LA SICUREZZA DELLE RETI

dall'analisi del rischio alle strategie di protezione

ar Analisi Rischi
Sicurezza tlc

Istituto Superiore delle Comunicazioni
e delle Tecnologie dell'Informazione
Ministero delle Comunicazioni

LA SICUREZZA DELLE RETI
dall'analisi del rischio alle strategie di protezione

Il presente documento è stato realizzato da:

Fabio Battelli	(Innovia Tech S.p.A.)
Danilo Bruschi	(Università degli Studi di Milano)
Roberta Bruzzone	(Innovia Tech S.p.A.)
Giuseppe Carducci Artenisio	(Securteam S.r.l.-Elsag [Gruppo Finmeccanica])
Sebastiano D'Amore	(PriceWaterhouseCoopers Advisory S.r.l.)
Luisa Franchina	(Istituto Superiore delle Comunicazioni e delle Tecnologie dell'Informazione)
Salvatore Leotta	(Electronic Data Systems Italia S.p.A.)
Paolino Madotto	(Proge-Software S.r.l.)
Antonio Menghini	(Electronic Data Systems Italia S.p.A.)
Simona Napoli	(KPMG S.p.A.)
Gian Luca Petrillo	(Consigliere del Ministro delle Comunicazioni)
Daniele Perucchini	(Fondazione "Ugo Bordoni")
Massimo Piccirilli	(Ministero delle Comunicazioni)
Francesco Pirro	(CNIPA)
Gianfranco Pontevolpe	(CNIPA)
Andrea Rigoni	(Symantec S.r.l.)
Marco Strano	(Polizia di Stato)
Andrea Valboni	(Microsoft S.r.l.)

Copertina e Progetto Grafico
Roberto Piraino (Graphics Lab - Istituto Superiore delle Comunicazioni e delle Tecnologie dell'Informazione)

Le opinioni e le considerazioni espresse in questo volume, nonchè le proposte avanzate, sono da considerarsi come personali dei singoli partecipanti e non riflettono necessariamente la posizione dei rispettivi Enti e Società d'appartenenza.
Il contenuto del presente volume è da considerarsi unicamente come studio tecnico/scientifico orientativo delle problematiche inerenti la sicurezza delle reti e la tutela delle comunicazioni.
Pertanto nessuna responsabilità potrà essere attribuita agli autori o all'Istituto Superiore delle Comunicazioni e delle Tecnologie dell'Informazione, che cura questa pubblicazione, per ogni eventuale conseguenza derivante da qualsivoglia utilizzo dei contenuti del presente testo.

Le citazioni di specifici marchi o nomi di prodotti presenti nel documento sono riportati a mero scopo esemplificativo, non esauriscono il novero di prodotti esistenti sul mercato e in nessun caso costituiscono elemento di valutazione o di raccomandazione per l'utilizzo dei prodotti stessi.

SICUREZZA DELLE RETI

dall'analisi del rischio alle strategie di protezione

Indice

Indice delle figure e delle tabelle

INDICE DELLE FIGURE

INDICE DELLE TABELLE

Introduzione

Questa pubblicazione nasce da una iniziativa dell'Istituto Superiore delle Comunicazioni e delle Tecnologie dell'Informazione e dell'Osservatorio per la Sicurezza e la Tutela delle Reti e delle Comunicazioni, con la collaborazione di autori appartenenti a vari organismi pubblici e privati.

L'Istituto Superiore delle Comunicazioni e delle Tecnologie dell'Informazione, costituito nel 1907, opera nell'ambito del Ministero delle Comunicazioni in qualità di organo tecnico-scientifico. La sua attività, rivolta specificatamente verso le aziende operanti nel settore ICT, le Amministrazioni pubbliche e l'utenza, riguarda fondamentalmente la normazione, la sperimentazione e la ricerca di base e applicata, la formazione e l'istruzione specializzata nel campo delle telecomunicazioni.

La normazione tecnica nazionale ed internazionale in cui l'Istituto è attore attivo e propositivo, riveste un ruolo importante per garantire migliore trasparenza ed accessibilità ai servizi a favore degli utenti, dei manifatturieri e dei gestori delle reti di telecomunicazione.

In questo campo, l'azione dell'Istituto è duplice: tramite il CONCIT (Comitato di coordinamento riconosciuto a livello europeo formato da CEI - Comitato Elettrotecnico Italiano, UNI - Ente Nazionale Italiano di Unificazione e dallo stesso Istituto) effettua la trasposizione nell'ordinamento nazionale delle norme europee e, simultaneamente, rappresenta l'Amministrazione nelle funzioni di indi-

rizzo e supporto nei gruppi nazionali presenti nelle varie commissioni e gruppi tecnici di studio dell'ITU (International Communication Union), della CEPT (Conférénce Européenne des Postes et des Télécommunications) e dell'ETSI (European Telecommunications Standard Institute).

L'Istituto gestisce la Scuola Superiore di Specializzazione in Telecomunicazioni (attiva dal 1923), cui è affidata la specializzazione post-laurea nel settore delle comunicazioni elettroniche e delle tecnologie dell'informazione, con rilascio del relativo diploma. D'intesa con la facoltà di Ingegneria dell'Università La Sapienza di Roma, la Scuola organizza corsi annuali il cui piano di studi prevede anche attività di laboratorio, seminari e stage.

L'Istituto provvede anche alla formazione ed all'aggiornamento tecnico del personale appartenente al Ministero e ad altre pubbliche amministrazioni nei settori delle comunicazioni elettroniche e delle tecnologie delle informazioni, della sicurezza, della multimedialità e della qualità dei servizi, attraverso la pianificazione e realizzazione di percorsi formativi mirati all'acquisizione di competenze specialistiche. In tale ottica, l'Istituto si è dotato di un Test Center accreditato dall'AICA per il rilascio della Patente europea del Computer (European Computer Driving Licence - ECDL).

Inoltre attualmente è in fase di costituzione il Centro di formazione dei dipendenti della PA nel campo della sicurezza ICT .

Il Centro di formazione dovrà svolgere attività di formazione e di sensibilizzazione su larga scala dei dipendenti della PA in materia di sicurezza ICT, predisponendo, in forma centralizzata e coordinata, un Piano di formazione e sensibilizzazione che diffonda in modo uniforme in tutta la Pubblica Amministrazione i principi e le metodologie della sicurezza.

L'Istituto, inoltre, promuove attività divulgativa tramite eventi di comunicazione esterna e pubblicizza le attività e le ricerche effettuate.

L'attività dell'Istituto nella ricerca è orientata allo sviluppo e al

miglioramento dei servizi di telecomunicazione e di quelli legati alla tecnologia dell'informazione. Perseguendo queste finalità, le attività investono quasi tutte le aree del settore, dalla telefonia alla televisione, dall'elaborazione al trattamento del segnale, dall'architettura delle reti alla implementazione dei servizi.

Viste le competenze e le risorse strumentali di cui dispone, il ruolo dell'Istituto è rilevante nella partecipazione a progetti europei di sviluppo tecnologico per una più diffusa utilizzazione dei fondi europei. Tali attività sono svolte sia direttamente, sia d'intesa con altri Enti di Ricerca, con Università e con Centri di studi internazionali.

Nel contesto della Società dell'Informazione, sono di rilievo le azioni in svolgimento anche in collaborazione con la Fondazione Ugo Bordoni (FUB) nei settori del telelavoro, della sicurezza informatica, del teleinsegnamento e dell'accesso ai servizi di comunicazione da parte di persone disabili ed anziani.

Grazie al supporto dell'Istituto, poi, il Ministero ha potuto sostenere, negli ultimi anni, una serie di iniziative per l'introduzione, sulle reti di comunicazione, di nuove tecnologie e nuovi sistemi. Tra queste, vanno sottolineati gli studi di fattibilità sull'applicazione di tecniche e di nuovi servizi televisivi e multimediali, lo studio di fattibilità per la fornitura di servizi macroregionali di televisione numerica via satellite, lo studio per la realizzazione di un sistema satellitare europeo per la fornitura di servizi a larga banda multimediali e interattivi, la partecipazione al progetto di ricerca e sviluppo tecnologico IST (Information Society Technologies) della Comunità Europea denominato ATLAS.

