Versione integrale in PDF (18 pp) con 2,5 ore di corso multimediale

Materiale didattico validato da AICA Certificazione EUCIP IT Administrator
Modulo 5 - IT Security
Sicurezza informatica

"AICA Licenziataria esclusiva in Italia del programma EUCIP (European Certification of Informatic Professionals), attesta che il materiale didattico validato copre puntualmente e integralmente gli argomenti previsti nel Syllabus IT Administrator e necessari per il conseguimento della certificazione IT Administrator IT Security. Di conseguenza AICA autorizza sul presente materiale didattico l'uso del marchio EUCIP, registrato da EUCIP Ltd e protetto dalle leggi vigenti"

Riferimento Syllabus 2.0 (curriculum ufficiale AICA)

5.1.1 Concetti di base

5.1.1.1 sapere quali sono i principali aspetti della sicurezza delle informazioni: riservatezza e integrità

(la numerazione dei punti di riferimento al Syllabus comincia con 5 perché si riferisce al quinto modulo della certificazione IT Administrator complessiva. Il quinto modulo riguarda la sicurezza informatica)

▶ Introduzione alla sicurezza delle informazioni

Diventate esperti di sicurezza con PC Open

Inizia il primo corso di taglio professionale destinato al conseguimento di una certificazione ufficiale, riconosciuta in tutta Europa. La certificazione fa parte di un nuovo filone denominato EUCIP (European Certification of Informatics Professionals) e si chiama IT Administrator – Sicurezza Informatica. *Il corso si articola in tre elementi: un articolo sulla rivista, un articolo, molto più esteso in formato PDF e un corso multimediale completo su CD e DVD* di Giorgio Gobbi

Obiettivo del corso IT Administrator – Sicurezza Informatica
Fornire al lettore familiarità con i vari modi di proteggere i dati sia su un singolo PC sia in una LAN connessa a Internet. In particolare, metterlo nelle condizioni di proteggere i dati aziendali contro perdite, attacchi virali e intrusioni. Inoltre, metterlo nelle condizioni di conoscere e utilizzare i programmi e le utility più comuni destinati a tali scopi.

La sicurezza delle informazioni è un'esigenza che ha accompagnato la storia dell'uomo fin dalle antiche civiltà. Oggi ci preoccupiamo di mantenere riservate le informazioni personali, militari e d'affari. Nel V secolo a.C. gli spartani inviavano gli ordini ai capi militari tramite messaggi scritti su una striscia di cuoio che, avvolta su un bastone (lo scitale) di un diametro ben preciso, permetteva di leggere il testo in chiaro lungo il bastone. Giulio Cesare cifrava i messaggi sostituendo ogni lettera con quella che nell'alfabeto segue di qualche posizione. La crittografia, cioè la scienza della scrittura segreta, ha avuto una progressiva evoluzione nel corso dei secoli, fino ai rapidi sviluppi teorici e tecnologici impressi dalla seconda guerra mondiale, che permisero la decifrazione dei codici giapponesi e tedeschi da parte degli alleati.

Oggi buona parte del pianeta vive nella società dell'informazione, basata cioè sull'uso delle informazioni come parte integrante delle attività umane. Pertanto, la sicurezza delle informazioni è diventata una componente della sicurezza dei beni in generale, o security, e non si limita alle tecniche per nascondere il contenuto dei messaggi. Qualunque programma che si occupi di preservare la sicurezza delle informazioni, persegue, in qualche misura, tre obiettivi fondamentali: la disponibilità, l'integrità e la riservatezza delle informazioni.

La **disponibilità** è il grado in cui le informazioni e le risorse informatiche sono accessibili agli utenti che ne hanno diritto, nel momento in cui servono. Questo significa che sistemi, reti e applicazioni hanno le capacità necessarie a fornire il livello di servizio e le prestazioni richieste e che, in caso di guasto o di eventi distruttivi, sono pronti gli strumenti e le procedure per ripristinare l'attività in tempi accettabili. Per impedire l'inaccessibilità delle informazioni, si deve preservare la disponibilità delle condizioni ambientali (energia, temperatura, umidità, atmosfera, ecc.) e delle risorse hardware e software a fronte sia di problemi interni (guasti, errori, blackout, disastri e altro), sia di attacchi esterni, per esempio provenienti da Internet, volti a impedire o a ridurre l'accessibilità ai sistemi e alle informazioni. Sistemi di backup locale e remoto, ridondanza dell'hardware e degli archivi, firewall e router configurati per neutralizzare attacchi DoS (denial of Service), sistemi di climatizzazione, gruppi di continuità, controllo dell'accesso fisico, monitoraggio delle prestazioni sono alcuni degli strumenti che servono per mantenere la disponibilità.

L'**integrità** è il grado di correttezza, coerenza e affidabilità delle informazioni e anche il grado di completezza, coerenza e condizioni di funzionamento delle risorse informatiche. Per l'hardware e i sistemi di comunicazione, l'integrità consiste di fattori come elaborazione corretta dei dati, livello adeguato di prestazioni e corretto instradamento dei dati. L'integrità del software riguarda fattori come la completezza e coerenza dei moduli del sistema operativo e delle applicazioni e la correttezza dei file critici di sistema e di configurazione.

Per le informazioni, l'integrità viene meno quando i dati sono alterati, cancellati o anche inventati, per errore o per dolo, e quando si perde, per esempio in un database, la

I contenuti delle 8 lezioni

In collaborazione con: Check Point SOFTWARE TECHNOLOGIES LTD. We Secure the Internet.

Lezione 1: *Informazioni generali*
Lezione 2: *Crittografia*
Lezione 3: *Autenticazione e controllo degli accessi*
Lezione 4: *Disponibilità*
Lezione 5: *Codice maligno*
Lezione 6: *Infrastruttura a chiave pubblica*
Lezione 7: *Sicurezza della rete*
Lezione 8: *Aspetti sociali, etici e legali della sicurezza informatica*

IT Administrator comprende sei moduli:

1 Hardware del PC (PC Hardware)
2 Sistemi operativi (Operating Systems)
3 Reti locali e servizi di rete (LAN and Network Services)
4 Uso esperto delle reti (Network Expert Use)
5 Sicurezza informatica (IT Security)
6 Progettazione reti (Network Design)

L'argomento di questo corso è il modulo 5 della certificazione EUCIP IT Administrator, dedicato espressamente alla sicurezza informatica. Il modulo 5 garantisce comunque il diritto a una certificazione a sé stante.

coerenza tra dati in relazione tra loro (per esempio i record coinvolti in una transazione).

Procedure di manutenzione e diagnosi preventiva, hardware e software per la rilevazione e prevenzione di accessi illeciti, attacchi virali e intrusioni, applicazioni che minimizzano errori logici e formali di data entry, accesso ristretto alle risorse critiche e controllo degli accessi sono alcuni degli strumenti utili a preservare l'integrità delle informazioni e delle risorse.

Anche le tecniche di hashing (calcolo di un numero di lunghezza fissa a partire da un qualsiasi messaggio o documento) sono usate per verificare che le informazioni non vengano alterate per dolo o per errore (anche di trasmissione).

La **riservatezza** consiste nel limitare l'accesso alle informazioni e alle risorse informatiche alle sole persone autorizzate e si applica sia all'archiviazione sia alla comunicazione delle informazioni. Un'informazione è composta generalmente di più dati in relazione tra di loro, ciascuno dei quali non necessariamente costituisce un'informazione. Il nome e il numero di conto corrente di una persona, separati, non sono informazioni; è la combinazione dei due dati che costituisce l'informazione.

La riservatezza dell'informazione può essere quindi garantita sia nascondendo l'intera informazione (per esempio con tecniche di crittografia) sia nascondendo la relazione tra i dati che la compongono. La riservatezza non dipende solo da strumenti hardware e software; il fattore umano gioca un ruolo chiave quando vengono ignorate le elementari regole di comportamento: tenere le password segrete, controllare gli accessi a reti e sistemi, rifiutare informazioni a sconosciuti (anche quando affermano di essere tecnici della manutenzione), cifrare i documenti e i messaggi riservati e così via.

Possiamo aggiungere altri due obiettivi di sicurezza che possono essere considerati un'estensione dell'integrità delle informazioni, applicata a eventi più complessi come l'invio di un messaggio o una transazione. L'autenticità garantisce che eventi, documenti e messaggi vengano attribuiti con certezza al legittimo autore e a nessun altro. Il non ripudio impedisce che un evento o documento possa essere disconosciuto dal suo autore. Queste due caratteristiche trovano applicazione nella firma digitale, che utilizza tecniche di hashing e crittografia per garantire che un documento resti integro e provenga da un autore univocamente identificato.

Gestione del rischio

Per esaminare i rischi connessi ai vari aspetti di sicurezza delle informazioni, iniziamo introducendo i termini del discorso: beni da difendere, obiettivi di sicurezza, minacce alla sicurezza, vulnerabilità dei sistemi informatici e impatto causato dall'attuazione delle minacce.

Beni

Un bene è qualsiasi cosa, materiale o immateriale, che abbia un valore e debba quindi essere protetta. Nel campo della sicurezza delle informazioni, tra i beni di un'azienda ci sono le risorse informatiche, il personale (utenti, amministratori, addetti alla manutenzione), le informazioni, la documentazione e l'immagine aziendale. Per un individuo, i beni comprendono non solo risorse informatiche, informazioni e mezzi di comunicazione, ma anche le informazioni personali e la privacy.

Per esempio, se un attacco via Internet causa a un'azienda il furto di informazioni riservate, magari relative alle carte di credito dei clienti, i beni colpiti sono molteplici: le informazioni, l'immagine, la reputazione, la stessa continuità operativa. Un altro esempio è il defacing, ovvero l'alterazione di un sito web per rovinare l'immagine del proprietario; è una forma di vandalismo che colpisce sia le informazioni sia l'immagine dell'azienda o persona titolare.

A livello personale, la privacy degli individui è minacciata da più parti: aziende che non proteggono adeguatamente le informazioni in loro possesso, applicazioni che trasmettono via Internet dati personali, software maligno che spia le abitudini degli utenti (acquisti, navigazione Internet ecc.) o che altera la navigazione Internet a scopo di truffa o furto di informazioni.

I beni possono essere distinti in beni primari, quelli che hanno valore effettivo, e beni secondari, che servono per proteggere i beni primari. Un esempio di bene secondario è la password che permette di accedere a un computer, a una rete, ai dati archiviati e a Internet. La password in sé non ha alcun valore, ma è un'informazione che permette a un altro utente o a un estraneo di accedere ai beni primari (sistemi, periferiche, reti, archivi) e di eseguire operazioni a nome dell'utente titolare della password, che ne sarà ritenuto responsabile. La password, bene secondario, assume un'importanza paragonabile a quella degli archivi e delle attrezzature hardware/software, bene primario a cui la password dà accesso. Lo stesso vale per i dispositivi di identificazione e autenticazione, come le Smart Card. Se la scheda viene utilizzata da qualcuno che si è procurato il corrispondente PIN (Personal Identification Number), il titolare della scheda sarà ritenuto responsabile dell'utilizzo fino alla denuncia di furto o smarrimento.

Altri esempi di beni secondari sono le attrezzature che permettono all'hardware di funzionare con continuità e sicurezza: gruppi di continuità, condizionatori, alimentatori e altri componenti ridondanti e così via. I beni secondari, in quanto investimento preventivo per mantenere alta la disponibilità dei servizi informatici, rappresentano un costo ampiamente inferiore rispetto al rimedio a situazioni non previste.

Obiettivi

Gli obiettivi di sicurezza sono il grado di protezione che si intende predisporre per i beni, in termini di disponibilità, integrità e riservatezza. Per definire gli obiettivi, si classificano i beni in categorie e si assegnano i criteri di sicurezza da applicare. Ci sono beni, come le password e i numeri di identificazione, che hanno più requisiti di riservatezza che

Alcuni beni da proteggere

- Hardware (sistemi e reti)
- Software
- Firmware
- Dati e informazioni
- Personale
- Documentazione
- Fondi
- Apparecchiature di controllo ambientale
- Immagine e reputazione aziendale
- Capacità operativa

5.1.2 Gestione del rischio

5.1.2.1 conoscere i principali elementi coinvolti nella valutazione del rischio (valore dell'informazione, vulnerabilità, minaccia, rischio, impatto, violazione, livello di rischio).

non problemi di integrità e disponibilità. Al contrario, le informazioni contabili di una banca che esegue transazioni on line hanno requisiti di disponibilità, integrità e riservatezza. Le informazioni pubblicate sul sito web di un'azienda richiedono disponibilità e integrità (per esempio per impedire il defacing), ma non certo riservatezza.

La selezione degli obiettivi in base al tipo di protezione richiesto dai beni, permette un approccio concreto e scalabile in base alle priorità e alle risorse disponibili. In assenza di una mappa di ciò che è urgente e importante da proteggere, si tende a improvvisare o a voler proteggere tutto, salvo poi mancare anche gli obiettivi minimi quando il costo preventivato supera di gran lunga le disponibilità.

Minacce

Una minaccia è un'azione potenziale, accidentale o deliberata, che può portare alla violazione di uno o più obiettivi di sicurezza. Le minacce possono essere classificate secondo la loro origine: naturale, ambientale o umana. Per esempio, un allagamento dovuto a forti piogge è una minaccia accidentale di origine naturale che ha un impatto sulla sicurezza, visto che può interrompere la disponibilità dei servizi informatici. Un cavallo di Troia installato all'apertura di un allegato di posta elettronica infetto, è una minaccia deliberata di origine umana e coinvolge tutti gli obiettivi di sicurezza: il computer può cadere sotto il controllo esterno e non essere più completamente disponibile per il suo proprietario (disponibilità), le sue informazioni possono essere alterate e cancellate (integrità) e dati da non divulgare (password, informazioni personali, informazioni sensibili aziendali) possono essere letti da estranei (riservatezza). Una rete wireless che opera senza protezione (a partire dalla cifratura delle comunicazioni) può essere intercettata o, perlomeno, usata per l'accesso a Internet, magari per operazioni illegali riconducibili all'indirizzo IP (e quindi alla responsabilità) del titolare della rete. In questo caso gli obiettivi violati coinvolgono la riservatezza, la disponibilità e potenzialmente anche l'integrità.

L'entità che mette in atto la minaccia viene chiamata agente. Esempi di agenti di minaccia sono un intruso che entra in rete attraverso una porta del firewall, un processo che accede ai dati violando le regole di sicurezza, un tornado che spazza via il centro di calcolo o un utente che inavvertitamente permette ad altri di vedere le password.

