEW

- Integrazione tra infosecurity e Sicurezza Fisica
- Budget Obbligatorio
- Uptime
- Open Access
- Servers, PCs, PDA Reti e Mobile
- Corporate Mandate
- External Emphasis



Security Business Trends

La sicurezza si trasforma....

Fonte: IDC

-da una opzione che costa per l'azienda ad una **variabile critica** per le attività interne ed esterne per la salvaguardia degli asset aziendali
-da diverse tecnologie frammentate ad una **soluzione integrata (e gestionale)**
- ... da un intervento una tantum ad un **progetto continuo** e quotidiano di intelligence

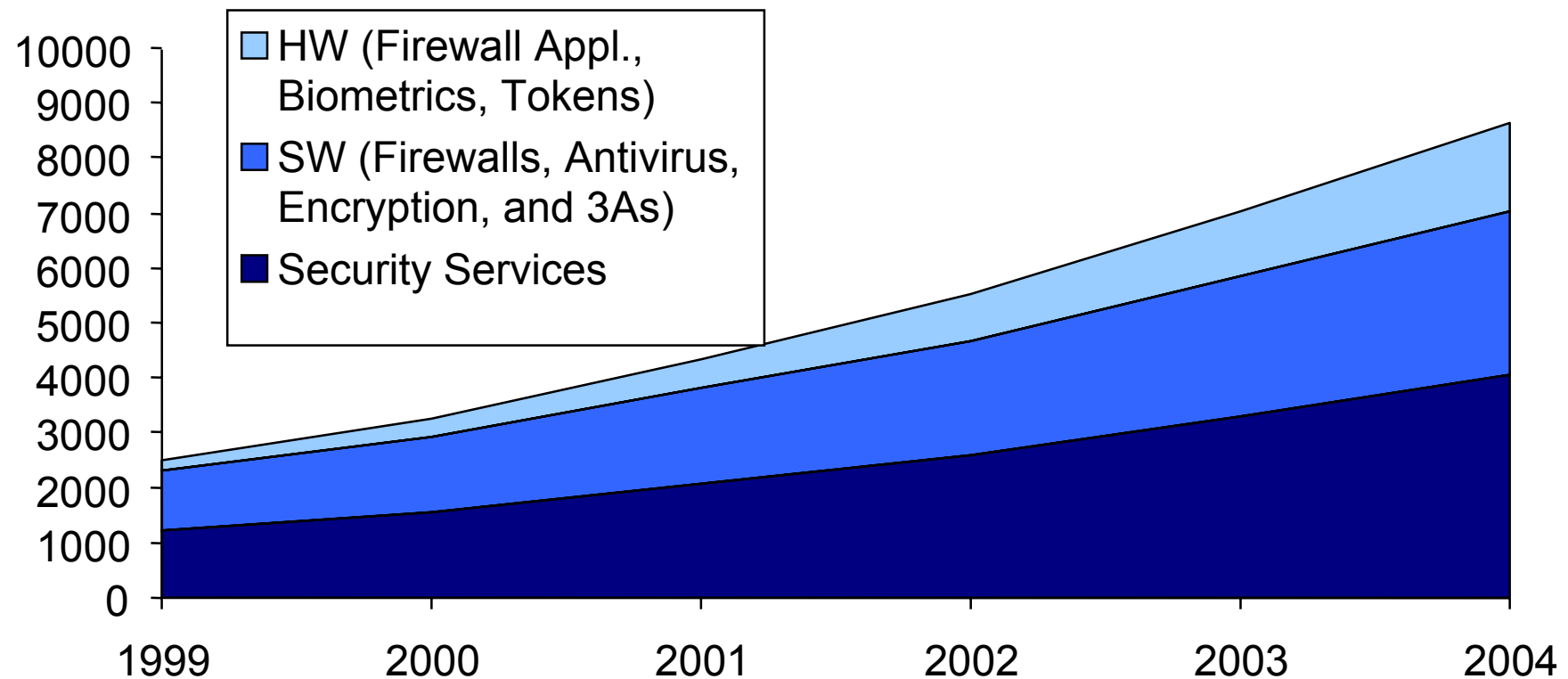


European Internet Security

Aggregated Forecast

Fonte: IDC

W. European Market for Internet Security by Submarkets, 1999-2004 (\$M)



Il contesto competitivo e la Certificazione



OBBLIGHI LEGALI (privacy)