Considerando il suo ruolo di organismo pubblico e super partes, il valore aggiunto dell'Istituto, dato in termini di garanzia e competenza, è l'aspetto che contraddistingue i servizi di supporto tecnico e consulenziale forniti alle imprese e ai soggetti coinvolti nel settore delle telecomunicazioni. Tali servizi si sostanziano non solo nelle tradizionali attività di certificazione, realizzate grazie alle competenze e alle strumentazioni dei laboratori dell'Istituto che consentono di verificare la conformità di ogni apparato telematico alle varie norme e raccoman-

dazioni di riferimento, ma anche in peculiari campagne di misura per la verifica della qualità del servizio (QoS), della sicurezza delle reti e per l'accertamento delle specifiche tecniche di interoperabilità dei servizi nell'ambito dell'interconnessione delle reti di vari operatori.

L'Istituto gestisce la banca dati relativa alle assegnazioni numeriche nella rete di telecomunicazione nazionale e alla portabilità dei numeri in tecnologia GSM e UMTS, gestisce inoltre il servizio di Orologio Nazionale di Riferimento (ONR) per la sincronizzazione della Rete Numerica di Telecomunicazione italiana e fornisce un supporto istituzionale ai proponenti che si sottopongono ai bandi di gara del programma comunitario E-TEN (Trans European Network per le TLC). L'Istituto collabora con Organismi di Certificazione per le attività di verifica e controllo sui Sistemi di Qualità Aziendale in osservanza delle norme UNI EN ISO 9000, è impegnato nell'attività di controllo dei Laboratori Accreditati a fronte della norma UNI CEI EN ISO/IEC 17025 ed è Organismo Notificato per le attività di cui al Decreto Legislativo 9 maggio 2001 n. 269. L'Istituto ricopre il ruolo di Organismo di Certificazione della sicurezza dei sistemi e prodotti informatici commerciali (OCSI), ed è Centro di Valutazione (Ce.Va) di sistemi e prodotti ICT che trattano dati classificati. Inoltre è Organismo Notificato ai sensi della Direttiva riguardante le apparecchiature radio e le apparecchiature terminali di telecomunicazione ed è Competent Body ed Organismo Notificato in materia di compatibilità elettromagnetica. Nel 2002 è diventato l'Ente di Certificazione internazionale per conto del TETRA MoU.

La presente pubblicazione è stata realizzata grazie anche al contributo di alcuni esperti dell'Osservatorio per la Sicurezza delle reti e la tutela delle comunicazioni.

L'Osservatorio per la Sicurezza delle reti e la tutela delle comunicazioni è presieduto dal Segretario generale del Ministero delle Comunicazioni ed è composto da rappresentanti dei Ministeri delle Comunicazioni, della Giustizia, dell'Interno, della Difesa, delle Attività Produttive e della Presidenza del Consiglio dei Ministri - dipartimento per la Funzione Pubblica e dipartimento per l'Innovazione e le Tecnologie, nominati con apposito decreto interministeriale dei

La presente pubblicazione si inquadra in una serie di attività svolte dal Ministero delle Comunicazioni nel corso del 2004 e relative alla realizzazione di linee guida su:

- La sicurezza delle reti - dall'analisi del rischio alle strategie di protezione
- La sicurezza delle reti nelle infrastrutture critiche
- La qualità del servizio nelle reti ICT.

Scopo del documento, come indicato con maggior dettaglio nel successivo paragrafo di guida alla lettura, è quello di fornire un quadro d'insieme aggiornato delle problematiche di sicurezza e delle relative soluzioni concernenti l'utilizzo di Internet e delle reti geografiche e locali ad essa connesse.

Questo volume è rivolto agli utenti business: liberi professionisti e studi professionali, piccole e medie imprese, grandi imprese. Nel caso degli studi professionali e delle PMI, spesso non esiste, al loro interno, una figura professionale dedicata alla sicurezza: al massimo esiste un responsabile ICT. A lui sono dedicati molti capitoli del volume. Nel caso delle grandi imprese il destinatario del volume è il responsabile della sicurezza. In tutti i casi noi auspichiamo che alcuni paragrafi siano letti anche dal top management per ricevere una sensibilizzazione al problema e una percezione netta che le soluzioni esistono e sono sostenibili.

Più oltre, nella Guida alla Lettura, è riportata una mappa che indirizza il lettore ai paragrafi che lo possono interessare.

La gestione della sicurezza parte dalla conoscenza della realtà interna, delle criticità e delle vulnerabilità. Attraverso questa conoscenza profonda delle proprie strutture e caratteristiche si può ottimizzare l'investimento in sicurezza, centrando l'obiettivo ed ottenendo il massimo risultato in termini di efficienza ed efficacia.

Si coglie volentieri l'occasione per ringraziare quanti hanno, con entusiasmo e professionalità, collaborato alla redazione del presente documento: Fabio Battelli (Innovia Tech S.p.A.), Danilo Bruschi

(Università degli Studi di Milano), Roberta Bruzzone (Innovia Tech S.p.A.), Giuseppe Carducci Artenisio (Securteam S.r.l.-Elsag [Gruppo Finmeccanica]), Sebastiano D'Amore (PriceWaterhouseCoopers Advisory S.r.l.), Salvatore Leotta (Electronic Data Systems Italia S.p.A.), Paolino Madotto (Proge-Software S.r.l.), Antonio Menghini (Electronic Data Systems Italia S.p.A.), Simona Napoli (KPMG S.p.A.), Gian Luca Petrillo (Consigliere del Ministro delle Comunicazioni), Daniele Perucchini (Fondazione "Ugo Bordoni"), Massimo Piccirilli (Ministero delle Comunicazioni), Francesco Pirro (CNIPA), Gianfranco Pontevolpe (CNIPA), Andrea Rigoni (Symantec S.r.l.), Marco Strano (Polizia di Stato), Andrea Valboni (Microsoft S.r.l.).

Si ringraziano ancora, per il loro apporto e i loro suggerimenti: Michele Boccadoro (Consorzio Thyraeus), Maurizio Bonanni (Ministero delle Comunicazioni), Stefania Caporalini Ajello (Consorzio Thyraeus), Andrew Christian Dell (Consorzio Thyraeus), Renzo Dell'Agnello (Elea S.p.A.), Andrea Mariotti (KPMG S.p.A.), Dario Nasca (Symantec S.r.l.), Claudio Petricca (Istituto Superiore delle Comunicazioni e delle Tecnologie dell'Informazione), Giampaolo Scafuro (Sicurezza e Sistemi S.r.l.), Mario Terranova (CNIPA).

Roma, marzo 2005

Il Direttore
dell'Istituto Superiore delle Comunicazioni
e delle Tecnologie dell'Informazione

Ing. Luisa Franchina

Guida alla lettura

Il documento si ripropone di fornire al lettore un quadro per quanto possibile completo relativo al processo della messa in sicurezza di una rete. Le moderne architetture ICT sono caratterizzate dalla qualità di costituire esse stesse una rete a propria volta connessa con reti di dimensione maggiore e con Internet stessa. Questa caratteristica infrastrutturale, che ha rivoluzionato la società dell'informazione nell'ultimo decennio, comporta vulnerabilità elevate a fronte delle quali è necessario predisporre un adeguato sistema di protezione.

Caratteristica di questo grande sistema interconnesso è la partecipazione al sistema di soggetti eterogenei: multinazionali, aziende di dimensioni medio-piccole, organizzazioni, enti governativi e cittadini privati. Ciascuna di queste entità, fruitrici dei servizi della Rete, ricopre un ruolo importante per garantire la sicurezza delle infrastrutture, delle informazioni e dei relativi trattamenti.