Vulnerabilità

Mentre una minaccia è sempre portata da un agente esterno (fenomeno naturale o intervento umano), una vul-

Esempi di minacce

(**D** = deliberata, **A** = accidentale, **E** = ambientale)

Minaccia	D	A	E
Terremoto			x
Inondazione		x	x
Uragano			x
Fulmine			x
Bombardamento	x	x	
Incendio	x	x	
Uso di armi	x	x	
Vandalismo	x		
Furto	x		
Blackout		x	
Linea elettrica instabile		x	x
Guasto climatizzatore		x	
Temperatura alta o bassa	x	x	x
Umidità eccessiva	x	x	x
Polvere			x
Radiazioni elettromagnetiche			x
Guasto hardware		x	
Uso improprio delle risorse		x	x
Errori software	x	x	
Uso non autorizzato supporti di memoria		x	
Deterioramento supporti di memoria			x
Errori degli utenti	x	x	
Errori del personale operativo		x	x
Errori di manutenzione	x	x	
Accesso illegale alla rete	x		
Uso illegale di password	x		
Uso illegale del software	x		
Indirizzamento illecito messaggi	x		
Software dannoso	x	x	
Installazione/copia illegale di software	x		
Interruzione servizio provider Internet		x	
Interruzione servizio hosting web		x	
Errori di trasmissione			x
Traffico eccessivo	x	x	
Intercettazione in rete		x	
Infiltrazione in rete	x		
Analisi illecita del traffico	x		
Carenze di personale			x

Esempi di vulnerabilità

Infrastruttura
Mancanza di protezione fisica
Mancanza di controllo degli accessi
Linea elettrica instabile
Locali soggetti ad allagamento

Hardware e impianti
Mancanza di sistemi di backup
Suscettibilità a variazioni di tensione
Suscettibilità a variazioni di temperatura
Suscettibilità a radiazioni elettromagnetiche
Programma di manutenzione insufficiente

Comunicazioni
Linee di comunicazione non protette
Uso di password in chiaro
Traffico wireless non cifrato
Presenza di linee dial-up
Libero accesso ai dispositivi di rete

Documentazione
Locali non protetti
Carenza di precauzioni nell'eliminazione
Assenza di controllo nella duplicazione

Software
Complessità interfaccia applicazioni
Mancanza autenticazione utente
Mancanza logging accessi
Errori software noti
Password non protette
Cattiva gestione password
Diritti di accesso scorretti
Uso del software incontrollato
Sessioni aperte senza presenza utente
Assenza di backup
Carenza nella dismissione dei supporti

Personale
Personale insufficiente
Procedure reclutamento inadeguate
Personale esterno incontrollato
Addestramento di sicurezza inadeguato
Uso improprio o scorretto hardware/software
Carenza di monitoraggio

nerabilità è un punto debole del sistema informatico (hardware, software e procedure) che, se colpito o sfruttato da una minaccia, porta alla violazione di qualche obiettivo di sicurezza. Una vulnerabilità presenta due caratteristiche: è un aspetto intrinseco del sistema informatico ed esiste indipendentemente da fattori esterni. Una vulnerabilità, di per sé, non causa automaticamente una perdita di sicurezza; è la combinazione tra vulnerabilità e minaccia che determina la probabilità che vengano violati gli obiettivi di sicurezza. Un centro di calcolo situato nel seminterrato di un centro urbano ha le stesse vulnerabilità in una zona poco soggetta a terremoti come in una zona sismica. Quello che cambia è la probabilità che si attui la minaccia terremoto, a scapito della disponibilità dell'impianto.

Un computer dedicato alla contabilità di un negozio, non protetto da firewall e antivirus e privo delle patch di sicurezza del sistema operativo, è assai vulnerabile, ma se è tenuto al sicuro, viene usato solo dal titolare e non è collegato a Internet, può funzionare a lungo senza essere colpito dalle minacce più comuni.

Impatto

L'impatto è la conseguenza dell'attuazione di una minaccia. Esso dipende dal valore del bene colpito e dagli obiettivi di sicurezza violati. Per una piccola azienda, se la minaccia "guasto dell'hard disk" colpisce la vulnerabilità "backup poco frequenti", l'impatto è serio, perché può includere il blocco temporaneo dell'attività e inconvenienti nei rapporti con i clienti. Gli obiettivi di sicurezza violati sono la disponibilità ed eventualmente l'integrità delle informazioni. Se un dirigente in viaggio connette il portatile a Internet senza protezione (programmi firewall e antivirus), apre un'e-mail infetta e di ritorno propaga l'infezione alla rete aziendale, l'impatto può essere grave e coinvolgere tutti gli obiettivi di sicurezza (disponibilità, integrità e riservatezza). In questo esempio l'agente della minaccia è l'utente, le vulnerabilità sono la cattiva configurazione del portatile e le falle di sicurezza di Windows e la minaccia sta nelle cattive abitudini e incompetenza dell'utente. L'impatto può includere il blocco temporaneo della rete e dei computer e un'attività generalizzata di disinfestazione con possibile perdita di dati e reinstallazione di software; anche parte dei backup potrebbe essere compromessa.

Rischio

Concettualmente, il rischio è la possibilità che si verifichi un evento dannoso ed è tanto maggiore quanto è forte l'impatto causato dall'evento e quanto è alta la probabilità che esso si verifichi. In una zona statisticamente non soggetta ad alluvioni, il rischio informatico connesso a questo tipo di eventi è trascurabile, anche se l'impatto potenziale è ingente. In una rete aziendale soggetta a tentativi di intrusione, a parità di protezione, la sottorete delle finanze corre un rischio maggiore rispetto alla sottorete amministrativa, perché a parità di probabilità di attacco, l'impatto dell'attacco è più grave.

In termini numerici, il rischio R può essere definito come il prodotto scalare tra la gravità G dell'impatto (conseguenze di un evento dannoso) e la probabilità P che si verifichi l'evento dannoso (la minaccia).

Le fasi della gestione del rischio

Nella gestione del rischio si possono individuare due fasi distinte.

1) **Analisi del rischio**. In questa fase si classificano le informazioni e le risorse soggette a minacce e vulnerabilità e si identifica il livello di rischio associato a ogni minaccia. Ci sono vari metodi per quantificare il rischio, basati su un approccio quantitativo, qualitativo o combinazione dei due. L'approccio quantitativo è basato su dati empirici e statistiche, mentre quello qualitativo si affida a valutazioni intuitive. Entrambi hanno vantaggi e svantaggi. Il primo richiede calcoli più complessi ma può basarsi su sistemi di misura indipendenti e oggettivi, fornisce risultati numerici (il valore delle perdite potenziali) e un'analisi dei costi e benefici. Il secondo utilizza l'opinione del personale che ha esperienza diretta in ciascuna delle aree interessate.
2) **Controllo del rischio**. In questa fase vengono individuate le modalità che l'azienda intende adottare per ridurre i rischi associati alla perdita della disponibilità di informazioni e risorse informatiche e della integrità e riservatezza di dati e informazioni. Ogni tipo di minaccia deve essere trattata separatamente e la pianificazione delle contromisure richiede un'analisi di costi e benefici che ottimizzi il valore della protezione. Se, per esempio, il rischio per l'intrusione in un server web è stimato di 12.000 euro in un anno e con una spesa annua di 1.000 euro esso scende a 3.000 euro, possiamo calcolare il valore della protezione in 12.000 (rischio iniziale) – 3.000 (rischio dopo l'allestimento delle contromisure) – 1.000 (costo annuale delle contromisure) = 8.000 euro.

Analisi del rischio

L'analisi del rischio è un processo composto di una sequenza di fasi, che inizia con la classificazione dei beni (informazioni e risorse informatiche), prosegue con l'identificazione delle minacce e delle vulnerabilità e si conclude con l'identificazione del livello di rischio.

1) **Classificazione delle informazioni** e delle risorse informatiche. Questa fase ha lo scopo di censire e classificare le informazioni gestite dal sistema informativo aziendale (attraverso sistemi informatici e altri mezzi) e le risorse informatiche utilizzate. Il risultato è la documentazione delle informazioni che hanno valore per l'azienda, in modo che nelle fasi successive si possa valutare il rischio a fronte della perdita di disponibilità, integrità e riservatezza di ogni categoria di informazioni. Visto che le informazioni sono aggregazioni di dati che, singolarmente, potrebbero essere (o apparire) privi di valore, si dovrà tenere conto delle relazioni tra dati e informazioni.

La sicurezza delle informazioni è strettamente legata alla disponibilità delle risorse informatiche, quindi, in questa fase, vengono documentati anche i sistemi, le attrezzature di rete, la capacità di elaborazione, la capacità dei canali di comunicazione, i processi vitali e altre risorse necessarie per gli obiettivi di sicurezza delle informazioni.

2) **Identificazione delle minacce**. Una minaccia è un'azione potenziale, accidentale o deliberata, che può portare alla violazione di uno o più obiettivi di sicurezza e quindi causare un danno all'azienda. In questa fase si compila l'elenco delle minacce, avendo cura di includere gli eventi di origine naturale, gli eventi accidentali (guasti hardware, errori software, errori umani ecc.) e le azioni umane deliberate (sia interne, sia esterne). Le minacce a cui è soggetta un'organizzazione hanno aspetti generali e aspetti specifici riguardanti il campo di attività, il modello di business, le caratteristiche del sistema informativo e del sistema informatico, la dislocazione e le comunicazioni dell'organizzazione. Esempi di minacce generali sono quelle ambientali che possono impedire il funzionamento delle attrezzature informatiche (alimentazione elettrica, temperatura ecc.), i guasti hardware (hard disk, supporti di backup, alimentatori, ventole ecc.), gli errori software, la cancellazione accidentale di dati, gli errori degli utenti, i virus e altro malware (worm, trojan, spyware, ecc.), i tentativi di intrusione da Internet, l'esecuzione di software insicuro, la sottrazione e/o la divulgazione di informazioni e software e via dicendo.

Minacce più specifiche sopratutto per le aziende che eseguono transazioni economiche on line (banche, siti di e-commerce, broker ecc.) sono ad esempio le azioni di social engineering (fingersi altre persone, come pubblici ufficiali o addetti all'assistenza) per procurarsi password e altre informazioni utili per avere accesso alle informazioni.

L'analisi del rischio in tre formule

R = G x P

Il rischio *R* può essere definito come il prodotto scalare fra la gravità *G* dell'impatto (conseguenze di un evento dannoso) e la probabilità *P* che si verifiche l'evento dannoso.

P = f(V, M)

per minacce di tipo deliberato

Per una minaccia di tipo deliberato, la probabilità *P* che la minaccia si verifichi è una funzione delle vulnerabilità *V* presenti nel sistema (hardware, software e procedure) e delle motivazioni *M* dell'agente attaccante.

P = f(V, p)

per minacce di tipo accidentale e ambientale

Per una minaccia di tipo accidentale e ambientale, la probabilità *P* che essa si verifichi è una funzione delle vulnerabilità *V* del sistema e della probabilità *p* che i rilevamenti statistici permettono di associare all'evento in questione (per esempio la probabilità di cancellare per errore un file importante o la probabilità che un blackout prolungato causi un'interruzione del servizio).

5.1.2 Gestione del rischio

5.1.2.2 conoscere la classificazione più comune dei mezzi tecnici per controllare il rischio (identificazione e autenticazione), controllo degli accessi, rendicontabilità (accountability), verifica (audit), riutilizzo degli oggetti, accuratezza, affidabilità del servizio, scambio dati sicuro).

Tabella 1 - Analisi del rischio quantitativa

Bene	Minaccia	Valore del bene	Aspettativa di perdita singola	Probabilità annua	Aspettativa di perdita annua
Locali	Incendio	300.000	200.000	0,1	20.000
Progetti	Furto	100.000	80.000	0,5	40.000
Server	Guasto	8.000	6.000	0,3	1.800
Dati	Virus e simili	40.000	30.000	0,5	7.500
Dati	Errori utente	40.000	20.000	0,5	10.000
Rete	Guasto	6.000	2.000	0,75	1.500

Identificazione delle vulnerabilità. Le vulnerabilità sono tutti quei punti deboli del sistema informativo tali che, se sfruttate dall'attuarsi di una minaccia, permettono la violazione degli obiettivi di disponibilità, integrità e riservatezza delle informazioni. In precedenza abbiamo mostrato esempi di vulnerabilità in diverse categorie. Per esempio, l'assenza di un gruppo di continuità e l'intolleranza di alte temperature ambiente rientrano nella categoria impianti. La categoria software include le falle di sicurezza e gli errori dei sistemi operativi e delle applicazioni. La categoria hardware comprende computer, periferiche, accessori e dispositivi di rete, tutti soggetti a guasti e malfunzionamenti. L'assenza di regole e di strumenti adeguati per il backup degli archivi fa parte delle vulnerabilità procedurali. Alla categoria del personale competono carenze come l'inadeguata preparazione e istruzione degli utenti, l'utilizzo improprio di Internet e delle risorse informatiche e la scarsa diligenza nel custodire le password e altre informazioni riservate.

Come per le minacce, anche le vulnerabilità sono specifiche per il tipo di azienda, il campo di attività e l'organizzazione interna. Inoltre, la stessa vulnerabilità può avere diversi livelli di importanza secondo le caratteristiche dell'azienda. La vulnerabilità di un particolare servizio di comunicazione del sistema operativo può essere considerata irrilevante per un'azienda manifatturiera tradizionale ma allo stesso tempo grave per un'azienda che progetta strumenti ad alta tecnologia per un mercato competitivo.

Identificazione del livello di rischio. Dopo aver censito i beni da proteggere e quantificato il loro valore, e dopo aver calcolato la probabilità di attuazione delle minacce (in base alle vulnerabilità e agli agenti di attacco individuati), è possibile calcolare il rischio seguendo l'approccio quantitativo. A tale scopo si possono utilizzare fogli elettronici o apposite applicazioni per automatizzare il calcolo del rischio secondo i settori di attività.

In alternativa, l'approccio qualitativo non quantifica i danni e le probabilità, ma esamina le aree di rischio assegnando, in base a intuizione, esperienza e giudizio, valori relativi (per esempio da 1 a 5) alla gravità della minaccia, alla sua probabilità di attuazione e alla perdita potenziale per l'azienda. Anche le contromisure sono valutate con lo stesso criterio, in modo da selezionare quella che il personale interessato ritiene più adatta per fronteggiare la minaccia.

In tabella 1 consideriamo un piccolo esempio di analisi quantitativa, ridotto a poche righe a scopo illustrativo.

In questo esempio sono indicate le previsioni di danno (perdita economica) per un singolo evento (attuazione della minaccia) e la probabilità stimata in base a statistiche di frequenza o dati empirici. Nella realtà, l'attacco a un bene materiale di valore limitato, come un server di rete, può causare un danno superiore per ordini di grandezza a beni immateriali come l'immagine, la reputazione e il credito dell'azienda. Inoltre, certi tipi di minacce, in assenza di appropriate difese, possono attuarsi ripetutamente in un anno, come le perdite e alterazioni di dati per errori degli utenti e/o del software applicativo. Va detto che un'analisi del rischio puramente quantitativa è pressoché impossibile, vista la difficoltà di assegnare valori precisi ai danni subiti dai beni e alle probabilità di attuazione delle minacce. In ogni caso, l'analisi permette di identificare i beni da proteggere, le fonti di danno e l'entità del rischio; in base a queste informazioni si potrà definire una strategia per proteggere i beni nel modo più efficiente.

Vediamo ora un esempio di analisi qualitativa, basata sul giudizio, l'esperienza e l'intuito delle persone che operano nelle aree soggette a minacce. Ci sono diversi metodi per raccogliere le informazioni per un'analisi qualitativa del rischio. Il metodo Delphi, per esempio, si basa su decisioni di gruppo per assicurare che ogni membro del gruppo di valutazione possa esprimere onestamente il proprio parere sulle minacce e sui rimedi più efficaci. Ogni membro del gruppo scrive le proprie valutazioni in modo anonimo, senza pressioni o influenze da parte degli altri. I risultati vengono compilati e distribuiti ai membri del gruppo, che scrivono i loro commenti, ancora anonimi. Il processo si ripete finché non si forma un consenso su costi, perdite potenziali, e probabilità di attuazione delle minacce, senza discussioni verbali.

Altri metodi qualitativi fanno uso di brainstorming, focus group, sondaggi, questionari, liste di verifica, interviste, incontri individuali e altro ancora.

Nella tabella 2 vediamo un piccolo esempio semplificato di analisi qualitativa applicata alla minaccia di intrusione da Internet.

In questo esempio gli addetti all'analisi del rischio hanno distribuito una descrizione della minaccia (intrusione da Internet) a cinque persone con diverse mansioni nell'area IT, con la richiesta di valutare, da 1 a 5, la gravità della minaccia, la probabilità che accada, la perdita conseguente e l'efficacia di alcune possibili misure di protezione. La valutazione è quindi sottoposta al management, che vedrà qual è il punto di vista del personale interessato sulla gravità delle minacce e sui modi di proteggersi.