- 675/96
 - art. 15: «i dati personali oggetto di trattamento devono essere custoditi e controllati, **anche in relazione alle conoscenze acquisite** in base al progresso tecnico, alla natura dei dati e alle specifiche caratteristiche del trattamento, in modo da ridurre al minimo, mediante l'adozione di idonee e preventive misure di sicurezza, i rischi di distruzione o perdita, anche accidentale, dei dati stessi, di accesso non autorizzato o di trattamento non consentito o non conforme alle finalità della raccolta»
 - DPR 318/99
 - misure minime di sicurezza



OBBLIGHI LEGALI (privacy)

- Responsabilità civile:
 - Art. 18: richiamo alla disciplina in materia di attività pericolose sancita dall'art. 2050 Codice Civile (-> ribaltamento onere della prova)
 - Art. 29: estesa ai "danni morali"
- Responsabilità penale
 - In caso di violazione delle misure del DPR 318/99
 - Può abbattersi su chiunque possa essere considerato tenuto a garantire la loro osservanza: in primis perciò, oltre che sulle persone che si occupano del trattamento o della gestione del sistema informativo e degli archivi, anche su coloro che amministrano e dirigono la società.



ONERI LEGALI

- Protezione del sistema informatico o telematico
 - art. 615-ter: «chiunque abusivamente si introduce in un sistema informatico o telematico **protetto da misure di sicurezza** ovvero vi si mantiene contro la volontà espressa o tacita di chi ha il diritto di escluderlo, è punito con la reclusione fino a tre anni»
- ! Sentenza per introduzione abusiva sul sito telematico del G.R.1 21/4/2000



ONERI LEGALI

- Protezione e-mail

- L'art. 616 punisce «chiunque prende cognizione del contenuto di una corrispondenza chiusa, a lui non diretta», ove «per "corrispondenza" si intende quella epistolare, telegrafica, telefonica, informatica o telematica ovvero effettuata con ogni altra forma di comunicazione a distanza»

! Il livello di segretezza attribuito dagli esperti in sicurezza agli scambi di e-mail non cifrata è quello della corrispondenza "aperta"



ONERI LEGALI

- Teoria della “**downstream liability**”
 - Tema scottante in discussione su cause civili per fenomeni di hacking
 - In genere un'organizzazione colpita non potrà essere risarcita da un hacker (che spenderà tutti suoi soldi per un legale)
 - L'organizzazione colpita potrà rivalersi “a valle” nei confronti dell'organizzazione che ha lasciato l'hacker entrare nei suoi sistemi, consentendogli l'attacco.
 - L'organizzazione chiamata in causa dovrà dimostrare di non essere stata negligente, di avere misure di sicurezza aggiornate ed adeguate.