Il primo capitolo - "La struttura sociale delle reti" - descrive la società attuale e la sua connotazione di dipendenza dalle informazioni. Viene ripercorsa la nascita e lo sviluppo di Internet, il particolare sistema di gestione che la caratterizza, le esigenze più generali di sicurezza e privacy che il cittadino della Società dell'informazione avverte.

Il secondo capitolo - "Le infrastrutture di rete e le problematiche di sicurezza" - descrive in un'ottica più tecnica le caratteristiche delle reti, i criteri di sicurezza correlati e si conclude con un esempio esplicativo di rete sicura identificato nella Rete Unitaria per la Pubblica Amministrazione.

Una tecnologia così socialmente utile ma anche intrinsecamente critica come quella ICT ha necessariamente attratto, nel corso dell'ultimo decennio, l'interesse del legislatore. Giustificati dall'alto numero di settori della vita sociale, economica, culturale ed amministrativa, permeati dai trattamenti informatizzati, e sotto l'impulso della normativa UE, numerosi provvedimenti hanno iniziato a regolare e, in molti casi, a prescrivere l'utilizzo di meccanismi di protezione basati sulla tecnologia e sugli aspetti organizzativi. Un quadro dei provvedimenti dei documenti "ufficiali" emessi nel nostro Paese e a livello UE concernenti la sicurezza dell'informazione è tratteggiato nel capitolo terzo - "La normativa legale pertinente".

Il capitolo successivo, il quarto, intitolato "L'Analisi dei Rischi", è dedicato ad un aspetto recentemente emerso all'attenzione degli esperti e giunto anche all'attenzione del legislatore, europeo e italiano. La proliferazione e la rapida evoluzione nel tempo delle minacce ha condotto alla ribalta la necessità di individuare, con un approccio metodico, la criticità effettiva dei beni da proteggere, al fine di indirizzare opportunamente le risorse concentrandole nelle aree maggiormente critiche sia sotto il profilo economico sia etico. L'analisi dei rischi è anche alla base del moderno modo di fare sicurezza, basato sulla proattività e sulla periodica revisione dei livelli di rischio e della criticità dei beni. E' tramite il processo di analisi e gestione dei rischi che le contromisure vengono individuate e monitorate nel tempo.

Il quinto capitolo - "Tecnologie e strumenti per la protezione delle reti" - illustra gli ingredienti necessari per progettare il sistema di protezione, a valle della precedente fase di analisi e gestione dei rischi. Esso è diviso in due parti: la prima tratta delle tecnologie e dei componenti hardware e software, la seconda tratta dei servizi, che possono essere interni all'azienda o terziarizzati.

Il sesto capitolo, infine, denominato "Il governo della sicurezza nella PA e nel mondo privato" riconduce tutti gli argomenti trattati nell'alveo di una visione etico-politica della protezione delle reti, considerata come una delle componenti base del concetto più generale di Corporate Governance, argomento, com'è noto, in grande evidenza agli occhi di tutti e del legislatore, in particolare, nel corso degli ultimi anni.

Il documento, in cui a una fotografia dello scenario in essere si aggiungono, ipotesi e suggerimenti migliorativi per il futuro, vuole essere un'utile risorsa per chi vuole confrontare e verificare le proprie conoscenze in materia, nonché una fonte di stimolo e promozione per la sensibilizzazione alla sicurezza delle reti dei vari soggetti attivamente interessati e per individuare ipotesi di miglioramento e progresso sotto l'aspetto tecnologico e organizzativo.

Segue una tabella che ha lo scopo di indirizzare le diverse tipologie di lettori ai capitoli che potenzialmente presentano un maggior interesse per la loro attività.

	Vertici Azienda	Resp. ICT	Resp. Sicurezza	PMI e Studi Prof.	PA	Legislatore	Ufficio Legale
1							
1.1	❍	❍	❍	❍	❍	❍	❍
1.2	❍	❍	❍	❍	❍	❍	❍
1.3	❍	❍	❍	❍	❍	❍	❍
1.4	❍	❍	❍	❍	❍	❍	❍
1.5	❍	❍	❍	❍	❍	❍	❍
1.6	❍	❍	❍	❍	❍	❍	❍
2							
2.1	❍	❍	❍	❍	❍		❍
2.2		❍	❍		❍		❍
2.3.1		❍	❍	❍	❍	❍	❍
2.4.1	❍	❍	❍	❍	❍		
2.4.2	❍	❍	❍	❍	❍		
2.4.3	❍	❍	❍	❍	❍		
3							
3.1.1	❍	❍	❍	❍	❍	❍	❍
3.1.2			❍			❍	❍
3.1.3	❍		❍	❍	❍	❍	❍
3.1.4			❍			❍	❍
3.1.5			❍		❍	❍	❍
3.2.1	❍	❍	❍	❍	❍	❍	
3.2.2	❍		❍	❍			❍
3.2.3	❍		❍	❍			❍
3.3.1	❍	❍	❍	❍	❍	❍	
3.3.2		❍	❍			❍	
3.4	❍	❍	❍	❍	❍		
3.5			❍			❍	
3.6.1	❍	❍	❍	❍	❍		
3.6.2	❍	❍	❍	❍	❍		
3.6.3	❍		❍	❍		❍	
4							
4.1			❍				
4.2.1	❍	❍	❍	❍	❍	❍	❍
4.2.2		❍	❍				
4.2.3		❍	❍				
4.2.4		❍	❍				
4.2.5		❍	❍				
5							
5.1.1		❍	❍				
5.1.2		❍	❍				
5.1.3		❍	❍				
5.1.4		❍	❍				
5.1.5		❍	❍				
5.1.6		❍	❍				
5.1.7		❍	❍				
5.1.8		❍	❍				
5.1.9		❍	❍				
5.1.10		❍	❍				
5.1.11		❍	❍				
5.2.1	❍	❍	❍	❍	❍	❍	❍
5.2.2		❍	❍				
5.2.3		❍	❍				
6	❍	❍	❍	❍	❍	❍	❍

1 - Reti e Società

1.1 IL CONCETTO DI RETE

Il termine **rete**, stante l'esponenziale sviluppo nel corso dell'ultimo decennio dell'interconnessione tra gli elaboratori, ha assunto un significato assai ampio, sostituendosi, in alcuni contesti, all'acronimo ICT (Information and Communication Tecnology).

In questa accezione (che viene adottata estensivamente nell'intero documento e, in particolare, nel presente capitolo) le **reti** sono le strutture di interconnessione (nelle diverse tecnologie **wired** e **wireless**), ma anche le diverse **macchine**, insieme di hardware e software, che sono l'oggetto dell'interconnessione e tutti gli apparati a supporto della interconnessione stessa. Per estensione, e per dare credito al titolo di questo capitolo, anche gli utenti vengono a buon diritto a far parte della rete.

D'altra parte, accanto a questa accezione olistica del termine, utilizzato, in questo caso, al singolare, permane un'accezione di tipo operativo pratico che sta ad indicare una porzione più limitata del sistema, caratterizzato normalmente dal fatto di essere di proprietà e sotto la gestione di un soggetto ben specifico e individuabile. Nell'istanza di maggior dettaglio, si arriva alle reti locali e alle piccole reti **personali** che, in qualche raro caso, non sono interconnesse alla **grande rete** ma costituiscono sistemi **chiusi**.

Le reti, grandi o piccole che siano, sono quindi costituite da componenti trasmissive di tipo statico (doppino di rame, fibra ottica, onde radio, ecc.) e da un elevato numero di componenti, che possiamo definire **attivi**, hardware e software.

La molteplicità e complessità dei componenti, cui deve aggiungersi l'insieme **umano** degli utenti e degli addetti ai lavori, costituiscono il motivo principale della elevata vulnerabilità intrinseca dei sistemi e sono, d'altra parte, in virtù della loro **missione** di trattare le informazioni, gli elementi cui si riferiscono tutte le misure di sicurezza, di carattere organizzativo, fisico e logico, di cui si parlerà nel corso del documento.