Il controllo del rischio e le contromisure

Consideriamo l'analisi del rischio secondo l'approccio quantitativo; il documento finale elenca in modo dettagliato i beni con i relativi valori monetari, le vulnerabilità, le minacce con relativa probabilità di attuazione e le perdite potenziali (per esempio su base annua). La fase successiva,

Tabella 2 - Analisi del rischio qualitativa

Minaccia intrusione da Internet	Gravità della minaccia	Probabilità di attuazione	Perdita potenziale	Efficacia firewall	Efficacia firewall con IPS	Efficacia firewall più IDS
IT manager	4	2	4	3	5	4
Amministratore database	5	4	5	3	4	3
Programmatore	3	3	3	4	4	4
Operatore	2	4	3	3	4	3
Manager	5	4	4	4	5	5
Media	3,8	3,4	3,8	3,4	4,4	3.8

controllo del rischio, ha lo scopo di eliminare i rischi, o perlomeno di ridurli entro limiti accettabili. Parte dei rischi può essere ceduta a terzi, per esempio attraverso polizze di assicurazione (per cautelarsi da eventi come furto, incendio e disastri naturali). Anche l'outsourcing, cioè la delega a terzi di servizi che potrebbero essere svolti da personale interno, può essere utile a ridurre vari tipi di rischio, tra cui il mancato ritorno dagli investimenti in addestramento specialistico del personale. Anche la gestione dello storage, ovvero gli archivi e i backup, può essere affidata a terzi appositamente strutturati per garantire alti livelli di sicurezza (disponibilità, integrità e riservatezza delle informazioni). L'hosting dei siti web è un esempio di outsourcing conveniente alle piccole aziende, solitamente prive di impianti e personale per amministrare hardware, software e sicurezza dei siti.

Tolta la cessione a terzi di parte dei rischi, consideriamo la parte di gestione del rischio che avviene all'interno dell'azienda. Il controllo del rischio viene esercitato attraverso opportune contromisure che agiscano sulle due componenti del rischio: la gravità dell'impatto e la probabilità di attuazione della minaccia. Abbiamo visto che le minacce coprono un ampio spettro di fenomeni e attività; ognuna dovrà essere quindi trattata separatamente sia nel valutare l'impatto e la probabilità, sia nel selezionare le contromisure che risultano più efficaci nell'analisi di costo e benefici.

Contromisure

Le contromisure di sicurezza sono le realizzazioni e le azioni volte ad annullare o limitare le vulnerabilità e a contrastare le minacce. Una parte delle contromisure viene solitamente realizzata nel corso della progettazione di un sistema o di un prodotto. Le altre contromisure vengono adottate in fase di utilizzo del sistema o prodotto.

La scelta delle contromisure da mettere in campo è dettata dall'analisi del rischio e dall'analisi costo/benefici delle contromisure. Considerato un bene, il suo valore e il danno potenziale in base alle vulnerabilità e alle probabilità di attuazione di una minaccia, l'effetto di una contromisura si misura con la riduzione del rischio. Se la riduzione del rischio è ampiamente superiore al costo della contromisura, questa è efficace. Se un certo rischio è di scarsa entità e la contromisura risulterebbe più costosa rispetto ai benefici, si può decidere di accettare il rischio senza alcuna contromisura. Lo stesso dicasi nei casi in cui il rischio residuo (il rischio che rimane dopo l'adozione delle contromisure) non fosse significativamente inferiore al rischio iniziale. In pratica, la scelta e adozione delle contromisure è dettata sia dagli obiettivi di sicurezza (e relative priorità di urgenza e importanza) sia dal buon senso economico.

Si possono classificare le contromisure in tre categorie a seconda che siano di carattere fisico, di tipo procedurale o di tipo tecnico informatico.

Contromisure di carattere fisico. Queste contromisure sono generalmente legate alla prevenzione e al controllo dell'accesso a installazioni, locali, attrezzature, mezzi di comunicazione. Un esempio è un centro di calcolo realizzato in un edificio protetto e accessibile solo dopo il riconoscimento del personale autorizzato. Una server farm per ospitare migliaia di siti web è probabilmente dotata di varie contromisure di tipo fisico: la collocazione in zona elevata non soggetta ad alluvioni, pompe e rilevatori per evacuare l'acqua, sistemi antincendio, accessi blindati e sorvegliati e via dicendo. Dato che sistemi e installazioni comunicano in rete, anche le linee di comunicazione possono avere bisogno di protezione fisica contro intercettazioni, disturbi e danneggiamenti. Tra le contromisure fisiche ci sono le canalizzazioni dei cavi di rete, magari interrate o sotto traccia per ostacolare l'accesso e le schermature di vetri e pareti per contenere il campo delle reti wireless.

Contromisure di tipo procedurale. Queste contromisure definiscono passo per passo le operazioni per eseguire un certo compito oppure regolano il comportamento degli utenti per gli aspetti che riguardano la sicurezza delle informazioni e delle risorse.

Mentre le contromisure fisiche proteggono l'accesso fisico alle risorse e le contromisure informatiche agiscono a livello hardware, firmware e software, le procedure operative e le regole di comportamento si applicano alle persone (utenti e amministratori). Lo scopo, da un lato, è quello di evitare che gli utenti causino vulnerabilità e minacce e, dall'altro, che contribuiscano a mantenere alte le difese riducendo i rischi residui lasciati dalle altre contromisure.

Esempi di contromisure di tipo procedurale sono il controllo dell'identità dei visitatori e la limitazione delle aree a cui hanno accesso. Quando si usa un badge o altra scheda di riconoscimento, anche la sua custodia è oggetto delle procedure, così che non venga lasciato sulla scrivania o in un cassetto aperto o comunque a disposizione di altri.

Le password sono uno strumento di protezione informatico, ma le regole per la loro assegnazione, durata, utilizzo e custodia fanno parte delle contromisure procedurali per ridurre il rischio che cadano in cattive mani. Alcune norme comuni sono: utilizzare password non brevi, contenenti non solo lettere; raccomandare o imporre modifiche periodiche delle password; bloccare l'accesso dopo un numero limitato di tentativi errati; sensibilizzare e responsabilizzare gli utenti sugli effetti della mancata riservatezza (tenere la password su un post-it sotto la tastiera, in un cassetto ecc. o comunicare la propria password a un collega o a un sedicente tecnico di assistenza).

Come per le password, ci sono altre contromisure informatiche che sono efficaci solo se si rispettano certe norme d'uso o procedure organizzative. Un antivirus, per esempio, è efficace se è aggiornato di frequente, come minimo una volta al giorno. Una vulnerabilità degli antivirus è infatti quella di non proteggere dai virus di recente introduzione; il rimedio è installare un sistema centralizzato e una procedura che assicuri l'aggiornamento almeno quotidiano del file di riconoscimento dei virus e un aggiornamento periodico del software antivirus. Per un piccolo ufficio, lo stesso risultato può essere ottenuto installando un antivirus che scarichi automaticamente gli aggiornamenti tutti i giorni e che esegua una scansione giornaliera dei file.

In generale, le contromisure di tipo procedurale dovrebbero essere ridotte al minimo, sostituendole quando possibile con sistemi automatizzati, meno soggetti agli errori, dimenticanze e violazioni degli utenti. È il caso, per esempio, dei dispostivi di riconoscimento biometrici usati al posto dei badge o delle password. Anche l'aggiornamento periodico del firmware dei firewall, anziché essere oggetto di norme procedurali, può essere automatizzato utilizzando firewall che si aggiornano automaticamente collegandosi al sito del produttore. In questo modo, sia le funzionalità sia le protezioni sono tenute aggiornate evitando il costo degli interventi manuali, l'interruzione del servizio, il rischio di errori manuali e il rischio di una minore protezione a causa dell'invecchiamento del firmware.

Altri esempi riguardano le norme d'uso di hardware e software, dove una documentazione inadeguata e un addestramento sommario possono favorire errori o il mancato utilizzo di certe funzioni, aumentando i rischi per la sicurezza.

Nel campo dei backup, non tutte le aziende hanno procedure automatiche che garantiscano il ripristino dopo un disastro (disaster recovery) o la continuità operativa (business continuity) a dispetto di qualsiasi evento catastrofico. Vista l'entità dell'impatto e la frequenza di guasti ai supporti magnetici, è vitale avere una strategia di backup e mettere in atto procedure che garantiscano l'esecuzione dei back a più livelli (con diverse periodicità) e la verifica dell'integrità e utilizzabilità dei supporti di backup. Parte di queste operazioni può essere automatizzata, specialmente nelle aziende medio-grandi; la verifica dei supporti di

backup è invece spesso un punto trascurato. Nei piccoli uffici, i più soggetti a improvvisazione e omissioni in tema di backup, la difficoltà di imporre l'osservanza di procedure è aggirabile tramite applicazioni software commerciali che, in modo automatico e pianificato, salvano le immagini delle partizioni degli hard disk, senza interrompere il lavoro sui computer. In questo modo, si può utilizzare una contromisura tecnico informatica al posto di quella che, normalmente, è una contromisura procedurale.

Lo smaltimento dei supporti su cui risiedono informazioni è un altro esempio dell'opportunità di contromisure procedurali per evitare che informazioni riservate siano rese pubbliche. Le contromisure possono includere la distruzione dei documenti cartacei da gettare nella spazzatura, la cancellazione dei supporti magnetici da smaltire o da sostituire in garanzia, lo spostamento degli archivi o l'estrazione degli hard disk prima di mandare un computer in manutenzione (salvo l'uso di personale interno con qualifica di sicurezza) e la distruzione dei supporti ottici da smaltire.

Contromisure di tipo tecnico informatico. Queste sono le contromisure realizzate attraverso mezzi hardware, firmware e software e prendono anche il nome di funzioni di sicurezza. In base al loro campo d'azione, possono essere classificate nelle categorie che seguono.

Identificazione e autenticazione. Le funzioni di questa categoria servono a identificare un individuo o un processo e ad autenticarne l'identità. L'esempio più comune è la funzione di accesso (login) a un sistema tramite nome utente (per l'identificazione) e password (per l'autenticazione dell'identità). L'autenticazione viene usata anche nelle comunicazioni tra processi e nei protocolli di comunicazione per accertare l'identità del processo o dell'utente associato al processo.

Controllo degli accessi. In questa categoria troviamo le funzioni di sicurezza che verificano se il processo o l'utente, di cui è stata autenticata l'identità, ha il diritto di accedere alla risorsa richiesta (per esempio file, directory, stampanti) e di eseguire l'operazione specificata (per esempio lettura, esecuzione, modifica, creazione, cancellazione). Per i processi, anche l'accesso alla memoria è regolamentato, in modo che un processo non possa leggere i dati di un altro processo o, in certi casi, non possa eseguire istruzioni contenute in aree destinate esclusivamente a dati. Analoghe funzioni sono svolte a livello hardware dalla CPU nella sua gestione delle pagine di memoria.

Rendicontabilità (accountability). A questa categoria appartengono le funzioni che permettono di attribuire la responsabilità degli eventi agli individui che li hanno causati. L'accountability richiede l'attuazione delle misure d'identificazione e autenticazione degli utenti e l'associazione a ogni processo dell'identità del suo proprietario, come avviene nei moderni sistemi operativi.

Verifica (audit). A questa categoria appartengono le funzioni che registrano gli eventi in un file di logging, con informazioni riguardo a errori e a violazioni di sicurezza. Grazie a queste registrazioni, è possibile risalire a ciò che è accaduto e prendere provvedimenti. Nel caso di segnalazione di malfunzionamenti hardware o di errori software, si possono intraprendere azioni di diagnosi e manutenzione (per esempio la verifica e correzione del file system).

Nel caso di eventi che riguardano la sicurezza, il log permette di scoprire irregolarità, come tentativi di accesso illeciti e tentativi di intrusione. Esempi di funzioni di logging sono quelle di Windows, che registra log degli eventi di sistema, applicativi e di sicurezza oppure il demone syslogd dei sistemi Unix/Linux.

Nel caso dei firewall, il log comprende la registrazione selettiva degli eventi che si desidera tenere sotto controllo: tutti, se non non attiva nessun filtro, oppure solo quelli che superano un certo livello di gravità.

Solitamente i firewall offrono l'opzione di logging remoto, che consiste nell'inviare la segnalazione degli eventi a un computer, in modo da poter tenere registrazioni anche voluminose (su lunghi periodi di tempo) e poterle analizzare più facilmente.

Riutilizzo degli oggetti. Questa categoria comprende le funzioni che permettono di riutilizzare oggetti contenenti informazioni riservate: supporti magnetici, supporti ottici riscrivibili, aree di memoria RAM, zone di memoria dei processori (registri, cache, ecc.), buffer di periferiche e simili. Lo scopo è quello di evitare che informazioni riservate siano lasciate a disposizione di programmi e utenti dopo il loro regolare utilizzo. Le contromisure in questa area hanno il compito di cancellare le aree di memoria e di disco subito dopo il loro utilizzo per il transito di informazioni riservate. Un esempio riguarda le aree di memoria dove transitano le password o altre informazioni in chiaro prima della loro cifratura: buffer, registri e aree di lavoro dovrebbero essere cancellate per evitare che siano lette da altri processi autorizzati ad accedere a quelle aree ma associati a utenti non autorizzati alla conoscenza di quelle informazioni. Un altro esempio è offerto dalle aree di scambio su disco, come i file di swapping o paging del sistema operativo. È utile attivare l'opzione di cancellazione automatica di questi file alla chiusura del sistema, in modo che utenti non autorizzati non possano esaminarlo a caccia di informazioni riservate.

Accuratezza. Fanno parte di questa categoria tutte le funzioni intese a garantire l'accuratezza delle informazioni. Per esempio, perché i file di logging forniscano informazioni attendibili, la registrazione temporale (time stamp) dell'evento deve essere precisa. Questo accade se l'orologio interno è sincronizzato periodicamente con un time server di riferimento. Sistemi operativi, switch, firewall e altri dispositivi offrono questa funzionalità, che se necessario va attivata specificando il nome del time server (per esempio time.nist.gov). In campo software, esempi di funzioni a difesa dell'accuratezza delle informazioni sono le funzioni che controllano i limiti di occupazione di buffer e array e quelle che validano la correttezza dei dati immessi dagli utenti.

Affidabilità del servizio. Questa è una vasta categoria di contromisure, perché sono diverse le aree che potrebbero compromettere l'affidabilità dei servizi informatici. Si inizia dalle contromisure per mantenere condizioni di alimentazione elettrica stabile, filtrata e senza interruzione (gruppi di continuità), per passare alle difese dai malfunzionamenti hardware (monitoraggio e manutenzione preventiva) e software (monitoraggio degli errori nei file di logging, aggiornamenti, monitoraggio delle prestazioni, rollback delle transazioni non andate a buon fine, ripristino di uno stato precedente del sistema operativo, ripristino delle partizioni di disco a uno stato integro precedente). Altre contromisure possono essere sviluppate per difendere sistemi e applicazioni dagli errori degli utenti.

Scambio dati sicuro. In questa categoria ci sono le funzioni destinate a garantire la sicurezza delle trasmissioni. Il modello OSI Security Architecture (ISO 7498-2) le classifica nelle seguenti sottoclassi: autenticazione, controllo dell'accesso, riservatezza, integrità (dell'hardware, dei dati e dei flussi di pacchetti trasmessi sia in modo connectionless, come UDP, sia connection-oriented, come TCP, anche ai fini della corretta sequenza dei pacchetti) e non ripudio. Esempi di contromisure in questa area sono l'uso di crittografia a chiave simmetrica e asimmetrica (chiave pubblica più chiave privata) e l'autenticazione tramite Message Authentication Code (il risultato dell'hashing applicato al messaggio più una chiave segreta simmetrica; vengono trasmessi messaggio e MAC; a destinazione il MAC viene ricalcolato sul messaggio più chiave simmetrica e confrontato col MAC ricevuto, così da verificare l'integrità del messaggio e l'autenticazione del mittente).

Funzionalità e garanzia nel controllo del rischio

La sicurezza delle informazioni è caratterizzata da due

fattori di base indipendenti: la funzionalità e la garanzia (assurance).