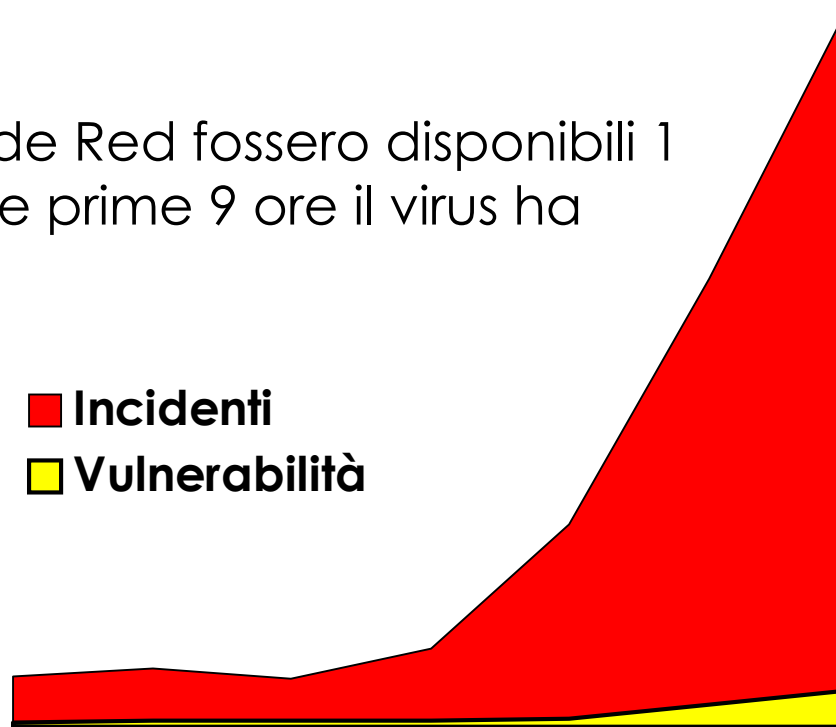


INTERNET SECURITY

Fonte: www.cert.org	1995	1996	1997	1998	1999	2000	Q1-Q2 2001
Incidenti	2412	2573	2134	3734	9859	21756	34754
Vulnerabilità	171	345	311	262	417	1090	1820

- Sebbene le patch per il virus Code Red fossero disponibili 1 mese prima dell'attivazione, nelle prime 9 ore il virus ha contagiato 250.000 server

■ Incidenti
■ Vulnerabilità



MINACCE DA INSIDER

installazione/uso di sw non autorizzato	78%
uso di risorse aziendali per comunicazioni /attività illegali o illecite (porn surfing, e-mail harassment)	60%
uso di risorse aziendali per profitto personale (scommesse, spam, gestione di personal e-commerce site, investimenti online)	60%
abuso di computer control access	56%
furto fisico, sabotaggio o distruzione intenzionale di computer equipment	49%
installazione/uso di hw/periferiche non autorizzate	47%
furto elettronico, sabotaggio o intenzionale distruzione/diffusione di dati/informazioni proprietari	22%
frode	9%



Fonte: True Secure - Predictive Systems

% aziende con risposta affermativa

MINACCE DA OUTSIDER

viruses/trojan/worms	89%
attacchi su bug di web server	48%
Denial of Service (Dos)	39%
buffer overflow attacks	32%
exploits dovuti a scripting/mobile code (acitveX, Java, javaScript, VBS)	28%
attacchi dovuti a protocol weakness	23%
attacchi dovuti a password non sicure	21%



Fonte: True Secure - Predictive Systems

% aziende con risposta affermativa

LE RISPOSTE DELLE AZIENDE

rafforzamento del perimetro di rete per prevenire intrusioni dall'esterno	4.31
sicurezza e disponibilità per siti web e/o operazioni di e-commerce	4.01
sicurezza di messaggi/e-mail	3.99
mettere in sicurezza gli accessi remoti per impiegati/telecommuters/utenti remoti	3.89
gestione centralizzata/correlazione di security policy/contromisure/alert data	3.79
prevenzione di abuso di accesso da parte di impiegati/insiders	3.66
altro	2.72



Fonte: True Secure - Predictive Systems

% aziende con risposta affermativa

GLI OSTACOLI

budget	3.55
mancaanza di training per gli utenti/consapevolezza per gli end-user	3.55
mancaanza di supporto della direzione	3.17
mancaanza di personale competente di sicurezza	3.08
mancaanza di policy di sicurezza interna	3.07
responsabilità poco chiare	3.04
technical challenges/complessità dei prodotti	3.00



Fonte: True Secure - Predictive Systems

% aziende con risposta affermativa

LE BAD PRACTICES

"La sicurezza si misura nel suo anello più debole"

- utilizzo di post-it per ricordarsi le password
- aggirare le misure di sicurezza (es. Disattivazione antivirus)
- lasciare i sistemi/documenti "unattended"
- aprire e-mail attachment
- utilizzo di password banali
- discorsi riservati in aree/locali pubblici
- applicazione poco rigorosa delle policy
- sottovalutazione dello staff (insider attacks)
- lentezza nell'update dei sistemi (patch)