1.2 L'ICT COME STRUMENTO PER LO SVILUPPO SOCIALE ED ECONOMICO

"La conoscenza è la nuova base della ricchezza. Questo non si è mai verificato prima. In passato, quando i capitalisti parlavano della loro ricchezza, si riferivano alle loro proprietà in termini di impianti, attrezzature e risorse naturali. In futuro, quando i capitalisti parleranno della loro ricchezza, intenderanno la loro capacità di controllare la conoscenza." [1]

Con queste parole l'economista Lester Thurow[2] mette in luce con efficacia l'importanza del ruolo assunto dall'informatica (o, come è meglio dire, dall'ICT intesa come la tecnologia dell'informazione e della comunicazione) nell'economia e nella nostra vita di tutti i giorni.

Solo dieci anni fa non era pensabile effettuare da casa un bonifico bancario, un investimento finanziario, un acquisto o una vendita. In questi dieci anni l'accelerazione della tecnologia ha determinato un cambiamento epocale del modo di lavorare e di trascorrere il tempo libero.

È possibile affrontare le sfide proposte dalla globalizzazione in

---

[1] *Thurow Lester C. ,"La costruzione della ricchezza", 2000, Ed. Il Sole 24 Ore.*

[2] *Insegna Management ed Economia al Massachusetts Institute of Technology (MIT).*

una economia sempre più legata al trasferimento di dati ed informazioni perché le reti sono divenute il vero sistema nervoso intorno al quale operano le economie occidentali (e non solo occidentali) evolute.

Molte imprese si sono **mondializzate**. Sempre più numerosi sono i prodotti che, pensati ed ideati in un luogo, sono realizzati a migliaia di chilometri di distanza. Il filo che collega il luogo della ideazione a quello della produzione è spesso una fibra ottica, un filo di rame, un ponte satellitare.

Alla fine del '700 i luoghi di produzione erano costruiti lungo i corsi d'acqua nei quali potevano navigare le imbarcazioni con le merci e dove era possibile approvvigionarsi di acqua e scaricare, in modo peraltro poco ecologico, i residui della lavorazione; alla fine del '800 i luoghi della produzione erano principalmente vicino a dove era possibile accedere alla corrente elettrica o ai binari. Oggi moderni ed importanti centri servizi sorgono nei **luoghi cablati**, nei quali è possibile facilmente avere a disposizione enormi quantità di banda passante con la quale trasferire dati.

Un altro modello che sta emergendo si basa sull'esternalizzazione sempre crescente di servizi **non core** dell'azienda. Ormai è sempre più frequente dare in **outsourcing** la gestione delle paghe, la contabilità, la logistica. Sempre più funzioni vengono affidate a società che si occupano di fornire un servizio completo. Ciò che ci consente di mantenere il legame con queste attività esterne è ancora una volta la rete.

E ancora, le aziende sempre più frequentemente utilizzano applicazioni informatiche ubicate presso società erogatrici di servizi che le sollevano dalla gestione quotidiana dei sistemi informativi. Per non parlare poi dei servizi di **e-government** che già da oggi ci consentono di presentare la nostra dichiarazione dei redditi, prendere visione della nostra posizione contributiva, richiedere certificati presso i comuni e le Pubbliche Amministrazioni, effettuare visure e molto altro ancora. Anche in questi casi la rete costituisce il fattore abilitante.

L'Europa ha ben chiaro lo scenario ed è opinione della Commissione UE che *"favorendo la crescita economica, le tecnologie dell'infor-*

mazione e della comunicazione possono creare posti di lavoro nuovi e migliorati e aumentare la prosperità. I governi europei vogliono che questi vantaggi siano a disposizione di tutti e non solo di una piccola minoranza. La nuova società basata sulla conoscenza deve essere una società aperta a tutti. Internet offre possibilità enormi: qualsiasi persona capace di usare un computer può partecipare alla vita sociale cliccando un mouse. e-Europe e i suoi programmi (e-Learning, e-Health, e-Government ed e-Business) mirano a sfruttare interamente questo potenziale a vantaggio dell'inclusione sociale." [3]

La **conoscenza**, intesa come carattere peculiare dell'economia della nostra età, annovera quattro caratteristiche distintive. La prima è l'**estensione** del fenomeno: le conoscenze acquisite negli ultimi vent'anni sono quantitativamente superiori a tutto il patrimonio di conoscenze accumulato negli anni precedenti. La gran parte dei prodotti che stiamo utilizzando solo vent'anni fa non esisteva.

La seconda caratteristica è la **maggiore integrazione delle conoscenze** utilizzate nella realizzazione dei prodotti e che è di gran lunga superiore a quella riscontrata in precedenza. Una moderna automobile oggi è un prodotto composito di conoscenze che spaziano dal design alla psicologia, dal marketing all'elettronica e all'informatica, fino all'aerodinamica, alla meccanica, alla chimica e così via.

La terza caratteristica è rappresentata dalla **smaterializzazione** dei prodotti. Progressivamente il peso della materia prima e del lavoro diretto è diventato minore rispetto alle componenti immateriali. Il design, la tecnologia, il know-how, i brevetti, la comunicazione hanno assunto un progressivo e crescente rilievo.

Il ruolo assunto dalla conoscenza rimette in discussione il modello produttivo tradizionale basato sulla sequenza di ricerca teorica che conduce alla scoperta, di ricerca applicata che conduce all'invenzione e, in fine, di sviluppo industriale, che conduce al prototipo e all'ingegnerizzazione del processo produttivo da cui deriva, appunto, la produzione su larga scala.

---

[3] *"Verso un'Europa basata sulla conoscenza -L'Unione europea e la società dell'informazione ", Commissione Europea, 2002.*

L'ultima caratteristica, infine, è la **contrazione temporale** tra la scoperta e la realizzazione del prodotto. Grandi aziende, ad esempio farmaceutiche o informatiche, continuano ad investire in ricerca teorica con l'obiettivo di individuare scoperte scientifiche da brevettare e da vendere. Il brevetto assume un ruolo nuovo: il diritto esclusivo al suo sfruttamento pone nuovi interrogativi, sul piano etico, ai cittadini e alla Società.

In una economia della conoscenza la rete e le informazioni diventano la linfa vitale dell'economia stessa. Internet è il grande sistema interconnesso che consente la divulgazione della conoscenza su scala mondiale.

Oggi su Internet transitano i dati di tutti, comprese le informazioni sensibili dell'economia: è quindi necessario prendere cognizione dei nuovi problemi che l'opportunità della rete ci pone davanti. *"Internet sta cambiando il nostro modo di vivere. L'Europa deve entrare nell'era digitale e basare la sua economia sulla conoscenza. La maniera in cui l'Unione europea gestirà questa transizione influenzerà la qualità della vita, le condizioni di lavoro e la competitività in generale dell'industria e dei servizi europei".*[4] Così l'Europa si appresta ad affrontare la sfida.

Una sfida che l'Unione Europea vede ambiziosa: *"Gli obiettivi generali fissati dai leader dell'Unione Europea a Lisbona mirano a rendere l'Unione Europea entro il 2010 la società basata sulla conoscenza più competitiva del mondo."* [5]

Internet si configura come un mare aperto nel quale navigano le informazioni su base planetaria. Come accade anche nel mare reale è necessario prendere tutte le precauzioni necessarie. Nessuno spedirebbe il proprio carico di merci per mare se non sapesse che è possibile tracciarne la rotta attraverso i satelliti, conoscere sempre l'ubicazione delle flotte via radio e avere la necessaria protezione dai mezzi militari che solcano gli oceani.