Il termine **funzionalità**, applicato alla sicurezza, conserva il significato generale che ha in altri settori; è l'insieme di ciò che un prodotto o un sistema informatico fornisce in relazione alla protezione delle informazioni e, di riflesso, delle risorse e dei servizi informatici. Il panorama di contromisure descritto nella sezione precedente (5.1.2.2) comprende gran parte delle funzionalità di sicurezza che potrebbero essere necessarie.

Il concetto di **garanzia** è stato introdotto da chi si occupa di sicurezza per esprimere il grado in cui l'implementazione di una funzionalità riduce una vulnerabilità o la possibilità di attuazione di una minaccia. Se la funzionalità rappresenta un elemento di protezione, la garanzia ne indica la validità.

Prendiamo ad esempio la funzionalità autenticazione dell'identità. Oggi l'implementazione più comune consiste nell'uso di una password segreta per convalidare il nome dell'utente. Tuttavia, ci sono altre soluzioni, come l'utilizzo di un oggetto fisico (come badge o smart card) o di un dispositivo biometrico (basato ad esempio sul riconoscimento dell'impronta digitale, della cornea, del volto o della voce). Nessuna di queste implementazioni è infallibile e la scelta dipende da vari fattori: il settore di attività, la dimensione aziendale, il livello di rischio, la sensibilità e la competenza degli utenti, le minacce ambientali, i costi sostenibili e via dicendo. Un laboratorio di ricerca in un settore avanzato competitivo potrebbe dotarsi di un sistema di riconoscimento vocale sofisticato da un punto di vista funzionale, ma di scarsa garanzia se le parole da pronunciare sono prevedibili (e quindi preventivamente registrabili).

Altrettanto scarsa garanzia offrirebbe un sistema di riconoscimento dell'impronta digitale dove un guardiano prevenisse frodi ma la precisione del riconoscimento fosse insoddisfacente.

Vediamo quindi che la garanzia è costituita a sua volta da due aspetti distinti: la correttezza e l'efficacia. La correttezza è un attributo intrinseco di un prodotto (o componente o procedura), che riflette il grado di corrispondenza tra le effettive funzioni svolte dal prodotto e le sue specifiche. Per esempio, un prodotto capace di riconoscere il 99% delle voci umane adulte con almeno 30 dB di rapporto segnale/rumore, riceverebbe un'alta valutazione di correttezza rispetto alla funzione "riconoscere la voce degli utenti".

La **correttezza** è una proprietà intrinseca del prodotto nell'ambito delle condizioni d'uso previste; non dipende da fattori esterni, come l'opportunità di utilizzare o meno quel prodotto per soddisfare una particolare esigenza.

L'**efficacia** è invece una proprietà che mette in relazione la contromisura (prodotto, procedura o altro) con il contesto in cui è utilizzata, in particolare le vulnerabilità, la gravità e la probabilità di attuazione delle minacce, le caratteristiche degli agenti che attuano le minacce, l'importanza del bene da proteggere e così via. Supponiamo che per il laboratorio del nostro esempio sia vitale consentire l'accesso solo al personale autorizzato, visto il valore delle informazioni e risorse da proteggere e l'alta probabilità di minacce di intrusione fisica e telematica da parte di agenti (software e individui) ritenuti pericolosi. Il progetto di sicurezza si basa sulla completezza delle funzionalità (le contromisure messe in campo) e sulla garanzia che le contromisure adottate riducano le vulnerabilità e le minacce a livelli accettabili. Supponendo che l'analisi del rischio abbia portato a identificare tutte le funzionalità di sicurezza utilizzabili, tra cui gli strumenti e le procedure per impedire una falsa autenticazione da parte di software e personale ostile, nella fase di valutazione della garanzia si dovranno esaminare correttezza ed efficacia delle soluzioni. Per esempio, un sistema di riconoscimento vocale potrebbe risultare adatto per ambienti con livello medio di rischio, ma essere inadeguato a fronte di un rischio elevato e di una minaccia agguerrita. Potrebbe risultare più efficace un sistema basato su domande a cui solo il legittimo utente possa rispondere o su un dispositivo fisico (tipo smart card) interattivo, da aggiornare ogni giorno per rimanere valido (in modo da perdere validità in caso di furto o manipolazione).

Un altro esempio ci viene offerto dalle contromisure di natura fisica per impedire l'accesso alle persone non autorizzate. Le contromisure per il controllo dell'accesso possono limitarsi a una porta blindata o includere sistemi di rilevamento del movimento, telecamere e registratore video, sistemi di allarme con chiamata di numeri telefonici e altri deterrenti per impedire e/o scoraggiare il tentativo di effrazione. In fase di analisi del rischio, supponiamo che sia emersa l'esigenza di installare una porta blindata capace di resistere a una determinata forza di sfondamento, priva di cardini a vista e resistente al fuoco. Queste sono quindi le specifiche rispetto alle quali verrà valutata la correttezza dei prodotti. Ora, anche se abbiamo individuato la migliore delle porte blindate sul mercato, dobbiamo valutare l'aspetto efficacia. Per quanto tempo la porta resisterà alle tecniche di scasso più evolute? Qual è la probabilità che le forze dell'ordine arrivino in tempo per impedire l'accesso alle risorse informatiche, agli archivi e alle informazioni? Se il rischio è rilevante, probabilmente si dovrà identificare un pacchetto di contromisure che, nell'insieme, costituiscano un percorso ad ostacoli capace di resistere al gruppo d'attacco più determinato.

Poiché i beni da proteggere possono essere assai diversi da un caso all'altro, il programma di sicurezza dovrà essere personalizzato per la situazione specifica, in modo che la scelta delle contromisure e relative funzionalità e garanzie siano commisurate all'entità del rischio e ai tipi di vulnerabilità e di minacce.

5.1.2 Gestione del rischio

5.1.2.3 conoscere la differenza tra funzionalità e garanzia e l'importanza di conseguire entrambe al fine di controllare il rischio.

Organizzazione della sicurezza

I processi

La sicurezza delle informazioni è il risultato di un insieme di processi ai vari livelli dell'organigramma aziendale. Non bastano strumenti e tecnologie per ottenere la sicurezza. Occorre, in primo luogo, creare un'organizzazione per la sicurezza che assuma la responsabilità di quanto attiene alla sicurezza e coinvolga l'intera struttura aziendale, in modo che tutto il personale contribuisca nel proprio ambito al disegno generale della sicurezza. Infatti, la sicurezza delle informazioni, delle risorse informative (non solo informatiche) e in generale dei beni e del valore dell'azienda dipende non solo dal lavoro del gruppo addetto alla sicurezza ma anche dal comportamento del personale (interno ed esterno) a tutti i livelli dell'organigramma.

Come avviene per il progetto di un edificio, l'organizzazione della sicurezza dovrebbe partire dall'alto, dove gli obiettivi e le politiche di sicurezza sono definiti in termini generali dal top management, per essere poi specificati nei dettagli man mano che si scende attraverso gli strati del modello organizzativo della sicurezza. In cima a questo modello ci sono gli obiettivi di business strategici, che ispirano i processi fondamentali di cui si deve fare carico l'organizzazione di sicurezza: classificazione dei beni e del loro valore, censimento di vulnerabilità e minacce, analisi del rischio, analisi costi/benefici delle contromisure, valutazione del grado di protezione, definizione delle politiche di sicurezza, pianificazione, implementazione e gestione dei progetti di sicurezza, monitoraggio della conformità tra le soluzioni adottate e le politiche di sicurezza e altro ancora.

L'approccio dall'alto al basso permette di coinvolgere tutti i livelli aziendali interessati, di assegnare precise responsabilità, di definire politiche coerenti per l'intera strut-

5.1.3 Organizzazione della sicurezza

5.1.3.2 conoscere i principali processi da attivare in un'organizzazione che mira a conseguire la sicurezza delle informazioni.

Un esempio di politica di sicurezza per le comunicazioni wireless

1.0 Scopo
Questa policy proibisce l'accesso alla rete della ACME SpA attraverso connessioni wireless insicure, cioè non protette tramite autenticazione dell'utente e cifratura dei dati. Solo i sistemi wireless conformi ai criteri di questa policy o che hanno ricevuto una speciale esenzione dal responsabile della sicurezza sono approvati per la connessione alle reti della ACME SpA.

2.0 Portata
Questa policy copre tutti i dispositivi di comunicazione dati senza fili (per es. personal computer, telefoni cellulari, PDA eccetera) connessi con una delle reti della ACME SpA. Questo comprende qualunque tipo di dispositivo wireless capace di trasmettere dati a pacchetti. I dispositivi e le reti wireless senza alcuna connessione alle reti della ACME SpA non rientrano nell'ambito di questa policy.

3.0 Policy
3.1 Registrazione degli access point e delle schede
Tutti gli access point o stazioni di base connessi alla rete aziendale devono essere registrati e approvati dal responsabile della sicurezza. Questi access point sono soggetti a test di intrusione e a periodici audit. Tutte le schede d'interfaccia wireless di rete usate sui desktop e notebook aziendali devono essere registrate presso il responsabile della sicurezza.

3.2 Tecnologie approvate
Ogni accesso wireless alla LAN deve utilizzare prodotti e configurazioni di sicurezza approvati dall'azienda.

3.3 Cifratura e autenticazione via VPN
Tutti i computer con dispositivi LAN wireless devono utilizzare una Rete Privata Virtuale (VPN) approvata dall'azienda e configurata per ignorare tutto il traffico non autenticato e non cifrato. Per conformità con questa policy, le implementazioni wireless devono mantenere una cifratura hardware di ogni connessione con chiavi di almeno 128 bit. Tutte le implementazioni devono supportare un indirizzo hardware (MAC address) registrato e rintracciabile. Tutte le implementazioni devono supportare e impiegare una forte autenticazione degli utenti tramite accesso a un server e database esterno come TACACS+, RADIUS o simile.

3.4 Impostazione dell'SSID
L'SSID (*Service Set Identifier* – un'intestazione aggiuntiva ai pacchetti mandati su una WLAN che funge da password per chi vuole accedere alla rete - sarà impostato in modo che non contenga alcuna informazione relativa all'organizzazione, come nome dell'azienda, nome della divisione o identificatore del prodotto.

4.0 Applicazione
Qualunque dipendente sia riconosciuto responsabile di aver violato questa policy può essere soggetto ad azione disciplinare, fino alla cessazione del rapporto di lavoro.

5.0 Definizioni

Termine	Definizione
Autenticazione	Un metodo per verificare se l'utente di un sistema wireless è un utente legittimo, indipendentemente dal computer o dal sistema operativo che viene usato.

6.0 Revisioni
10 luglio 2004, aggiunta la sezione 3.4
20 marzo 2004, sezione 3.3 modificata per includere gli indirizzi MAC

tura aziendale, di sensibilizzare ed educare il personale, di finanziare adeguatamente il progetto sicurezza e di rimuovere gli ostacoli che si presenteranno quando verranno adottate procedure e strumenti che avranno un impatto sull'operatività quotidiana e sulle abitudini del personale (a tutti i livelli).

A volte nelle aziende vengono prese iniziative di sicurezza dal basso, con le buone intenzioni di proteggere alcuni obiettivi di sicurezza immediati. Senza la forza di spinta, l'autorità, la responsabilità, il coinvolgimento generale e i mezzi assicurati dal management superiore, i tentativi dal basso si scontrano facilmente con ostacoli insormontabili e sono spesso destinati a fallire. Il migliore interesse dell'azienda esige che la responsabilità della sicurezza si diffonda a cascata dalla cima verso la base della piramide aziendale, con la partecipazione dei vari strati di utenti della sicurezza. In questo modo, anziché turare alcune falle senza un piano preciso, si potrà corazzare l'intera struttura aziendale nel modo più efficiente rispetto al rischio da controllare e al budget disponibile. Una volta definiti gli obiettivi, le politiche, un piano e le soluzioni da adottare, si potrà sensibilizzare e informare tutto il personale sugli aspetti concernenti la sicurezza, rendendo esplicite le responsabilità e le sanzioni per manager, amministratori e utenti.

La struttura organizzativa della sicurezza può assumere varie forme secondo il tipo e le dimensioni dell'azienda, il campo di attività, il rapporto con l'ambiente, il mercato e altri fattori. Può essere informale in una piccola azienda senza particolari problemi di sicurezza oppure essere complessa con rappresentanti delle diverse aree aziendali in una grande società. Può limitarsi alla sicurezza delle informazioni o estendere la propria sfera all'intera sicurezza aziendale, inclusa la gestione del rischio nei settori operativo, marketing, finanziario ecc.

Un aspetto che modella i processi di sicurezza è il costo in base al rischio e all'attività dell'azienda. A questo proposito, è facile immaginare una scala crescente di rischi e investimenti in sicurezza. Aziende manifatturiere, organizzazioni finanziarie, certification authority (organizzazioni fidate che rilasciano certificati digitali) e forze armate sono esempi di requisiti crescenti di sicurezza.

Uno dei primi compiti del gruppo incaricato della sicurezza è quindi quello di inquadrare l'azienda in base al modello di attività, all'esposizione ai rischi e alla dipendenza dall'infrastruttura informatica e di comunicazioni. Questo esame preliminare dovrà tenere in considerazione il quadro legislativo tracciato dalle leggi sulla criminalità informatica e sulla privacy che si sono succedute numerose nel corso degli anni e che sono culminati con il decreto legge 196 del 2003 (Codice in materia di protezione dei dati personali). Le norme di legge pongono dei vincoli, secondo il tipo di attività, che devono essere calcolati nel delineare l'organizzazione, le politiche e i progetti di sicurezza.

Di conseguenza, l'organizzazione della sicurezza dovrebbe partire dagli individui, top manager e personale delegato, che per legge sono ritenuti proprietari e custodi delle informazioni e pertanto responsabili delle eventuali violazioni da parte dell'intero personale aziendale e responsabili dei danni verso terzi che ne conseguono. Dopo di

che, la partecipazione dovrebbe allargarsi a tutti i livelli. Il management di livello superiore ha la visione globale dell'azienda e degli obiettivi di business. I manager intermedi sanno come funzionano i propri dipartimenti, conoscono il ruolo degli individui e possono valutare l'impatto diretto della sicurezza nelle loro aree. I manager di livello inferiore e lo staff sono a contatto con l'effettiva operatività dell'azienda e conoscono in dettaglio le esigenze tecniche e procedurali, i sistemi e il loro utilizzo; utilizzano i meccanismi di sicurezza nel lavoro quotidiano e sanno come essi si integrano nei sistemi e nei flussi di lavoro e come influiscono sulla produttività.

Il ruolo delle politiche di sicurezza

Di solito, le informazioni e le risorse informatiche hanno una relazione diretta con gli obiettivi e con l'esistenza stessa di un'azienda. Il management di livello superiore dovrebbe perciò considerare prioritaria la loro protezione, definendo gli obiettivi della sicurezza, fornendo il supporto e le risorse necessari e avviando il programma di sicurezza aziendale. Il management deve definire la sfera d'azione della sicurezza, che cosa deve essere protetto e in che misura, tenendo conto delle leggi vigenti e dei risultati dell'analisi del rischio. Quindi deve precisare ciò che ci si aspetta dal personale e le conseguenze delle violazioni. Un programma di sicurezza dovrebbe contenere tutti gli elementi necessari a fornire all'azienda una protezione completa secondo una strategia a lungo termine. Questi elementi comprendono tra l'altro le politiche di sicurezza, le procedure, gli standard, le linee guida, i criteri minimi di sicurezza, le azioni di sensibilizzazione e addestramento, le modalità di reazione agli incidenti e un programma per il controllo della sicurezza.

La definizione delle politiche di sicurezza a livello aziendale è il primo risultato dell'organizzazione di sicurezza. Una politica di sicurezza è un documento sintetico in cui il management superiore, o un comitato delegato allo scopo, delinea il ruolo della sicurezza nell'organizzazione o in un suo aspetto particolare.