Elementi della sicurezza

- Gli elementi che interagiscono nella sicurezza di una organizzazione sono:
 - il management
 - gli addetti ai sistemi (interni/esterni)
 - gli utenti (interni/esterni)
 - le informazioni
 - le apparecchiature Hardware/Software
 - le minacce in continuo divenire
 - l'evoluzione tecnologica



LA RISPOSTA GESTIONALE

Una risposta di tipo solamente tecnologico
(controllo accessi, protezione da virus/dos,..)
penalizza l'intero sistema di sicurezza
(tralascia "l'anello più debole")

La risposta gestionale (BS7799, ISO/IEC 17799)
parte da una visione globale della sicurezza

- Enterprise Security Management
- componenti fisica, logica, operativa,
legislativa ..,

focalizzandosi sugli aspetti **gestionali**.



Il contesto normativo volontario

La logica delle ISO 9000 ha generato standard normativi e gestionali affini:

Qualità

- ISO 9000:2000
- AVSQ'94
- QS 9000
- EN 729

Ambiente

- Regolamento EMAS CEE 1836/93
- ISO 14001 Sistemi di Gestione Ambientale
- ISO 14040 Ciclo di vita del prodotto (LCA)

Sicurezza dei dati

- ISO 17799



I principi

I principi di base di un SGSI sono:

- information security policy (volontà e supporto della direzione)
- allocazione delle responsabilità
- educazione, sensibilizzazione e training
- report degli incidenti
- business continuity management
- controlli necessari per assicurare che gli obiettivi posti sulla sicurezza siano raggiunti



Efficienza ed efficacia

- **Risk Analysis:** identificazione delle risorse da proteggere, dello scenario di minacce e vulnerabilità (interne all'impresa o esterne), calcolo del rischio, della probabilità del suo concretizzarsi, e dell'impatto sul business.
- **Risk Management:** definizione strategica del livello di rischio accettabile e conseguenti decisioni operative sulla gestione del rischio (riduzione, trasferimento, accettazione).

Ogni fase di questo processo richiede responsabilità definite e criteri di conduzione sistematici per assicurarne il controllo periodico, la ripetitività e la tracciabilità nel tempo.



SGSI: I benefici

- mantenersi aggiornati su minacce e vulnerabilità, gestirle in modo sistematico
- trattare incidenti e perdite in ottica di prevenzione e di miglioramento continuo del sistema
- sapere quando policy e procedure non sono implementate in tempo utile per prevenire danni
- implementare politiche e procedure di primaria importanza, in accordo con le “best practice” e un buon risk management



La Certificazione

- Occupando tale ruolo strategico, risulta evidente il beneficio di impostare un progetto di gestione della sicurezza con riferimento ad uno standard riconosciuto dal mercato.
- La certificazione BS7799 da parte del RINA rafforza la competitività e l'immagine dell'azienda.



Gli step progettuali

- **assessment iniziale:** valutare il livello di security di un sistema esistente. Parte dal presupposto che il valutatore non conosca per niente la situazione del valutato.
- **piano di adeguamento:** ha lo scopo di portare il sistema del cliente a un livello di security predeterminato.
- **assessment finale:** ha lo scopo di far subire al cliente un esame di certificazione simulato, con due obiettivi. Se il cliente non è ancora certificato, consentirgli di evidenziare gli errori e porvi rimedio *prima* dell'esame di certificazione vero e proprio; se il cliente è già certificato, consentirgli un *check up* di valutazione della situazione.
- **piano di mantenimento:** riguarda gli interventi periodici di verifica della situazione aziendale rispetto agli standard adottati e l'eventuale scostamento rispetto al valore prefissato
- **audit per la sicurezza,** a fronte di check list congiuntamente definite, per valutare il livello di applicazione della sicurezza
- **test di intrusione,** simulazione di attacchi esterni
- **certificazione:** ha lo scopo di certificare il cliente per la norma (o le norme) per cui desidera essere certificato.
- **formazione,** per fornire le competenze al personale