---

[4] *ibid.*

[5] *ibid.*

Durante la seconda guerra mondiale ciò che stava mettendo in ginocchio il Regno Unito erano i continui attacchi ai convogli merci che i sommergibili tedeschi compivano sulla rotta commerciale tra USA e UK. La soluzione che fu adottata fu quella di proteggere i convogli incapsulandoli all'interno di scorte militari che rendevano sicure le vie d'accesso. È quello che un po' accade quando i dati vengono inviati da un luogo ad un altro attraverso un protocollo **sicuro** che ne protegge la loro integrità.

In questo contesto è emersa sempre più la necessità di **sicurizzare** la rete, un neologismo rispetto al termine **assicurare** che nell'uso comune ha assunto il significato di accendere una polizza assicurativa a garanzia dei possibili danni provocati da un evento inatteso. **Sicurizzare** i dati significa adottare delle misure che proteggano l'operatività e il business dell'azienda.

In questo quadro l'Unione Europea, nel documento già citato, prosegue: *"Più le reti e i computer diventano un elemento centrale del commercio e della vita quotidiana, maggiore diventa l'esigenza di garantire la protezione dei dati. Rendere sicure le reti e i sistemi di informazione è quindi il requisito preliminare per promuovere il commercio elettronico e tutelare la privacy. A tal fine l'Unione Europea ha varato una strategia basata sulle sue comunicazioni, sulla sicurezza e la cibercriminalità e sulla direttiva concernente la protezione dei dati".*

In questi mesi ha avviato la propria attività operativa ENISA (European Network Information Security Agency), l'Agenzia Europea che ha il compito specifico di governare le tematiche della sicurezza in rete, alla cui nascita il Ministero delle Comunicazioni ha notevolmente contribuito.

La conoscenza è dunque il vero volano dell'economia che stiamo vivendo, conoscenza che sempre di più viene codificata nei computer, ai quali vengono delegati molti dei trattamenti attuati manualmente solo pochi anni addietro.

1.3 LE VARIE TIPOLOGIE DI RETE COME PRESUPPOSTO DI INTERNET[6]

Prima di esaminare con un certo dettaglio la genesi di **Internet** e i diversi soggetti che ne curano il funzionamento è interessante considerare, in rapida successione, le caratteristiche di alcune tipologie di rete sviluppatesi nel tempo e oggi ampiamente in uso: la **rete telefonica**, la **rete televisiva** e la **rete cellulare**.

Costruite e cresciute nel corso di lunghi decenni, le **reti telefoniche e televisive** (o più correttamente, radio-televisive) hanno avuto ben poco in comune l'una con l'altra. Le prime, fondate sulla connettività, sono state reti **senza contenuti**, essendo il contenuto fornito dagli utenti ai due estremi della linea, senza alcun coinvolgimento da parte del fornitore del servizio di telefonia. Le seconde, fondate sulla diffusione via etere, sono sempre state le **reti dei contenuti**, senza i quali la radio e la televisione sarebbero state scatole vuote. Inoltre, fino a tempi recenti, è stata netta la separazione, a livello societario, tra la proprietà/gestione di reti telefoniche e quella di reti televisive.

Conseguentemente, reti telefoniche e reti televisive non hanno mai condiviso le risorse di trasmissione. Sia le reti televisive sia le reti telefoniche sono state, per decenni, gestite in condizioni di monopolio, protette da confini nazionali e da standard nazionali o continentali.

La terza grande rete, quella **cellulare** della telefonia mobile, è nata in questo contesto, ma ha fin dalla cosiddetta **seconda generazione** (metà degli anni Novanta) evitato la barriera delle gestioni monopolistiche, mentre non ha potuto contare su standard globali, principalmente per motivi di reciproca concorrenza tra le parti in gioco.

---

[6] *Il paragrafo contiene contributi tratti da "Le reti di telecomunicazione in Italia" della Fondazione Ugo Bordoni (2003).*

La rete telefonica mobile si caratterizza tecnicamente come un'appendice della rete fissa, alla quale apporta una nuova fondamentale valenza, quella della reperibilità continua, della mobilità e della possibilità di consentire comunicazioni personali sempre e ovunque.

Oggi lo sviluppo delle reti mobili rappresenta per l'Italia l'unico settore delle telecomunicazioni in cui i tassi di penetrazione nazionali non siano inferiori a quelli dei Paesi guida. Questi tassi, non solo sono maggiori di quelli americani, ma sono praticamente allineati (in percentuale) a quelli dei Paesi scandinavi, pionieri e leader in questo settore.

Proprio grazie alla esistenza delle reti sopra indicate (in particolare delle prime due) e alla sua natura intrinsecamente distribuita, **Internet** si è sviluppata negli ultimi trent'anni con tassi di crescita mai verificatisi in tutta la storia dell'umanità, dalle origini di Arpanet, negli USA dei primi anni Settanta, all'attuale **ragnatela** (web).

Internet e le sue applicazioni stanno diffondendo informazioni e conoscenze con un'estensione mai riscontrata prima nella storia dell'umanità. Si sta in pratica attivando un processo di **democratizzazione del flusso dei dati** irreversibile e di enorme impatto sociale.

Dal punto di vista logico, Internet si configura come una rete che attraverso milioni di nodi di scambio (router) interconnette centinaia di milioni di calcolatori, comprendendo fra questi non solo i server, ma anche i dispositivi di elaborazione in possesso degli utenti (workstation, personal computer, palmari, cellulari con avanzate capacità di elaborazione e comunicazione dati).

I collegamenti fisici necessari al trasferimento di dati tra router e calcolatori sono forniti in area locale (edificio, campus universitari, campus industriale) dalle reti appositamente concepite come reti di calcolatori LAN (Local Area Networks), mentre per la copertura di distanze metropolitane o geografiche sono mutuati (sotto forma di risorse permanentemente assegnate su base contrattuale o allocate su base singolo utilizzo) da infrastrutture appartenenti ai gestori telefonici, ai gestori di reti mobili e ai gestori TV via cavo.

La circostanza che Internet, dal punto di vista delle funzioni di trasmissione, non abbia una sua infrastruttura indipendente è determinante per l'analisi della situazione presente. Anzi, si può dire che solo grazie al sistematico ricorso a risorse di trasmissione preesistenti o comunque attivabili da gestori di connettività con una lunga storia alle spalle Internet ha potuto svilupparsi con gli incredibili ritmi sopra delineati. In termini strettamente economici, basta dire che gli investimenti per Internet, almeno per quanto riguarda le risorse di trasmissione, in ogni regione del globo, sono stati quasi esclusivamente marginali, non comportando quasi mai la posa di cavi ad hoc e la realizzazione di costose opere d'impiantistica civile.

1.4 I PRINCIPALI SOGGETTI COINVOLTI NELLA GESTIONE DELLE RETI

La nascita di Internet viene fatta risalire al 1° settembre 1969, con l'avvento di ARPANET. Questa rete collegava tra loro il Dipartimento di Stato USA e le università che vi collaboravano. Veniva utilizzata sia per condividere le ricerche ma anche per scopi di comunicazione personali.

Ben presto si rese necessario dividere i due ambiti di attività e nel 1983 si decise di separare l'ambito militare con la nascita di una specifica rete denominata MILNET, destinando ARPANET (ridenominata Internet) all'ambito scientifico e di collaborazione tra università. Tra il 1990 e il 1995 la sempre maggiore diffusione di Internet porta ad un'esplosione di connessioni tra il primo nucleo e altri, sia pubblici che privati, che progressivamente vengono a costituire la **Rete delle reti** che vediamo oggi.

Internet si è sviluppata senza autorità di sorveglianza ma attraverso l'accordo e la collaborazione delle diverse entità che vi prendevano parte. Spesso l'autorevolezza di alcune università e centri di ricerca veniva di fatto riconosciuta e le indicazioni da esse proposte erano adottate dalle altre entità collegate, sia pubbliche che private.

Tuttavia nel gennaio del 1992 venne costituita la **Internet Society** [7], tra i cui fondatori ed animatori vi sono i personaggi che contribuirono alla creazione della tecnologia di base. Alla Internet Society venne conferita la responsabilità delle strutture di coordinamento che nel frattempo si erano formate come l'**Internet Activity Board**[8] e l'**Internet Engineering Task Force**[9].