Generalmente sono necessarie diverse politiche di sicurezza a più livelli, da quello superiore riguardante l'intera azienda, scendendo ad argomenti più specifici, come il sistema informatico e i singoli aspetti tecnici. Il linguaggio, il livello di dettaglio e il formalismo dei documenti di sicurezza dovranno essere realistici per avere efficacia. Un'organizzazione altamente strutturata sarà più portata a seguire politiche e linee guida dettagliate, mentre un'azienda meno strutturata richiederà maggiori spiegazioni e una particolare enfasi per ottenere l'applicazione delle misure di sicurezza.

La terminologia usata per individuare i livelli principali delle politiche di sicurezza può variare. In una grande organizzazione si può parlare di organizational security policy, issue-specific policies e system-specific policies per indicare le politiche di sicurezza aziendale, le politiche per l'implementazione di funzioni di sicurezza specifiche e quelle riguardanti direttamente i computer, le reti, il software e i dati.

Un'altra suddivisione, applicabile anche su scala medio-piccola, individua tre livelli: la politica di sicurezza aziendale (corporate security policy), la politica di sicurezza per il sistema informativo (system security policy) e la politica di sicurezza tecnica (technical security policy).

La **politica di sicurezza aziendale** indica tutto ciò che deve essere protetto (beni materiali e immateriali) in funzione del tipo di attività dell'azienda, del modello di business, dei vincoli esterni (mercato, competizione, leggi vigenti) e dei fattori di rischio. Questo documento definisce gli obiettivi del programma di sicurezza, assegna le responsabilità per la protezione dei beni e l'implementazione delle misure e attività di sicurezza e delinea come il programma deve essere eseguito. La politica di sicurezza aziendale fornisce la portata e la direzione di tutte le future attività di sicurezza all'interno dell'organizzazione, incluso il livello di rischio che il management è disposto ad accettare.

La **politica di sicurezza del sistema informatico** definisce, coerentemente con la politica di sicurezza aziendale, in che modo l'azienda intende proteggere le informazioni e le risorse informatiche, senza entrare nel merito delle tecnologie che verranno adottate. In questa fase vengono presi in considerazione requisiti di sicurezza di tipo fisico e procedurale, mentre gli aspetti tecnici sono demandati al livello inferiore.

La **politica di sicurezza tecnica** traduce in requisiti tecnici funzionali gli obiettivi che si desidera raggiungere attraverso le contromisure di tipo tecnico informatico, nel contesto dell'architettura di sistema adottata o pianificata dall'azienda.

In un'azienda di piccole dimensioni potranno essere sufficienti singole politiche di sicurezza per ciascuno dei due livelli inferiori, ma in presenza di più sistemi, dipartimenti e divisioni, è probabile che le politiche di sicurezza si suddividano per area e per argomento. (Esempi di politiche di sicurezza sono forniti dal SANS Institute alla pagina http://www.sans.org/resources/policies/).

Disaster Recovery e Business Continuity

La Disaster Recovery, nel contesto informatico, è la capacità di un'infrastruttura di riprendere le operazioni dopo un disastro. La maggior parte dei grandi sistemi di calcolo include programmi di disaster recovery, inoltre esistono applicazioni di disaster recovery autonome che, periodicamente, registrano lo stato corrente del sistema e delle applicazioni, in modo da poter ripristinare le operazioni in un tempo minimo. Il termine disaster recovery può essere usato sia dal punto di vista della prevenzione contro la perdita di dati sia delle azioni per rimediare a un disastro.

Due caratteristiche per valutare l'efficacia di un sistema di disaster recovery sono il **Recovery Point Objective** (RPO, il momento nel tempo a cui il sistema è riportato) e il **Recovery Time Objective** (RTO, il lasso di tempo che intercorre prima di ripristinare l'infrastruttura). Per ridurre la distanza dell'RPO rispetto al presente occorre incrementare il sincronismo della data replication, ovvero la replica di archivi e database su un altro sistema, generalmente remoto per motivi di sicurezza. Per ridurre l'RTO, ossia il tempo di ripristino, occorre che i dati siano tenuti on line su un sistema di riserva pronto a subentrare in caso di avaria al sistema principale.

La **business continuity** (talvolta chiamata business continuance) descrive i processi e le procedure che un'organizzazione mette in atto per assicurare che le funzioni essenziali rimangano operative durante e dopo un disastro. Il Business Continuity Planning cerca di prevenire l'interruzione dei servizi critici e di ripristinare la piena operatività nel modo più rapido e indolore possibile.

Il primo passo nel pianificare la business continuity è decidere quali delle funzioni aziendali sono essenziali e destinare di conseguenza il budget disponibile. Una volta che siano identificati i componenti principali, si possono installare i meccanismi di failover (sistemi di riserva che subentrano in caso di avaria). Tecnologie appropriate, come la replica dei database o il mirroring dei dischi su Internet, permettono a un'organizzazione di mantenere copie aggiornate dei dati in ubicazioni remote, in modo che l'accesso ai dati sia garantito anche quando un'installazione cessa di funzionare.

Un piano di business continuity dovrebbe includere: un piano di disaster recovery che specifichi le strategie per le procedure in caso di disastro; un piano di business resumption che specifichi i mezzi per mantenere i servizi essenziali presso il luogo di crisi; un piano di business recovery che specifichi i mezzi per ripristinare le funzioni azien-

5.1.3 Organizzazione della sicurezza

5.1.3.1 conoscere il ruolo delle politiche di sicurezza nel guidare il management della sicurezza IT.

5.1.3 Organizzazione della sicurezza

5.1.3.3 essere consapevoli delle necessità di pianificare la continuità operativa dell'azienda (business continuity) e il ripristino dopo un disastro (disaster recovery).

dali in una località alternativa e un contingency plan che specifichi il modo di reagire a eventi esterni che causino un serio impatto sull'organizzazione.

Nel mondo degli affari, il disaster recovery planning si sta evolvendo verso il business continuity planning da parecchi anni e i recenti eventi terroristici hanno accelerato questa tendenza. Già nel 1995 il Disaster Recovery Institute International ha rimpiazzato la designazione di Certified Disaster Recovery Planner (CDRP) con quella di Certified Business Continuity Planner (CBCP).

La differenza tra disaster recovery e business continuity è che un piano di disaster recovery è reattivo e si focalizza di solito sul ripristino dell'infrastruttura informatica. Sebbene sia logico irrobustire l'infrastruttura informatica per prevenire un disastro, lo scopo principale del piano di disaster recovery è rimediare ai danni all'infrastruttura. Al contrario, un piano di business continuity non soltanto è proattivo, ma ha anche l'obiettivo di mantenere in funzione le attività dell'azienda durante qualsiasi evento, non limitandosi a ripristinare i computer dopo il fatto.

Come parte del processo di pianificazione della business continuity, un'azienda dovrebbe riesaminare la continuità o il ripristino di produzione, imballaggio, stoccaggio, spedizione, supporto clienti e qualsiasi altra struttura o funzione critica per la sopravvivenza dell'azienda. Un fattore chiave per un piano di continuità funzionale è il coinvolgimento degli utenti, in modo da non trascurare procedure, attrezzature, documentazione e altre necessità necessarie per ripristinare i processi di business, non soltanto l'hardware e il software.

Un piccolo esempio della differenza tra ripristino dopo un disastro e continuità operativa viene offerto dall'uso personale del computer. L'utente che si organizza per un rudimentale disaster recovery, tiene backup periodici dei dati e dei file importanti e tiene sotto mano il software originale; se il sistema si blocca o l'hard disk si guasta, reinstalla il sistema operativo e le applicazioni, applica di nuovo tutte le personalizzazioni (Windows, e-mail, Internet, applicazioni eccetera) e ripristina i dati dal backup, perdendo solo le aggiunte e le modifiche successive all'ultimo backup.

L'utente orientato alla business continuity si attrezza con almeno due hard disk e un software di backup automatico delle immagini delle partizioni di disco; quindi pianifica copie complete settimanali e copie incrementali giornaliere.

Se si è dotato di un hard disk di backup ben dimensionato, può anche conservare più immagini delle partizioni per scegliere quale ripristinare secondo le circostanze (per esempio una più affidabile o una più aggiornata). Anche se si guasta il disco principale, basta sostituirlo e ripristinare le partizioni dai file immagine per riprendere la normale operatività in poco tempo (può bastare un'ora), senza reinstallare nulla.

In sintesi, l'obiettivo generale delle attività di sicurezza è mantenere la continuità del business aziendale e, in particolare, del lavoro del personale e del servizio ai clienti. Hardware, software, sistemi, reti, informazioni, attrezzature e personale sono elementi da proteggere, ma vanno inquadrati nel piano di sicurezza generale con l'obiettivo di assicurare la continuità operativa.

5.1.3 Organizzazione della sicurezza

5.1.3.4 conoscere le responsabilità di tutti i ruoli coinvolti in un'organizzazione (addetti alla sicurezza, amministratori di sistema, utenti qualunque).

Strati di responsabilità

Ogni membro del personale di un'azienda, dalla cima al fondo dell'organigramma, ha una parte di responsabilità per le condizioni operative dell'azienda e, in particolare, per il mantenimento e il miglioramento della sicurezza.

Il **management superiore** ha la responsabilità di tracciare obiettivi e strategie a lungo termine per l'intera azienda; inoltre ha la responsabilità globale per la sicurezza dell'azienda e per la protezione dei beni. In base alle leggi vigenti, ai beni da proteggere, ai rischi da controllare e agli altri fattori, spetta al management superiore dar vita a un'organizzazione di sicurezza, assegnare gli obiettivi di sicurezza, fornire i mezzi per raggiungerli e far sì che l'intero personale partecipi agli obiettivi e osservi le politiche, le linee guida, le procedure e le direttive in materia di sicurezza.

Il **management di livello divisionale e dipartimentale**, avendo conoscenza diretta del funzionamento dei propri dipartimenti e delle mansioni del personale, ha la responsabilità di contribuire alla formazione delle politiche di sicurezza, di partecipare ai processi di analisi e di controllo del rischio, all'analisi costi/benefici delle contromisure e al monitoraggio delle attività di sicurezza, delegando parte dei compiti, ma condividendo le responsabilità con il management operativo, gli specialisti di sicurezza, i system administrator, gli auditor e gli utenti.

I **manager operativi e lo staff** sono a contatto con l'effettiva operatività dell'azienda e conoscono in dettaglio i requisiti tecnici e procedurali, i sistemi e il loro utilizzo. Il loro compito è fornire informazioni utili per pianificare, organizzare e monitorare i programmi di sicurezza e implementare le politiche, le linee guida e le procedure stabilite dal management e dall'organizzazione di sicurezza.

Gli **esperti di sicurezza**, sia che si tratti di funzionari o di dirigenti interni (come security officer o Chief Information Officer) o di professionisti esterni, hanno la funzione e la responsabilità di realizzare gli obiettivi di sicurezza e di implementare le direttive del management superiore. Gli esperti di sicurezza, grazie alla loro competenza specifica, sono un fattore chiave per dare solide fondamenta all'organizzazione di sicurezza e per metterne in funzione i processi, inclusi i meccanismi di monitoraggio e controllo per mantenere la rotta senza un rilassamento delle policy, delle linee guida, degli standard e delle procedure. Una delle principali responsabilità degli esperti di sicurezza è il coinvolgimento del management, a cui spetta la firma su ogni decisione e direttiva dopo aver recepito requisiti, informazioni e analisi dal gruppo di sicurezza e dal personale (coinvolto tramite questionari, interviste ecc.).

Due ruoli importanti per la sicurezza, che devono essere chiaramente definiti, sono il proprietario dei dati e il custode dei dati.

Il **proprietario dei dati** è generalmente un membro del management superiore ed è, in definitiva, il massimo responsabile della protezione delle informazioni e della sicurezza in generale. A lui verrà imputata ogni negligenza che abbia come conseguenza la perdita o la divulgazione illecita delle informazioni e i danni conseguenti. Le violazioni vanno dalla inosservanza della legge sulla privacy (per esempio consentendo l'accesso illegale al database tramite Internet) alla copia illecita di dati soggetti a copyright (come software, musica e film scaricati dai dipendenti) alla inadeguata implementazione di procedure di disaster recovery e business continuity (gli azionisti potrebbero denunciare inadempienze che causino grosse perdite all'azienda).

Il **custode dei dati** ha la responsabilità della manutenzione e della protezione dei dati, un ruolo che di solito è ricoperto dal system administrator o, in una grande azienda, da un ruolo senior a system administrator e network administrator. Tra le funzioni ci sono l'esecuzione di backup periodici (generalmente secondo una strategia a più livelli, con diversi tipi di supporto, diverse periodicità e, nel caso dei database, sistemi di replicazione remota sincroni o asincroni secondo i requisiti). Deve inoltre implementare i meccanismi di sicurezza, validare periodicamente l'integrità dei dati e dei supporti (sia on line sia di backup), ripristinare i dati (e i programmi) dai backup quando necessario e soddisfare i requisiti delle politiche di sicurezza, degli standard e delle linee guida che riguardano la sicurezza delle informazioni e la protezione dei dati. In particolare, un system administrator è responsabile dei singoli computer

e dispositivi collegati, mentre un network administrator è responsabile delle connessioni, dell'hardware e del software di networking, oltre che del funzionamento in rete dei computer e delle periferiche. Nelle aziende piccole le due figure si sovrappongono.

Gli **utenti** sono tutti gli individui che quotidianamente utilizzano i dati per motivi di lavoro. Ogni utente dovrebbe avere i privilegi di accesso necessari per svolgere le proprie mansioni ed è responsabile di applicare le procedure di sicurezza per preservare la disponibilità, l'integrità e la riservatezza delle informazioni.

Una cattiva gestione della sicurezza, non conforme agli strati di responsabilità, causa buona parte dei problemi in tale campo. L'organizzazione della sicurezza dovrebbe prevedere un comitato di alto livello per assicurare che le istanze di sicurezza ricevano la dovuta attenzione da parte del management superiore.

Un **CIO** (*Chief Information Officer*) o security officer dovrebbe lavorare con il management superiore per definire le procedure di sicurezza strategiche e supportare i business manager nel definire le loro necessità in tema di informazioni e sicurezza. I business manager (responsabili ad esempio di attività commerciali, di marketing, di rapporti con i clienti, di progetti di espansione) hanno la principale responsabilità nel determinare i requisiti di protezione delle risorse informative, quindi dovrebbero essere coinvolti direttamente nella scelta delle misure di protezione. Spetta ai business manager anche approvare i nuovi account degli utenti, mentre gli amministratori della sicurezza creano gli account, assegnano le password, si occupano del software di sicurezza, testano le patch prima di applicarle ai sistemi.

Le decisioni sui beni da proteggere e sulle contromisure da adottare sono compito del management superiore (assistito dallo staff e dagli organismi predisposti), non dei system administrator e dei professionisti della sicurezza. Un errore molto frequente è gestire la sicurezza a livello di security administrator o system administrator. In tal caso, la sicurezza non è vista nei termini ampi e generali che richiede, non viene eseguita alcuna analisi del rischio, un'attività che richiede le valutazioni del management superiore e quest'ultimo non prende consapevolezza dei rischi a cui l'azienda è esposta. Inoltre, non vengono stanziati i fondi necessari per le attività di sicurezza e non viene svolta opera globale di sensibilizzazione ed educazione del personale.

Il dipartimento del Personale ha responsabilità specifiche in tema di sicurezza. Metà dei problemi di sicurezza sono originati da cause interne alle aziende, sia per carenze nella gestione della sicurezza sia per pratiche di reclutamento inadeguate. Al dipartimento del Personale spetta assumere o ingaggiare personale qualificato, verificare il curriculum di studi e lavoro e le informazioni personali, far firmare un impegno di non divulgazione delle informazioni (e di rispetto del copyright).

Spetta sempre al dipartimento del personale fornire l'addestramento necessario, imporre uno stretto controllo degli accessi, monitorare l'utilizzo dei sistemi e, in caso di violazione, provvedere immediatamente per impedire ulteriori danni e proteggere le informazioni, le risorse e tutte le parti interessate (non dimentichiamo la condanna dell'amministratore delegato per i film pirata scaricati abusivamente dall'impiegato).