Offerta del RINA

Assessment Iniziale

- individuazione dell'ambito gestionale per la sicurezza esistente:
 - stato dell'organizzazione
 - definizione delle responsabilità
 - livello di sicurezza delle sedi aziendali
 - modalità di gestione delle operazioni e delle comunicazioni
- censimento degli asset aziendali
- individuazione di criteri per la valutazione della strategicità degli asset aziendali
- criteri di valutazione del rischio ed ipotesi di rischi prioritari legati agli asset strategici
- individuazione dei requisiti di sicurezza
- valutazione del livello di soddisfacimento dei requisiti di sicurezza (*gap analysis*)
- ipotesi di modalità gestionali dei rischi
- selezione di possibili obiettivi dei controlli ed individuazione di criteri per la selezione e l'implementazione dei controlli

Audit per la sicurezza

permettono di verificare con la migliore attendibilità l'applicazione dei provvedimenti presi, ad esempio, per la conformità a:

- standard riconosciuti de facto o internazionali
- disposizioni interne derivanti dagli obblighi di legge
- performance o gestione di un servizio in outsourcing, avanzamento delle commesse, conformità a contratti



Formazione

- La sicurezza non si costruisce certo solo acquistando “box e tools”, strumenti che invece devono essere amministrati e soprattutto utilizzati correttamente
- L'elemento umano è quindi centrale per la sicurezza delle informazioni
- Per questo eroghiamo la formazione adatta ai vari livelli di competenza e responsabilità:
 - ✓ per il management
 - ✓ per gli utenti
 - ✓ per il personale tecnico



La certificazione BS7799

- La certificazione del proprio sistema di sicurezza delle informazioni costituisce:
 - **un forte asset competitivo in termini di autorevolezza (valutazione di una terza parte indipendente)**
 - **il naturale ed autorevole coronamento di un percorso di crescita organizzativa e tecnologica**
- > viene percepita e compresa dal mercato come uno strumento utile al business



I benefici diretti

- **valorizzazione degli investimenti**
- **rafforzamento dell'immagine aziendale**
- **segnale forte verso un mercato sempre più sensibile alla problematica sicurezza**
- **fattore di vitalità per il sistema di gestione stesso, assicurandone**
 - efficienza/efficacia
 - rispondenza ai requisiti legali e contrattuali
 - finalizzazione degli investimenti



I benefici indiretti

- ◆ influenza positiva sul prestigio aziendale, sull'immagine, sui parametri di goodwill esterna fino ad una possibile incidenza sulla valutazione patrimoniale dell'azienda o delle quote azionarie
- ◆ valenza dello strumento nella gestione delle informazioni, in termini di risk management tramite la definizione di ruoli, responsabilità e modalità operative che mettono in sicurezza l'azienda anche rispetto ai parametri di legge (a salvaguardia del management)
- ◆ riduzione dei costi di gestione della sicurezza e vantaggi competitivi legati al miglioramento dell'efficienza dei processi
- ◆ l'adozione di un sistema di misurazione completo e bilanciato per valutare le performance nella sicurezza e suggerire aggiunte, miglioramenti
- ◆ miglioramento delle ROI sugli investimenti informatici dovuto ad una focalizzazione mirata di tali investimenti alla luce dell'analisi e della valutazione dei rischi

CONCLUSIONI

La ricerca scientifica e tecnologica hanno messo a punto una serie di strumenti e metodologie che, se correttamente adottati, consentono di ridurre al minimo le minacce alla sicurezza delle informazioni

Tecnologie, sistemi, infrastrutture, applicativi devono essere gestiti, aggiornati, mantenuti adeguati per far fronte a minacce accidentali o intenzionali che evolvono nel tempo, provenienti dall'interno o dall'esterno dell'azienda.

La norma BS7799 propone gli step operativi per un buon risk management, con il vantaggio della standardizzazione.