L'**Internet Society** (ISOC) è un'organizzazione internazionale non governativa per la cooperazione e il coordinamento globali per la rete Internet e le sue tecnologie ed applicazioni.

Nel 1999 viene costituita l'**Internet Corporation for Assigned Names and Numbers** (ICANN)[10]: l'organizzazione non-profit costituita per gestire l'allocazione dello spazio per gli indirizzi Internet e le funzioni di **domain name system** e di **root server system**.

Il 1998 vede la nascita del **Consiglio dei Registri Nazionali europei per i Top Level Domain** (Council of European National Top Level Domain Registries - CENTR), con il fine di favorire lo scambio di informazioni e garantire lo sviluppo di procedure (**best practices**) tra i registri europei per il coordinamento dei nomi di dominio di primo livello (quali quelli con il suffisso **".it"**).

Tra gli altri organismi a livello internazionale che si occupano di Internet e Domain Name System segnaliamo, in particolare, il **RIPE Network Coordination Centre** che agisce come Registro Internet Regionale d'Europa e che si occupa di coordinare le attività delle organizzazioni che ne fanno parte e il **Governmental Advisory Committee** [11] che riunisce rappresentati di tutti i governi con l'obiet-

---

7 www.isoc.org - In Italia www.isoc.it

8 www.iab.org

9 www.ietf.org

10 www.icann.org

11 www.gac.org

tivo di favorire il rapporto pubblico-privato nella gestione della Rete.

In questa ragnatela di competenze esiste il **W3C** (World Wide Web Consortium)[12] che ha l'obiettivo di standardizzare le tecnologie utilizzate in ambito Web che oggi sono fondamentali in Internet.

Questi organismi sono spesso costituiti per autonoma iniziativa di privati, università, istituzioni e hanno ambiti di attività diversi. In moltissimi casi, per farne parte, non è necessario un processo di affiliazione, ma è sufficiente dimostrare di avere le competenze necessarie per poter contribuire e proporre la propria disponibilità.

Per far funzionare tutto questo sono necessarie regole condivise e accettate. La principale base di convivenza civile in Rete è data da un codice di autoregolamentazione denominato **netiquette**[13]. In questo codice, che si tramanda da decenni con aggiornamento periodico, vi sono le basi della convivenza civile in Rete. Eventuali violazioni possono essere denunciate sia al proprio provider che alla Naming Authority Italiana[14]. Tali violazioni possono essere sanzionate anche con la estromissione dalla Rete.

A livello nazionale, in accordo con ciò che è avvenuto negli altri paesi, si è proceduto nei primi anni '90 alla creazione del gruppo per la Naming Authority italiana.[15] Il gruppo **Naming Authority ITA-PE** si è costituito nell' Ottobre 1994, e si è dato a suo tempo una struttura di gruppo di lavoro aperto, basando le proprie procedure operative sul modello destrutturato dei gruppi della Internet Engineering Task Force (IETF).

La partecipazione al gruppo era pertanto libera e il lavoro veni-

---

12 www.w3c.org

13 la cui traduzione italiana ufficiale è a www.nic.it/NA/netiquette.txt

14 vedi oltre

15 www.nic.it

va svolto sia durante le riunioni periodiche del gruppo stesso che tramite posta elettronica. Le decisioni venivano prese in base al principio del più ampio consenso.

Successivamente, la necessità di avere a disposizione una struttura in grado di prendere rapidamente delle decisioni operative e la difficoltà di raggiungere sempre il pieno consenso hanno portato ad un processo di revisione di alcune modalità di lavoro ed alla formale costituzione della Naming Authority Italiana.

A tal fine sono state modificate le sue procedure operative dotandola di una maggiore organizzazione. La Registration Authority, struttura esecutiva della Naming Authority, ha la responsabilità dell'assegnazione dei nomi a dominio con il suffisso **.it**.

La RA Italiana ha quindi il compito di gestire i registri operativi del Top Level Domain **.it**. Le modalità operative generali e le norme (**Regole di Naming**) in base alle quali la RA Italiana opera sono definite dalla Naming Authority Italiana. Oltre che alla gestione del **.it**, la RA è responsabile dell'assegnazione di nomi definiti da altri standard. Le attività della RA sono svolte dall'**Istituto di Informatica e Telematica** del **Consiglio Nazionale delle Ricerche** (IIT-CNR).

Il ruolo di Registration Authority deriva al CNR dalla posizione che esso ricopre nella comunità scientifica nazionale ed internazionale quale Ente pubblico di ricerca. Le attività relative sono state affidate ai tecnici dell'Istituto di Informatica e Telematica con l'accordo dello IANA (Internet Assigned Number Authority[16]), sulla base delle riconosciute competenze acquisite.

La Registration Authority Italiana riveste un ruolo di primaria importanza anche a livello mondiale per lo sviluppo del Domain Name System e delle politiche ad esso correlate. Tra gli organismi di cui la RA è membro attivo rientrano CENTR[17] ed ICANN.

---

16 www.iana.org

17 www.centr.org

In conclusione, Internet ha una storia **confusionaria** e nello stesso tempo **organizzata**, che nasce da persone che hanno condiviso competenze e responsabilità per dare vita a questo straordinario fenomeno. I media e il senso comune confondono spesso questi aspetti con la pirateria informatica, gli hacker, i virus e quant'altro. In realtà molte delle persone che hanno fatto Internet, come Vinton Cerf e Joseph Licklider (tra i fondatori di ARPANET ed Internet), Tim Berners-Lee (inventore del World Wide Web), Ray Tomlinson (inventore dell'e-mail), Marc Andressen (inventore del Browser Web e poi fondatore della Netscape), Bill Joy (inventore di Java[18] e di UNIX BSD) per citarne solo alcuni, sono, nell'accezione positiva del termine, **hacker**[19].

Questa parziale panoramica sull'insieme di soggetti che hanno creato e gestiscono la **Rete delle reti** ci pone di fronte alla considerazione che lì fuori, fuori, cioè, dal nostro computer personale o aziendale, vi è un mondo variegato costituito da aziende che forniscono connessione alla rete, utenti (benintenzionati e malintenzionati), organismi, governativi e non, di gestione e controllo ecc.

Questa galassia, dalla quale è nato un potentissimo strumento la cui regolamentazione comporta delicati problemi di equilibrio tra normazione e libertà, ci pone di fronte la sfida della sicurezza.

---

18 Una tecnologia molto diffusa per la distribuzione di applicazioni su rete.

*19 Il termine **hacker**, che successivamente, grazie ad un equivoco perpetrato dai media, ha assunto una connotazione negativa, nasce, infatti, con una accezione positiva indicando un ideale di condivisione del lavoro e delle conoscenze. L'hacker è, nell'accezione iniziale, una persona entusiasta del proprio lavoro, disposto a condividerlo per far crescere le competenze comuni ricavandone il giusto compenso.*

*L'hacker, sin dalle origini, segue una sorta di codice cavalleresco che impone una sfida di intelligenza esercitata tramite la tecnologia. Il termine hacker deriva da **hack**, far mobili con l'accetta: produrre con la propria opera ciò che serve.*

*È piuttosto il termine **cracker** quello con cui gli hacker indicano il pirata-vandalo informatico. È una persona che, avendo la conoscenza tecnica, utilizza gli strumenti degli hackers per **rompere** le sicurezze di un sistema per furto o vandalismo. La parola è nata nell' 85 dagli hackers per difendersi, appunto, dall'uso improprio da parte dei giornalisti della parola **hacker**.*

Spesso si crede che basti delegare la propria sicurezza alla compagnia telefonica o ad un noto Service Provider per essere tranquilli. In realtà è necessario prendere atto che la sicurezza è una cultura continua e una pratica costante da affidare a professionisti in grado di supportare adeguatamente le aziende e di cui, comunque, una notevole parte rimane affidata al senso di responsabilità e alla preparazione dell'utente. La sicurezza su Internet non è né più né meno della sicurezza sulla strada. É possibile girare liberamente perché la maggior parte dei cittadini è onesta e sarebbe disposta a denunciare un reato contro un proprio simile, ma nessuno può garantire che non possa verificarsi, nella realtà quotidiana, uno scippo o un reato più grave.