CERT, CSIRT e la gestione degli incidenti

Con la diffusione delle connessioni in rete e l'espansione di Internet, dopo i primi attacchi si sentì l'esigenza di costituire organizzazioni per reagire prontamente a eventi che minacciassero la sicurezza dei computer collegati a Internet. Il primo **Computer Emergency Response Team** (CERT, squadra di intervento per le emergenze informatiche) fu creato negli USA dalla DARPA (*Defense Advanced Research Projects Agency*), nel novembre 1988, in risposta al primo grave attacco alla rete, quando un worm mandò in avaria il 10% di Internet.

La missione del CERT è quella di operare con la comunità di Internet per facilitare la risposta agli eventi riguardanti la sicurezza degli host (i computer collegati a Internet), prendere iniziative per sensibilizzare la comunità sugli aspetti della sicurezza e condurre ricerche rivolte a incrementare la sicurezza dei sistemi esistenti.

Il primo CERT (www.cert.org) è diventato il CERT Coordination Center (CERT-CC) ed è situato presso il Software Engineering Institute, finanziato dal governo USA e gestito dalla Carnegie Mellon University di Pittsburg.

Si focalizza sulle violazioni alla sicurezza, allerta sulle nuove minacce, reagisce agli attacchi (i cosiddetti incidents) e fornisce assistenza, informazioni sulla vulnerabilità dei prodotti e istruzione con documenti e tutorial.

Nel 2003 è stato formato lo United States Computer Emergency Readiness Team (US-CERT, www.us-cert.gov), una partnership tra il Department of Homeland Security (nato nel 2002 per fronteggiare gli attacchi terroristici in USA) e il settore privato.

L'US-CERT opera a Washington e a Pittsburg, in stretto coordinamento con il CERT-Coordination Center. Il suo compito è analizzare e ridurre le minacce e vulnerabilità informatiche, disseminare informazioni per allertare sulle nuove minacce e coordinare le attività di risposta agli incidenti.

Vista la dimensione delle reti, il numero di comunità di utenti e la richiesta di supporto per fronteggiare i problemi di sicurezza, il **CERT-CC** è impegnato ad aiutare la formazione degli **CSIRT** (*Computer Security Incident Response Team*), squadre di intervento per gli incidenti di sicurezza informatica, a cui fornisce guida e addestramento. Nella maggior parte delle aziende, i system e network administrator non hanno a disposizione personale, competenze e procedure per fronteggiare prontamente gli attacchi informatici e minimizzare i danni, come dimostra il numero crescente di incidenti di sicurezza.

In questi casi è necessaria una risposta rapida ed efficace; più tempo trascorre per riconoscere, analizzare e rispondere a un incidente, maggiori sono i danni e i costi di ripristino. Le grandi organizzazioni hanno la possibilità di crearsi il proprio CSIRT, come avviene negli USA con l'aiuto del CERT CSIRT Development Team.

In alternativa, si ricorre a gruppi di intervento pubblici, come il **CERT-IT** (http://security.dico.unimi.it) e il **GARR-CERT** (www.cert.garr.it) entrambi italiani.

I CERT o CSIRT delle varie nazioni sono collegati in una struttura internazionale che permette la rapida condivisione delle informazioni utili a fronteggiare minacce e attacchi. Il **FIRST** (*Forum for Incident Response and Security Teams*, www.first.org) è nato nel 1990.

Nel 2003 FIRST contava la partecipazione di 150 organizzazioni per la risposta agli incidenti di sicurezza in ogni parte del mondo. Il **CERT-IT**, ubicato presso l'Istituto di Scienza dell'Informazione dell'Università degli Studi di Milano, è il primo membro italiano di FIRST, a cui è stato ammesso nel 1995.

La segnalazione degli incidenti al CERT-IT avviene in forma riservata e autenticata tramite PGP (Pretty Good Privacy), un programma di cifratura gratuito usato da milioni di utenti per proteggere la riservatezza della posta elettronica (www.it.pgpi.org). La gestione degli incidenti prevede tre fasi:

1) la segnalazione dell'incidente, via e-mail o via Web, con allegate le informazioni sull'attacco e i file rilevanti (come quelli di log);

2) la registrazione dell'incidente da parte del CERT-IT e l'indagine sull'attacco fino a informare l'utente, se le informazioni fornite sono sufficienti, sui rimedi da adottare;

3) la chiusura della segnalazione.

5.1.3 Organizzazione della sicurezza

5.1.3.5 sapere come partecipare a una squadra d'intervento per le emergenze informatiche.

5.1.4 Standard ed enti di standardizzazione

5.1.4.1 conoscere i principali enti di standardizzazione e il loro ruolo.

Standard ed enti di standardizzazione

Gli enti di standardizzazione principali e il loro ruolo

Gli enti di standardizzazione sono organizzazioni di natura molto differente, che coprono aspetti normativi diversificati e hanno avuto una genesi diversa a seconda dei casi. Operano in ambito nazionale o internazionale ed emettono norme e linee guida (gli standard) che 1) permettono di realizzare prodotti, processi e servizi secondo lo stato corrente delle tecnologie e 2) forniscono le basi per garantire l'interoperabilità tra prodotti di produttori diversi. Oltre a emettere standard, questi enti svolgono altre attività, come la pubblicazione di documenti interpretativi per facilitare l'applicazione degli standard secondo determinati profili di utilizzo.

Generalmente gli enti di standardizzazione operano sulla base del consenso con un'attività di coordinamento e armonizzazione. A volte il documento che descrive uno standard è il risultato del lavoro di ricerca e sviluppo di un gruppo di aziende e un compito dell'ente di standardizzazione è far sì che le norme raggiungano un vasto campo di applicabilità nel settore industriale interessato. In qualche caso diversi gruppi industriali adottano tecnologie in concorrenza tra loro e l'ente di standardizzazione, se non prevalgono interessi economici o politici particolari, riesce ad armonizzarne le caratteristiche definendo uno standard a cui tutti i partecipanti si uniformano.

Casi di questo genere sono frequenti, per esempio nel campo delle comunicazioni e del networking, quando alla fase di rapida uscita sul mercato segue la ricerca del consenso e della massima interoperabilità. In generale, un ente di standardizzazione permette che le tecnologie con la migliore combinazione di caratteristiche e consenso siano codificate in modo da superare l'ambito locale di origine e siano applicabili uniformemente e in modo interoperabile su scala nazionale e internazionale. Gli organismi di standardizzazione possono essere istituzioni formalmente riconosciute dagli stati nazionali o essere consorzi privati di imprese che operano in un certo settore del mercato. Vediamo ora quali sono gli enti di standardizzazione rilevanti ai fini della sicurezza informatica.

- **ITU** (*International Telecommunication Union*, www.itu.int): è un'organizzazione internazionale, nell'ambito dell'ONU, dove governi e settore privato coordinano le reti e i servizi globali di telecomunicazioni. Ha sede a Ginevra e comprende i settori ITU-T (standardizzazione), ITU-R (radiocomunicazioni) e ITU-D (sviluppo). Ai fini della sicurezza delle informazioni, sono di interesse le raccomandazioni ITU-T della serie X.500 (servizi di directory) e, in particolare, la norma X.509 che descrive il formato dei certificati digitali.

- **ISO** (*International Organization for Standardization*, www.iso.org): è la maggiore organizzazione internazionale di standardizzazione e comprende gli enti di standardizzazione nazionali di 146 paesi (l'UNI è il membro italiano). L'ISO, il cui nome non è un acronimo ma deriva dalla parola greca isos - uguale - ha sede a Ginevra e opera a stretto contatto con IEC (International Electrotechnical Commission), ITU, CEN (Comitato Europeo di Normalizzazione) e CESI (Centro Elettrotecnico Sperimentale Italiano). Le norme ITU X.500, in realtà, sono state emesse congiuntamente all'ISO e sono contenute nella serie ISO 9594. ISO/IEC/JTC1 è il comitato che si occupa di standardizzazione nel campo dell'ICT (http://www.jtc1.org). I membri del JTC1 (Joint Technical Committee 1) sono gli enti nazionali di standardizzazione IT. Il JTC 1 è responsabile della gestione di un vasto e complesso programma di lavoro ed è strutturato in sottocomitati e gruppi di lavoro in base alle aree di interesse. Il sottocomitato 27 (ISO/IEC JTC1/SC27) è quello che si occupa di tecniche di sicurezza e vi partecipa, per l'Italia, l'UNINFO.

- **IETF** (*Internet Engineering Task Force,* www.ietf.org): è una vasta comunità internazionale di progettisti, operatori, produttori e ricercatori nel campo del networking, interessati all'evoluzione dell'architettura di Internet e all'affidabilità del suo funzionamento. È aperta a tutti gli interessati e il lavoro tecnico effettivo è svolto dai gruppi di lavoro, che sono organizzati per argomento in aree come routing, trasporto, sicurezza e così via. L'IETF emette norme sotto forma di *Request For Comment* (RFC). Ne fa parte la serie dedicata alle infrastrutture a chiave pubblica, normalmente indicate con la sigla PKIX (Internet X.509 Public Key Infrastructure).

- **CEN** (*Comitato Europeo di Normalizzazione, www.cenorm.org*): è un organismo europeo composto dagli enti di standardizzazione dei paesi membri dell'Unione Europea e dell'EFTA (*European Fair Trade Association* - tra cui l'UNI per l'Italia). CEN, CENELEC ed ETSI sono i tre enti europei di standardizzazione a cui è riconosciuta la competenza nell'area della standardizzazione tecnica su base volontaria e che sono elencati nell'Allegato I della Direttiva 98/34/EC riguardante la "procedura informativa" per gli standard e la normativa tecnica. Insieme, essi preparano gli standard europei in settori di attività specifici e costituiscono il "sistema di standardizzazione europeo". La maggior parte degli standard è preparata su richiesta dell'industria, ma anche la Commissione Europea può farne richiesta. Le direttive UE normalmente contengono principi generali obbligatori, demandando i requisiti tecnici dettagliati agli enti di standardizzazione. Il CENELEC è il Comitato Europeo per la Standardizzazione Elettrotecnica (www.cenelec.org). L'EFTA (European Fair Trade Association, www.eftafairtrade.org) è lo spazio di libero scambio nato nel 1960 tra Austria, Danimarca, Norvegia, Portogallo, Svezia, Svizzera e Gran Bretagna.

- **ETSI** (*European Telecommunications Standards Institute,* www.etsi.org): è un'organizzazione europea indipendente, riconosciuta dalla Commissione Europea e dall'EFTA. Ha sede a Sophia Antipolis (Francia) ed è responsabile per la standardizzazione delle tecnologie informatiche e di comunicazioni (ICT) in Europa. Queste tecnologie includono le telecomunicazioni, il broadcasting e le aree collegate come i trasporti intelligenti e l'elettronica medica. L'ETSI raggruppa 688 membri in 55 nazioni (dato di febbraio 2005) dentro e fuori l'Europa, tra cui produttori, gestori di reti, amministratori, service provider, enti di ricerca e utenti. Tra i campi d'interesse, l'ETSI si occupa di algoritmi di sicurezza e di servizi TTP (*Trusted Third Party Services*); tra i progetti, segnaliamo l'European Electronic Signature Standardization Initiative (www.ict.etsi.org/EESSI_home.htm), che tra il 1999 e il 2004 ha coordinato l'attività di standardizzazione per implementare la direttiva CE sulla firma elettronica.

- **UNINFO** (www.uninfo.polito.it): è una libera associazione a carattere tecnico, con lo scopo di promuovere e di partecipare allo sviluppo della normativa nel settore delle tecniche informatiche. Rientrano nel suo campo d'attività i sistemi di elaborazione e di trasmissione delle informazioni e le loro applicazioni nelle più diverse aree, quali, ad esempio, le attività bancarie e le carte intelligenti. L'UNINFO è associato all'UNI, l'ente nazionale italiano di unificazione (www.uni.com/it) e rappresenta l'Italia presso CEN e ISO. Le attività dell'UNINFO nell'ambito della sicurezza informatica sono svolte dalla commissione STT (*Sicurezza delle Transazioni Telematiche*), che si occupa delle norme di sicurezza nelle transazioni telematiche, con particolare riferimento alla firma elettronica.

Normative relative alla sicurezza delle informazioni

L'attività normativa relativa alla sicurezza può essere suddivisa in tre aree: norme funzionali, criteri di valutazione della garanzia e norme relative al sistema di gestione della sicurezza.

1) **Norme funzionali**: queste sono relative ai prodotti e hanno lo scopo principale di ricercare l'interoperabilità dei prodotti informatici. Coprono argomenti quali i protocolli di comunicazione, il formato dei dati (per esempio in un certificato digitale o in una smartcard) e così via. Oltre agli standard emessi dagli enti formali di standardizzazione, ci sono numerose specifiche tecniche pubbliche emesse da associazioni e talvolta anche da industrie private. Oltre agli enti già citati, segnaliamo anche i seguenti: **ANSI**, *American National Standards Institute* (www.ansi.org), **IEC**, *Commissione Elettrotecnica Internazionale:* (www.iec.ch), **DIN**, *Deutsches Institut für Normung* (www.din.de), SEIS, *Swedish Secured Electronic Information in Society Specifications, Sweden* (www.seis.se).Tra le associazioni, oltre al citato IETF, segnaliamo l'**IEEE**, *Institute of Electrical and Electronics Engineers* (www.ieee.org.). Tra gli standard di aziende private segnaliamo la serie **PKCS#1-15** (*Public Key Cryptography Standards*) di RSA Security (www.rsa.com).
2) **Criteri di valutazione della garanzia**: sono i metodi con cui viene valutata la fiducia che può essere accordata ai sistemi e ai prodotti informatici di sicurezza. Tra le pubblicazioni disponibili, le tre più significative sono i criteri americani **TCSEC** (Trusted Computing Security Evaluation Criteria, 1985), i criteri europei ITSEC (Information Security Evaluation Criteria, 1991) e i criteri internazionali **ISO/IEC 15408**, noti come **Common Criteria** e pubblicati nel 1999.
3) **Norme e linee guida relative al sistema di gestione della sicurezza nell'azienda**: segnaliamo le linee guida ISO/IEC 13335 (Part 1: Concepts and models for IT Security, Part 2: Managing and planning IT Security, Part 3: Techniques for the management of IT Security, Part 4: Selection of safeguards, Part 5: Management guidance on network security) e le norme BS (British Standard) 7799 (Part 1: Code of Practice, recepita dalla ISO/IEC 17799 Code of practice for information security management del 2000 e Part 2: Controls, riveduta nel 2002).

I criteri per la valutazione della garanzia

Abbiamo visto in precedenza che i sistemi di sicurezza sono caratterizzati dalla funzionalità (quello che il sistema deve fare per la sicurezza) e dalla garanzia (la fiducia nella protezione offerta dalla funzionalità), a sua volta costituita da correttezza (qualità di implementazione della funzionalità) e da efficacia (in quale grado la contromisura protegge dalle minacce).

Le tre fonti citate sopra a proposito dei criteri di valutazione della garanzia si chiamano appunto criteri di valutazione, anziché norme o standard, perché, sia pure con diversa attenzione ai requisiti funzionali, tutti si esprimono sui livelli di garanzia, un concetto troppo astratto per essere ridotto a uno standard. In ogni caso, TCSEC mischia funzionalità e garanzia, ITSEC tenta di separare le due categorie, ma non ci riesce del tutto, mentre questo risultato è stato raggiunto nei Common Criteria, più efficaci e agevoli da applicare.

I criteri di valutazione dei processi di sicurezza hanno seguito idee e metodi diversi nel tempo e nelle varie aree geografiche. Oggi il TCSEC viene considerato troppo rigido, l'ITSEC troppo morbido e complicato e i Common Criteria accettabili da tutti.