1.5 SICUREZZA E PRIVACY: DUE ASPETTI CHIAVE

Oggigiorno qualsiasi organizzazione pubblica e privata affida gran parte dei propri processi, di business o istituzionali, ai sistemi informativi e quindi alle informazioni trattate. Quando un evento dannoso, sia esso di origine naturale o doloso, colpisce i sistemi che gestiscono le informazioni di cui l'organizzazione ha bisogno (comprese le reti), quasi sempre questo si traduce in una brusca interruzione dei processi produttivi che può compromettere la continuità dell'organizzazione.

Oggi, più di ieri, **essere sicuri** vuol dire fronteggiare qualsiasi evento, dalle catastrofi naturali (allagamenti, incendi, terremoti) all'attacco informatico, garantendo l'integrità e la continuità dei più **intimi** e **vitali** processi dell'organizzazione.

Per capire fino in fondo quali sono i principi fondamentali su cui basare il significato della sicurezza, e quindi la strategie di protezione, è bene chiarire i seguenti concetti.

Una rete di telecomunicazione, e con essa, più in generale, le informazioni che vi transitano, per essere considerata sicura, deve soddisfare almeno i seguenti requisiti:

- **confidenzialità** delle informazioni, intesa come la garanzia

che i dati vengano acceduti, conosciuti e trattati solo da chi ne ha diritto

- **disponibilità** delle informazioni, intesa come la possibilità di accedere ai dati quando richiesto. I sistemi dovrebbero avere capacità sufficienti per soddisfare le richieste di accesso da parte degli utenti
- **integrità** delle informazioni, intesa come la garanzia che il dato sia accurato ed esente da manomissioni, perdite e danneggiamenti.

I tre requisiti sopra indicati (e specificamente il primo) rivestono un ruolo primario nell'attuazione concreta di un principio giuridico prepotentemente emerso nel corso degli ultimi anni: la tutela dei dati personali delle persone fisiche e giuridiche, al fine di garantire la loro privacy. Adeguate misure di sicurezza devono essere previste, anche per legge, al riguardo.

Più in generale, si osserva che, fondamentalmente, la vulnerabilità complessiva delle reti e dei sistemi informativi di tutto il mondo, dipende da un nuovo modo di intendere e gestire i processi all'interno delle organizzazioni.

Fino a qualche decennio fa le organizzazioni erano governate da flussi collaborativi interni ed avevano una scarsa comunicazione con l'esterno. In sostanza le reti non avevano ancora fatto ingresso nel mondo dell'ICT, ma si parlava per lo più di collegamenti dedicati con sistemi centrali (**mainframe**).

La sicurezza di allora era pertanto fondata sull'isolamento ed era intesa come un fatto prettamente statico e passivo. È importante sottolineare, inoltre, che l'utilizzo dei dati avveniva in maniera abbastanza circoscritta e l'autonomia del dipendete rispetto al sistema informativo era pressoché inesistente.

In sostanza il sistema informativo e le risorse umane che lo componevano erano il catalizzatore di tutte le richieste d'informazioni provenienti dal resto dell'azienda. Seppure anche in simili scenari fosse

all'epoca frequente incontrare procedure poco attente alla sicurezza, le minacce erano abbastanza circoscritte, in quanto la stessa infrastruttura di comunicazione non comportava le vulnerabilità di oggi.

Rispetto a questi paradigmi l'organizzazione di oggi è radicalmente cambiata. Tende a portare all'esterno sia sotto-processi che processi interi; tende a distribuire le funzioni sul territorio facendo sempre più parte di realtà multinazionali; dialoga in tempo reale con i propri fornitori, clienti e committenti e soprattutto, a livelli diversi; consente al singolo utente di dialogare direttamente con la maggior parte delle applicazioni al fine di reperire più velocemente le informazioni.

Al centro di questo importante cambiamento ci sono le reti di telecomunicazione. Grazie all'introduzione ed allo sviluppo delle reti oggi possiamo effettivamente parlare di condivisione delle informazioni.

Questa maggiore apertura implica una maggiore fruibilità dei dati che espone le organizzazioni a considerevoli rischi. Rispetto al passato, la sicurezza diventa un fatto dinamico da affrontare necessariamente in modo attivo. Gli utenti interni all'organizzazione acquistano un ruolo fondamentale rispetto al sistema informativo e alle reti. Il rapporto **utente interno - sistema informativo - rete** è di gran lunga più critico del rapporto **utente esterno - sistema informativo - rete**. Il motivo è presto detto. La maggior parte delle operazioni necessarie alla gestione dell'organizzazione avvengono mediante applicazioni interne, che con le informazioni e le reti, costituiscono il Sistema Informativo Aziendale (SIA). Viene naturale pensare che, a differenza degli utenti esterni, abilitati ad utilizzare un numero ristretto e controllato di servizi, l'utente interno è coinvolto in prima istanza nell'utilizzo esclusivo e privilegiato del SIA, rappresentando pertanto uno dei principali fattori di rischio per la sicurezza delle informazioni e delle reti.

In questo contesto si inserisce, come ulteriore elemento che contribuisce alla domanda di sicurezza, l'esigenza di garantire la privacy nel trattamento delle informazioni. Anche se l'argomento sarà trat-

tato in maniera più diffusa nel corso di questo documento, è bene chiarire, al riguardo, alcuni aspetti fondamentali.

Alla base delle leggi sulla privacy emanate dai singoli governi dell'Unione Europea ci sono alcuni principi fondamentali, ampiamente condivisi, per la tutela dei dati personali. Tra questi abbiamo:

- i dati devono essere raccolti nel rispetto delle leggi
- le informazioni raccolte su singoli individui non possono essere diffuse ad altre organizzazioni o ad altri individui senza esplicita autorizzazione della legge o senza il consenso dell'individuo interessato
- le informazioni raccolte devono essere accurate ed aggiornate
- le informazioni devono essere usate solo per gli scopi per i quali sono state raccolte e solo per il periodo strettamente necessario
- gli individui hanno il diritto di correggere e aggiornare le informazioni personali
- gli individui a cui si riferiscono le informazioni hanno il diritto di ricevere un resoconto sulle informazioni personali raccolte e/o gestite dalle organizzazioni
- la trasmissione dei dati personali a locazioni diverse da quelle originarie è proibita se le misure di sicurezza esistenti non sono almeno equivalenti.

L'esigenza di ottemperare a questi principi ha contribuito fortemente, nel corso degli ultimi anni, a creare un interesse e una sensibilità crescente per la protezione delle informazioni e delle reti.

1.6 L'IMPORTANZA DEL FATTORE UMANO NELLA SICUREZZA

In linea con l'affermazione del cyberfilosofo Philippe Queau: *"siamo di fronte a una nuova maniera di essere nel mondo, di pensare il mondo e di agire su di esso"*, diversi studi condotti in ambito internazionale hanno ormai evidenziato in maniera incontrovertibile che l'introduzione su larga scala dell'ICT ha influenzato gli schemi cognitivi degli individui, arrivando ad indurre delle vere e proprie alterazioni percettive che possono interferire, a vario titolo, sui livelli di consapevolezza dei soggetti e sul complesso percorso cognitivo che li condurrà, o meno, verso una scelta di legalità.

Detto ciò, va osservato che dietro ad ogni tecnologia di sicurezza c'è una persona che deve utilizzarla e che anche il più sofisticato ed **apparentemente blindato** sistema di sicurezza, sia fisico che logico, può essere vanificato da utilizzatori non addestrati o poco convinti della sua necessità.