Il **TCSEC** è stato sviluppato dal Dipartimento della Difesa USA e pubblicato dal National Computer Security Center (parte della National Security Agency) nel cosiddetto Orange Book del 1985. Sebbene in Europa possa essere visto come superato, nella cultura di sicurezza americana occupa ancora uno spazio rilevante ed è considerato indicativo delle esigenze di sicurezza degli ambienti militari.

Il TCSEC serve per valutare sistemi operativi, applicazioni e prodotti di vario genere. I criteri di valutazione sono stati pubblicati in un volume dalla copertina arancione, detto perciò **Orange Book**. Le valutazioni di sicurezza risultanti dall'applicazione del TCSEC servono ai compratori per confrontare diverse soluzioni e ai produttori per sapere a quali specifiche conformarsi.

L'Orange Book viene usato per accertare se i prodotti offrono le caratteristiche di sicurezza dichiarate e per valutare se un prodotto è appropriato per una funzione o applicazione specifica. Durante la valutazione, l'Orange Book prende in considerazione la funzionalità e la garanzia di un sistema e fornisce un sistema di classificazione suddiviso in una gerarchia di livelli di sicurezza:

A. Protezione verificata
B. Protezione obbligatoria
C. Protezione discrezionale
D. Sicurezza minima.

Ognuna delle quattro divisioni, da A (massima sicurezza) a D (minima sicurezza), può avere una o più classi di sicurezza, ognuna numerata e corrispondente a un certo insieme di requisiti da soddisfare. Le classi con numero superiore indicano un maggiore grado di fiducia e garanzia. I criteri di valutazione includono quattro argomenti principali: politiche di sicurezza, rendicontabilità (accountability), garanzia (assurance) e documentazione, ciascuna delle quali si suddivide in sei aree:

- Politiche di sicurezza (la policy deve essere esplicita e ben definita e imposta da meccanismi interni al sistema)
- Identificazione (i singoli soggetti devono essere identificati)
- Etichette (le etichette per il controllo degli accessi devono essere associate in modo appropriato agli oggetti)
- Rendicontabilità (si devono raccogliere e proteggere i dati di audit per imporre la rendicontabilità)
- Garanzia del ciclo di vita (software, hardware e firmware devono poter essere testati individualmente per assicurare che ciascuno imponga la politica di sicurezza in modo efficace per tutto il ciclo di vita)
- Protezione continua (i meccanismi di sicurezza e l'intero sistema devono funzionare con continuità in modo prevedibile e accettabile in tutte le diverse situazioni).

Queste categorie sono valutate in modo indipendente, ma alla fine viene assegnata una valutazione complessiva. Ogni divisione e classe di sicurezza include i requisiti delle classi e divisioni inferiori (per esempio la B2 include i requisiti di B1, C2 e C1).

Le classi sono: **C1** (protezione di sicurezza discrezionale), **C2** (protezione ad accessi controllati), **B1** (protezione obbligatoria), **B2** (protezione strutturata), **B3** (domini di sicurezza) e **A1** (progetto controllato). TCSEC s'indirizza alla riservatezza, ma non all'integrità. Mette grande enfasi su controllare quali utenti possono accedere al sistema e ignora praticamente che utilizzo costoro facciano delle informazioni. Funzionalità e garanzia dei meccanismi di sicurezza non sono valutate separatamente, ma combinate tra loro.

Viste le numerose carenze dell'Orange Book, specialmente se applicato in ambito civile, furono pubblicate diverse estensioni, in quella che prese il nome di Rainbow Series (serie arcobaleno). Ne fa parte il Trusted Network Interpretation (TNI), detto Red Book, che si occupa di sicurezza delle reti, uno dei tanti argomenti non trattati dall'Orange Book.

L'**ITSEC** è stato il primo tentativo di stabilire un unico standard di valutazione degli attributi di sicurezza da parte di molti paesi europei. Durante gli anni '80, Regno Uni-

5.1.4 Standard ed enti di standardizzazione

5.1.4.3 conoscere le differenze essenziali tra gli standard pubblicati (ISO/IEC 17799, BS 7799 part 2) nati come supporto per la costruzione di un'infrastruttura di gestione della sicurezza all'interno di un'organizzazione.

5.1.4 Standard ed enti di standardizzazione

5.1.4.2 conoscere la disponibilità di una metodologia per valutare i diversi livelli di garanzia (ITSEC, Common Criteria).

to, Germania, Francia e Olanda avevano prodotto versioni dei loro criteri nazionali, in seguito armonizzate e pubblicate come **Information Technology Security Evaluation Criteria** (ITSEC).

La versione 1.2 corrente è stata pubblicata nel 1991 dalla Commissione Europea, a cui ha fatto seguito nel 1993 l'IT Security Evaluation Manual (ITSEM) che specifica la metodologia da seguire per realizzare le valutazioni ITSEC.

L'innovazione rispetto al TCSEC è stato il tentativo di rendere indipendente la definizione delle funzionalità, così da poter applicare i criteri ITSEC a un ampio spettro di prodotti e sistemi, che nel gergo ITSEC si chiamano **TOE** (*target of evaluation*).

La definizione delle funzionalità di sicurezza è scorporata in un documento chiamato **Security Target**, che descrive le funzionalità offerte dal TOE e l'ambiente operativo del TOE. Nel caso di un sistema, il Security Target contiene una System Security Policy (regole operative definite su misura per uno specifico ambiente operativo).

La valutazione ITSEC viene eseguita da terze parti chiamate CLEF (*Commercial Licensed Evaluation Facility*) a cui spetta fornire le certificazioni di conformità ai requisiti di sicurezza. Il processo ISEC inizia con lo sponsor (di solito lo sviluppatore del prodotto, o TOE) che nomina un CLEF. Il CLEF valuta il Security Target e produce un piano di lavoro. Viene nominato un certificatore e il processo ha inizio. Lo sponsor fornisce tutto il materiale al valutatore, che valuta se esso soddisfa i requisiti in termini di completezza, coerenza e accuratezza. Una volta soddisfatto, il valutatore produce un report e lo sottopone al certificatore per l'approvazione. Se il certificatore è soddisfatto, produce un report di certificazione e pubblica un certificato ITSEC.

Il Security Target è il documento chiave per la valutazione e contiene il target evaluation level, ossia il livello di valutazione di sicurezza a cui il produttore aspira per commercializzare il suo prodotto in un certo mercato. Ci sono sei livelli di valutazione da E1 a E6; maggiore è il livello, maggiore è il dettaglio e il rigore richiesto ai materiali sottoposti alla valutazione.

I requisiti di efficacia sono gli stessi per i sei livelli di valutazione e sono valutati in una serie di analisi: Suitability Analysis, Binding Analysis, Ease of Use Analysis, Construction Vulnerabilities Analysis e Operational Vulnerabilities Analysis.

Per valutare la correttezza del prodotto viene prodotto il documento **Architectural Design**, che identifica ad alto livello la struttura di base del TOE, le interfacce e la suddivisione in hardware e software. Il Detailed Design è un documento che scende nei dettagli dell'Architectural Design fino a un livello di dettaglio utilizzabile come base per l'implementazione. Durante il processo di valutazione, viene verificato se le specifiche di sicurezza del Detailed Design sono implementate correttamente e vengono esaminati i sorgenti del software e i diagrammi di progetto dell'hardware.

Ulteriori materiali forniti dal produttore per la valutazione includono l'ambiente di sviluppo (controllo di configurazione, linguaggi di programmazione, compilatori eccetera), la documentazione operativa (guida utente e manuale di amministrazione) e l'ambiente operativo (distribuzione, configurazione, installazione e utilizzo).

L'ITSEC ha tentato di fornire un approccio più flessibile del rigido TCSEC, di separare funzionalità e garanzia e di consentire la valutazione di interi sistemi. La flessibilità ha però portato con sé la complessità, perché i valutatori possono mescolare e abbinare le valutazioni di funzionalità e garanzia, facendo proliferare le classificazioni e rendendo il processo tortuoso.

I tempi erano maturi per tentare un approccio più efficace e unificato tra aree geografiche. Nel 1990 l'ISO riconobbe l'esigenza di criteri standard di valutazione di applicabilità globale. Il progetto Common Criteria iniziò nel 1993 quando diverse organizzazioni si associarono per combinare e allineare i criteri di valutazione esistenti ed emergenti: TCSEC, ITSEC, il canadese CTCPEC (*Canadian Trusted Computer Product Evaluation Criteria*) e i criteri federali USA. Il progetto fu sviluppato attraverso la collaborazione degli enti nazionali di standardizzazione di Stati Uniti, Canada, Francia, Germania, Regno Unito e Olanda. I benefici di questo sforzo comune comprendono la riduzione della complessità del sistema di valutazione, la disponibilità di un unico linguaggio per le definizioni e per i livelli di sicurezza e, a beneficio dei produttori, l'uso di un unico insieme di requisiti per vendere i prodotti sul mercato internazionale.

La versione 1.0 dei Common Criteria è stata completata nel gennaio 1996. Sulla base di approfondite prove, valutazioni e reazioni del pubblico, la versione 1.0 subì un'estesa revisione e diede vita alla versione 2.0 dell'aprile 1998, che divenne lo standard ISO 15408 nel 1999. Il progetto ha in seguito incorporato modifiche di lieve entità che hanno prodotto la versione 2.1 dell'agosto 1999. Oggi la comunità internazionale ha adottato i CC attraverso il *Common Criteria Recognition Arrangement*, un accordo in base al quale i firmatari concordano nell'accettare i risultati delle valutazioni CC eseguite da altri membri della CCRA.

La flessibilità dell'approccio dei Common Criteria sta nel fatto che un prodotto è valutato a fronte di un certo profilo di protezione, strutturato in modo da soddisfare specifici requisiti di protezione. Rispetto all'ITSEC, di cui conserva molti aspetti, come la separazione tra funzionalità e garanzia, i Common Criteria forniscono cataloghi di funzionalità e requisiti di garanzia che rendono più formale e ripetibile la compilazione del Security Target. Alla valutazione di un prodotto viene assegnato un *Evaluation Assurance Level* (EAL) che va da 1 a 7 (massima garanzia). La completezza e il rigore dei test crescono con il livello di garanzia assegnato. I sette livelli hanno questi significati:

EAL1 testato funzionalmente
EAL2 testato strutturalmente
EAL3 testato e verificato metodicamente
EAL4 progettato, testato e riveduto metodicamente
EAL5 progettato e testato in modo semi-formale
EAL6 verifica del progetto e testing semi-formali
EAL7 verifica del progetto e testing formali

Il sistema Common Criteria utilizza i protection profile per la valutazione dei prodotti. Il protection profile contiene l'insieme di requisiti di sicurezza, il loro significato e le ragioni per cui sono necessari, oltre che il livello EAL che il prodotto deve soddisfare. Il profilo descrive le condizioni ambientali, gli obiettivi e il livello previsto per la valutazione della funzionalità e della garanzia. Viene elencata ogni vulnerabilità e come dev'essere controllata da specifici obiettivi di sicurezza. Inoltre il documento fornisce le motivazioni per il livello di garanzia e la robustezza dei meccanismi di protezione.

Nella struttura del sistema Common Criteria, il protection profile descrive la necessità di una specifica soluzione di sicurezza, che è l'input per il prodotto da valutare (TOE). Il TOE è il prodotto proposto per fornire la soluzione alle esigenze di sicurezza. Il security target è scritto dal produttore e spiega le funzionalità di sicurezza e i meccanismi di garanzia che soddisfano i requisiti di sicurezza. I Security Functionality Requirements e i Security Assurance Requirements formano dei componenti (package) riutilizzabili che descrivono gli insiemi dei requisiti di funzionalità e di garanzia da soddisfare per ottenere lo specifico EAL a cui il produttore aspira. Questi documenti di requisiti sono indipendenti dalle tecnologie con cui vengono realizzati i prodotti.

L'utilizzo di prodotti certificati, oltre a rispondere a requisiti formali di approvvigionamento, offre numerosi benefici, tra cui la disponibilità di un documento di specifi-

che di sicurezza formalizzate (il security target) contenente la descrizione delle minacce che il prodotto è in grado di contrastare e l'esistenza di test e verifiche effettuate, secondo metodologie documentate, da un ente indipendente. Le pubblicazioni relative ai Common Criteria sono inoltre di ausilio per tenere conto dei requisiti di funzionalità e di garanzia nella progettazione di sistemi informatici con requisiti di sicurezza, anche se non s'intende sottoporli al processo di certificazione.

Riferimenti:
csrc.nist.gov/cc, www.rycombe.com/cc.htm, www.clusit.it/whitepapers/iso15408-1.pdf, www.clusit.it/whitepapers/iso15408-2.pdf e www.clusit.it/whitepapers/iso15408-3.pdf

Le norme sul sistema di gestione della sicurezza

Gli sviluppi normativi nel campo dei sistemi di gestione della sicurezza delle informazioni sono avvenuti in tempi più recenti rispetto all'evoluzione dei criteri di valutazione della garanzia (come TCSEC, ITSEC e Common Criteria) e dei sistemi di gestione della qualità (come ISO 9000).

ISO/IEC ha pubblicato, tra il 1996 e il 2001, una serie di cinque documenti (ISO/IEC TR 13335), la cui sigla TR (technical report) indica che si tratta di linee guida del tipo best practice (modalità operative consigliate), non di specifiche formali. Questi documenti sono una possibile alternativa alla coppia ISO/IEC 17799 - BS 7799 di fonte britannica. Le cinque parti della serie TR 13335 sono le seguenti:

- Parte 1: **Concepts and models for IT security**. Il primo documento fornisce una panoramica dei concetti relativi alla sicurezza delle informazioni e dei modelli che un'organizzazione può utilizzare per definire la propria sicurezza IT.

- Parte 2: **Managing and planning IT security**. Questo documento si occupa degli aspetti di pianificazione e di gestione della sicurezza delle informazioni.

- Parte 3: **Techniques for the management of IT security**. Questo documento si occupa delle attività di management che sono direttamente legate al ciclo di vita dei progetti: pianificazione, progettazione, implementazione, testing eccetera.

- Parte 4: **Selection of safeguards**. In parte complementare alla parte 3, descrive la selezione delle contromisure e l'importanza e la modalità d'impiego dei modelli di sicurezza di base e delle verifiche.

- Parte 5: **Management guidance on network security**. Questo documento fornisce linee guida sulle comunicazioni e sulle reti, in particolare l'analisi dei fattori che devono essere presi in considerazione per definire requisiti di sicurezza e contromisure appropriati. Inoltre fornisce un approccio alla definizione dei livelli di fiducia basato sulla valutazione del rischio.

Le linee guida BS 7799, oggi ISO/IEC 17799 e BS 7799-2, hanno una storia che risale agli inizi degli anni '90, quando il Department of Trade and Industry britannico istituì un gruppo di lavoro con l'intento di fornire alle aziende linee guida per la gestione della sicurezza delle informazioni. Nel 1993 questo gruppo pubblicò il *Code of practice for information security management*, un insieme di buone regole di comportamento per la sicurezza delle informazioni. Questo costituì la base per lo standard BS 7799 pubblicato da BSI (British Standards Institution) nel 1995 e noto come Code of Practice. Nel 1998 BSI aggiunse la seconda parte, Specification for Information Security Management, che fu sottoposta a revisione e ripubblicata nel 1999. Il Code of Practice fu sottoposto a ISO/IEC per essere approvato come standard internazionale, una volta nel 1995 senza successo e in seguito di nuovo nel 1999 con esito positivo. Il BS 7799 Parte 1 è stato quindi recepito come ISO/IEC 17799. La sua edizione del 2000 è in corso di aggiornamento nel 2005. La seconda parte, BS 7799-2, è stata aggiornata nel 2002.

L'ISO/IEC 17799 presenta una serie di linee guida e di raccomandazioni compilata a seguito di consultazioni con le grandi aziende. I 36 obiettivi e le 127 verifiche di sicurezza contenuti nel documento sono suddivisi in 10 aree, o domini, riportati nel riquadro A, Il dieci domini formano una piramide che scende dalla prospettiva organizzativa (1, 2, 3, 4, 9, 10) verso quella operativa (6, 7, 8), con inclusi gli aspetti tecnici (5).

Le verifiche di sicurezza ulteriormente dettagliate nel documento, portano a oltre 500 il numero di controlli ed elementi di best practice dell'ISO/IEC 17799. Il documento sottolinea l'importanza della gestione del rischio e chiarisce che non è indispensabile implementare ogni singola linea guida, ma solo quelle che sono rilevanti. Lo standard copre tutte le forme d'informazione, incluse la voce, la grafica e i media come fax e cellulari. Esso riconosce anche i nuovi metodi di business, come l'e-com-

Riquadro A - Le dieci aree delle linee guida dello standard ISO/IEC 17799

1. **Security Policy.** Fornire le linee guida e i consigli per la gestione, allo scopo di migliorare la sicurezza delle informazioni
2. **Organizational Security.** Facilitare la gestione della sicurezza delle informazioni all'interno dell'organizzazione.
3. **Asset Classification and Control.** Eseguire un inventario dei beni e proteggerli efficacemente.
4. **Personnel Security.** Minimizzare i rischi di errore umano, furto, frode o uso illecito delle attrezzature.
5. **Physical and Environment Security.** Prevenire la violazione, il deterioramento o la distruzione delle attrezzature industriali e dei dati.
6. **Communications and Operations Management.** Assicurare il funzionamento adeguato e affidabile dei dispositivi di elaborazione delle informazioni.
7. **Access Control.** Controllare l'accesso alle informazioni.
8. **Systems Development and Maintenance.** Assicurare che la sicurezza sia incorporata nei sistemi informativi.
9. **Business Continuity Management.** Minimizzare l'impatto delle interruzioni dell'attività aziendale e proteggere da avarie e gravi disastri i processi aziendali essenziali.
10. **Compliance.** Evitare ogni violazione delle leggi civili e penali, dei requisiti statutari e contrattuali e dei requisiti di sicurezza.

merce, Internet, l'outsourcing, il telelevoro e il mobile computing.

Mentre l'ISO/IEC 17799 fornisce le linee guida, gli aspetti di sicurezza e le buone norme da applicare, in sé sufficienti per un'azienda medio-piccola, lo standard **BS 7799-2** fornisce le direttive per istituire un sistema di gestione della sicurezza delle informazioni (SGSI in italiano o ISMS, Information Security Management System, nella letteratura) da sottoporre alla certificazione di un ente accreditato. L'applicazione del BS 7799-2 permette all'azienda di dimostrare ai suoi partner che il proprio sistema di sicurezza è conforme allo standard e risponde alle esigenze di sicurezza determinate dai propri requisiti.

Un'organizzazione che ottiene la certificazione è considerata conforme ISO/IEC 17799 e certificata BS 7799-2.

L'aggiornamento del 2002 del BS 7799-2 ha introdotto varie modifiche suggerite dall'esigenza di dare continuità al processo di gestione della sicurezza. Il modello di ISMS definito dallo standard comprende quattro fasi in un loop ciclico, analogo a quello dell'ISO 9001.

Il modello è detto PDCA dalle iniziali delle quattro fasi: Plan (pianifica: la definizione dell'ISMS), Do (esegui: l'implementazione e utilizzo dell'ISMS), Check (verifica: i controlli e le revisioni dell'ISMS) e Act (agisci: la manutenzione e miglioramento dell'ISMS).

Le quattro fasi dell'Information Security Management System

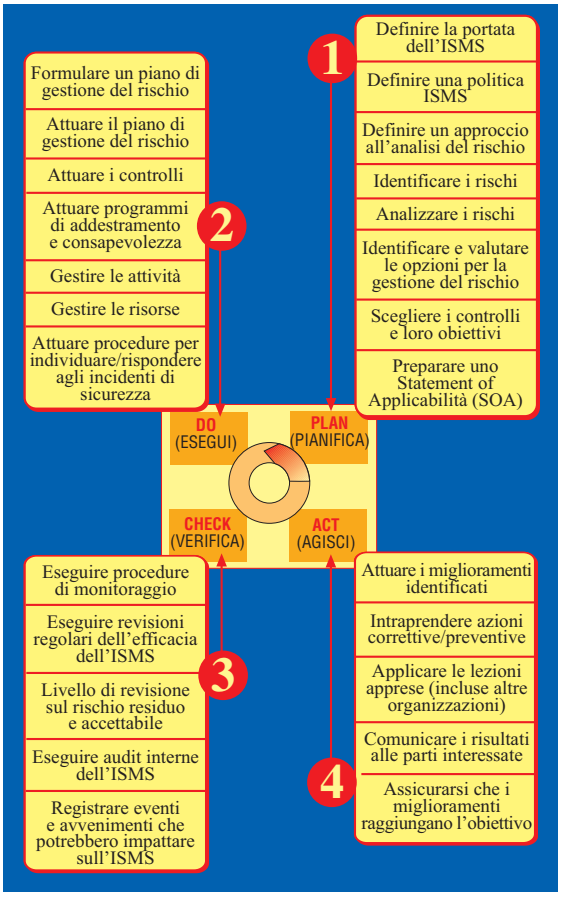
Plan:
1. la definizione dell'ambito di applicazione dell'ISMS
2. la definizione di una politica di sicurezza di alto livello
3. la definizione di un approccio sistematico per l'analisi del rischio
4. l'identificazione dei rischi
5. la valutazione dei rischi
6. l'identificazione delle opzioni per il trattamento dei rischi (eliminazione, cessione e riduzione)
7. la selezione delle contromisure per il controllo dei rischi
8. la redazione della dichiarazione di applicabilità, comprendente l'esplicitazione delle ragioni che hanno portato alla selezione delle contromisure e alla non applicazione di misure indicate nell'appendice A della norma.

Do:
1. la formulazione di un piano di trattamento dei rischi
2. l'implementazione del piano
3. l'implementazione delle contromisure selezionate
4. lo svolgimento di programmi d'informazione e di formazione
5. la gestione delle operazioni connesse alla fase Do
6. la gestione delle risorse connesse alla fase Do
7. l'implementazione di procedure e altre misure che assicurino la rilevazione e le opportune azioni in caso di incidenti relativi alla sicurezza

Check:
1. l'esecuzione delle procedure di monitoraggio dell'ISMS
2. l'esecuzione di revisioni del rischio residuo
3. la conduzione di audit interni all'ISMS
4. la conduzione di review al massimo livello dirigenziale dell'ISMS
5. la registrazione delle azioni e degli eventi che potrebbero avere impatti sulla sicurezza o sulle prestazioni dell'ISMS

Act:
1. l'implementazione delle azioni migliorative dell'ISMS identificate
2. l'implementazione delle azioni correttive e preventive
3. la comunicazione dei risultati
4. la verifica che i miglioramenti raggiungano gli obiettivi identificati alla loro base.

L'appendice A della norma BS 7799-2 del 2002 include una serie di misure per il controllo del rischio suddivise in 10 capitoli, gli stessi delle 10 aree sopra elencate per l'ISO/IEC 17799.



Le quattro fasi *dell'Information Security Management System*

Naturalmente, la conformità all'ISO/IEC 17799 o la certificazione BS 7799-2 non implicano che un'organizzazione sia sicura al 100%, un obiettivo peraltro irraggiungibile. Tuttavia, l'adozione di questo standard, apprezzato a livello internazionale, offre diversi vantaggi a livello organizzativo (efficacia dello sforzo di sicurezza a tutti i livelli, diligenza degli amministratori), a livello legale (osservanza di leggi e regolamenti), a livello operativo (gestione del rischio, qualità di hardware e dati), a livello commerciale (distinzione dalla concorrenza, partecipazione a gare), a livello finanziario (costo delle violazioni, costi assicurativi) e a livello umano (consapevolezza e responsabilità del personale). La popolarità della coppia ISO/IEC 17799 e BS 7799-2 è dovuta in parte alla sua flessibilità e alla sua complementarità con altri standard di sicurezza IT. Mentre l'ISO/IEC 17799 delinea le migliori pratiche per la gestione della sicurezza delle informazioni, l'ISO 13335 (Guideline for the Management of IT Security, GMITS) può essere visto come il suo fratello maggiore, con l'aggiunta di aspetti tecnologici e un'estensione della gestione del rischio. C'è forte complementarità anche tra l'ISO/IEC 17799 e l'ISO 15408, ossia i Common Criteria. Mentre il primo si focalizza più sugli aspetti organizzativi e amministrativi, il secondo copre gli aspetti tecnici della sicurezza. Ulteriori relazioni si possono individuare tra questi standard e gli standard ISO 18044 (Incident Management), ISO 17944 (Financial Systems), ISO 18028 (Communications Management) e ISO 14516 (E-commerce Security). Il BS 7799-2 del 2002 è anche armonizzato con l'ISO 9001:2000 (Vision 2000) e l'ISO 14001:1996.

Il processo di standardizzazione di Internet

Quello che segue è un elenco di alcune delle organizzazioni più importanti che operano nell'interesse dell'intera comunità di Internet e dei suoi standard.

Internet Society – *ISOC* (www.isoc.org)
Un'organizzazione privata senza fini di lucro che riunisce professionisti nel mondo del networking e che ha la missione di garantire il continuo funzionamento di Internet e il suo potenziamento. Opera attraverso una serie di comitati tecnici che definiscono gli standard e i protocolli utilizzati da qualsiasi apparecchiatura che si collega a Internet (IETF, IESG, IAB, IRTF). L'ISOC fornisce la leadership nella gestione di Internet per quanto riguarda gli standard, l'istruzione e lo sviluppo della politica amministrativa.

IETF (*Internet Engineering Task Force,* www.ietf.org)
È la comunità internazionale dei progettisti, operatori, produttori, e ricercatori nel campo del networking, interessati all'evoluzione dell'architettura di Internet e della sua continuità e affidabilità di funzionamento. Sviluppa standard tecnici su base consensuale, per esempio in relazione ai protocolli di comunicazione.

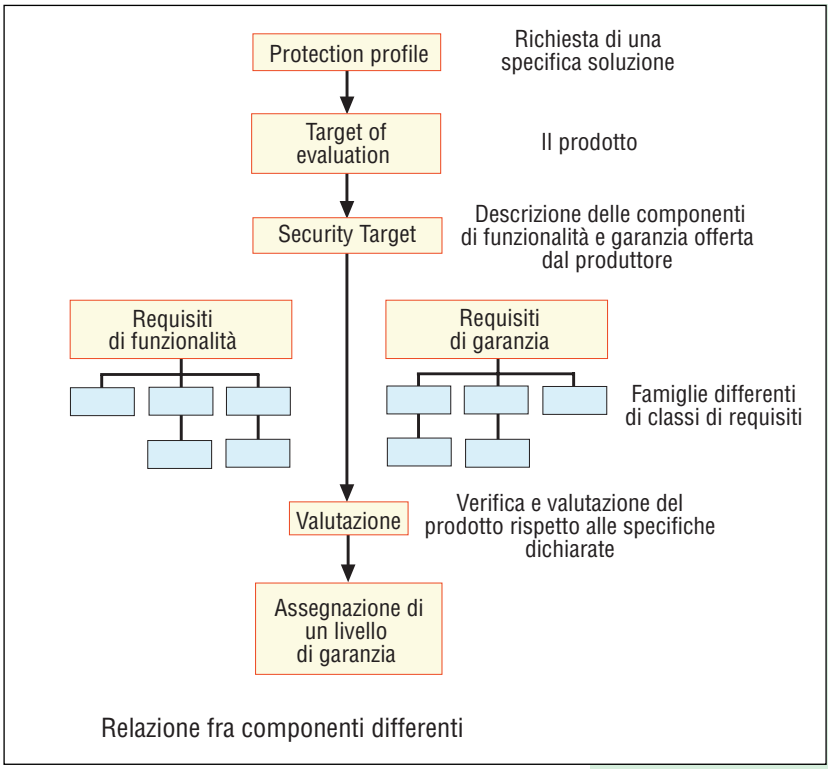
IESG
(*Internet Engineering task Group,* www.ietf.org/iesg.html)
Lo IESG è responsabile della gestione tecnica delle attività dell'IETF e del processo di standardizzazione di Internet. Come parte dell'ISOC, amministra tale processo secondo le regole e le procedure che sono state ratificate dai fiduciari dell'ISOC. Lo IESG è direttamente responsabile delle azioni associate all'avvio e alla prosecuzione dell'iter di standardizzazione, inclusa l'approvazione finale delle specifiche come Standard Internet. Lo IESG coordina e approva gli standard tecnici.

IAB (*Internet Architecture Board,* www.iab.org)
Lo IAB è un gruppo tecnico consultivo della Internet Society, responsabile della selezione dello IESG, della supervisione dell'architettura, della supervisione del processo di standardizzazione e della procedura di appello, della serie delle RFC (Request For Comment), dei collegamenti esterni e di consiglio all'ISOC.

IRTF (*Internet Research Task Force,* www.irtf.org)
La missione dell'IRTF consiste nel promuovere attività di ricerca che possano contribuire in modo significativo al futuro sviluppo di Internet. Opera creando gruppi di ricerca focalizzati sui seguenti temi: protocolli, applicazioni, architettura e tecnologia.

ICANN (*Internet Corporation for Assigned Names and Numbers,* www.icann.org)
È l'azienda non-profit che fu creata per assumere la responsabilità dell'attribuzione degli spazi d'indirizzamento IP, dell'assegnazione dei parametri dei protocolli, della gestione del sistema dei domini e della gestione del sistema dei server root, funzioni che in precedenza erano eseguite, sotto contratto con il governo USA, dalla IANA e da altre entità. È l'autorità per l'assegnazione dei nomi di dominio a livello globale.

IANA
(*Internet Assigned Numbers Authority,* www.iana.org)
La IANA mantiene le funzioni di coordinamento centrale dell'Internet globale nel pubblico interesse. La IANA custodisce i numerosi parametri e valori di protocollo unici necessari per il funzionamento di Internet e per il suo sviluppo futuro.
Il processo di definizione degli Standard Internet è un'attività della Internet Society, che è organizzata e gestita per conto della comunità Internet dallo IAB e dallo IESG. Comprende una serie di passi e di attività che producono come risultato gli standard dei protocolli e delle procedure.
"Uno Standard Internet è una specifica stabile e ben compresa, è scritto con competenza tecnica, conta diverse implementazioni indipendenti e interoperabili con sostanziale esperienza operativa, gode di un supporto pubblico significativo e la sua utilità è riconosciuta in tutta Internet o in parti di essa" - RFC 2026, 1996.
Per essere adottata come standard, una specifica è sottoposta a un periodo di sviluppo e a numerose iterazioni di revisione da parte della comunità di Internet e a un esame basato sull'esperienza.
Per prima cosa, una specifica diventa un documento RFC. Non tutte le RFC diventano Standard Internet. Poi, se la RFC diventa uno standard, viene adottata dall'ente appropriato ed è resa disponibile al pubblico quale standard. Il processo di standardizzazione attraversa i seguenti stadi di sviluppo, collaudo e accettazione.



Relazione fra componenti differenti

Proposta di standard
(almeno sei mesi)
- generalmente stabile
- scelte di progettazione risolte
- sembra godere di sufficiente interesse della comunità per essere considerato valido

Bozza di standard
(almeno quattro mesi dall'approvazione della riunione IETF
- ben capito
- ottenuta una sufficiente esperienza operativa

Standard
(fino a una successiva revisione o sostituzione)
- ottenuta un'implementazione significativa e un'esperienza operativa positiva
- alto grado di maturità tecnica
- fornisce benefici di rilievo alla comunità Internet

***Le fasi del ciclo** di certificazione*

5.1.4 Standard ed enti di standardizzazione

5.1.4.4 conoscere il processo di standardizzazione di Internet.