Le ricerche psicologiche[20] più avanzate sul **computer crime** hanno infatti evidenziato l'esistenza di modifiche percettive indotte dalla tecnologia digitale, soprattutto quando tale tecnologia media una

---

[20] *Bruzzone R., "L'importanza del fattore umano nelle policy di sicurezza informatica." Pubblicato su ICT Security (Febbraio 2004).*
Galdieri P., Giustozzi C. Strano M, "Sicurezza e privacy in azienda", Apogeo editore, Milano, 2001.
Rogers, M. "A social learning theory and moral disengagement analysis of criminal computer behavior: An exploratory study." Unpublished dissertation, 2001.
Rogers M., "Psychological Theories of Crime and Hacking", Department of Psychology, University of Manitoba, Telematic Journal of Clinical Criminology, www.criminologia.org , 2003
Strano M., "Computer crime", Edizioni Apogeo, Milano, 2000.
Strano M., "Il computer crime nelle aziende" in BYTE, gennaio 1999.
Strano M., Bruzzone R., "Il computer crime nelle aziende: gli insiders", in: M. Strano (a cura di) "Manuale di Criminologia Clinica", See Edizioni, Firenze, 2003.
Strano M., Battelli F., Bruzzone R., Giustozzi C., Boccardi M., "Inside attack: tecniche di intervento e strategie di prevenzione", In press, 2005.

relazione tra l'autore di un crimine e la sua vittima: operare un illecito senza spostarsi dalla propria **familiare e rassicurante** postazione di lavoro e soprattutto senza guardare negli occhi la propria vittima rappresenta uno scenario meno ansiogeno per l'individuo.

La psicologia umana è quindi un fattore che deve essere considerato da chi progetta e gestisce la sicurezza informatica. Del resto nei contesti lavorativi più moderni e sviluppati la psicologia ha già da diversi anni a che fare con le procedure di sicurezza.

Specialmente negli USA e in Gran Bretagna lo **human factor** viene, ad esempio, particolarmente curato nel settore della sicurezza delle persone sul luogo di lavoro. La funzione dello psicologo in tali ambiti è quella di convincere le persone, al di là delle prescrizioni, ad attuare un comportamento sicuro, facendo leva anche sulla loro sfera motivazionale.

Gli operai di alcuni cantieri all'avanguardia vengono, ad esempio, sottoposti ad interventi psicologici (corsi di formazione, focus-group, colloqui individuali) per instillare in loro l'abitudine all'uso di strumenti di protezione individuale e collettiva per ridurre gli infortuni, e i lavoratori che svolgono mansioni pericolose vengono addestrati al rispetto di regole di sicurezza sotto la supervisione di uno psicologo.

Sul versante della sicurezza informatica e della prevenzione del crimine all'interno delle organizzazioni, le esperienze di ricerca e di intervento psicologico appaiono invece maggiormente mirate a valutare il livello di consapevolezza del crimine (per la valutazione del rischio relativo agli utenti interni) e la percezione del rischio di attacco (per la valutazione delle vulnerabilità dei sistemi di sicurezza legate al fattore umano).

Gli aspetti principali relativi al fattore umano, da considerare quando parliamo di sicurezza informatica, sono i seguenti:

- la conoscenza delle conseguenze di eventuali comportamenti illegali, in quanto le persone, quando commettono un'azione illegale, valutano i pro e i contro anche in termini di danni pro-

vocabili e, in tale prospettiva, avere delle informazioni corrette consente di avere un'esatta percezione delle conseguenze della propria azione aumentando il livello di consapevolezza e diminuendo il rischio di sottostimare l'atto

- la conoscenza e la percezione del rischio, che è alla base del comportamento **leggero/disfunzionale** di alcune persone perché ritengono che il loro gruppo di lavoro o la propria organizzazione non rappresenti un target per un attacco, mostrando quindi una ridotta percezione del rischio
- la motivazione al rispetto delle procedure di sicurezza, in quanto spesso le procedure di sicurezza sono **faticose/noiose** da applicare e risulta quindi di fondamentale importanza riuscire a motivare le persone al rispetto di tali procedure che altrimenti non verranno applicate in maniera sistematica, pregiudicando la sicurezza dell'organizzazione nel suo complesso.

2 - Le infrastrutture di rete e le problematiche di sicurezza

2.1 IL CONCETTO DI RETE: COMPONENTI FISICHE E VIRTUALI

L'idea di un collegamento di rete è genericamente legata ad un filo che unisce due punti. Su questo filo viaggiano informazioni sotto forma di bit, inviate e ricevute secondo determinate regole che ne consentono l'interpretazione.

Alla base di quest'idea troviamo il telegrafo sul quale, ai primi del XX secolo, un operatore esperto azionava un unico tasto ritmando un flusso di segnali sulla base del codice Morse.

Negli anni settanta nasce la tecnologia **a pacchetto** che consente di inserire su uno stesso cavo elettrico più flussi contemporanei di trasmissione. La più recente nascita e diffusione di Internet complica i concetti di base.

Anzitutto oggi una rete è fatta da supporti fisici molto differenti: esistono collegamenti satellitari, radio, basati su tecnologia GSM, GPRS e UMTS, su rame, fibra ottica, wireless, ecc. Ogni supporto fisico ha caratteristiche differenti per latenza, capacità trasmissiva, sicurezza, affidabilità di connessione, ecc.

È possibile gestire la moderna complessità delle reti grazie al **protocollo TCP/IP**, il protocollo utilizzato da Internet. Si tratta di un protocollo di rete che consente a due sistemi di condividere un **dizionario**, in grado di tradurre dei segnali in informazioni e garantire che

queste siano trasmesse e ricevute correttamente. Il protocollo continua a trasmettere per un determinato periodo, anche utilizzando percorsi alternativi, fin quando ottiene un messaggio di avvenuta ricezione.

Un'altra importante funzione delle reti moderne è il **routing**, effettuata da particolari dispositivi (**router**). Tali dispositivi leggono i vari pacchetti trasmessi in formato TCP/IP e li instradano lungo i diversi collegamenti.

Esiste poi il protocollo **NAT/PAT (Network Address Translation/Port Address Translation)** che consente di utilizzare un solo indirizzo IP per un'intera rete. Questa tecnologia consente di avere una rete privata, non visibile ad Internet. Un nodo di rete provvede a mantenere traccia di mittente e destinatario in modo da stabilire la comunicazione, da un punto interno alla rete privata verso un punto esterno, come se fossero direttamente connessi.

In fine il **tunnelling** permette di creare collegamenti virtuali sui convenzionali collegamenti TCP/IP. All'interno di questi collegamenti virtuali le informazioni vengono trasferite in modalità crittografata e trasparente, impedendo ad eventuali intrusi di intercettare i dati scambiati tra mittente e ricevente. La decifrazione dell'informazione è eseguita presso particolari punti di accesso alla rete che possono essere composti da firewall, router, server o perfino client, a secondo della necessità.

Considerando quanto sopra esposto si comprende come sia ormai difficile risalire ad una connessione fisica. La connessione di rete è sempre più virtuale, le nostre informazioni viaggiano su segmenti di rete che non possiamo conoscere e sono garantite solo dal grado di protezione previsto.

In questo senso è particolarmente interessante la tecnologia **MPLS (Multi Protocol Label Switching)**, la quale consente, ad un mittente, di mettere in una busta virtuale le proprie informazioni, applicando un'etichetta che consente alla busta di viaggiare all'interno della rete senza che possa essere vista dai nodi intermedi. MPLS rappresenta un'importante novità nel campo delle reti perché consente di condividere pressoché qualsiasi supporto fisico.

2.2 LA RETE E I SUOI SOGGETTI

Il paradigma che normalmente rappresenta una rete dati è rappresentato dalla pila ISO/OSI. La pila ISO/OSI è composta da sette livelli ed è rappresentata in fig. 2-1

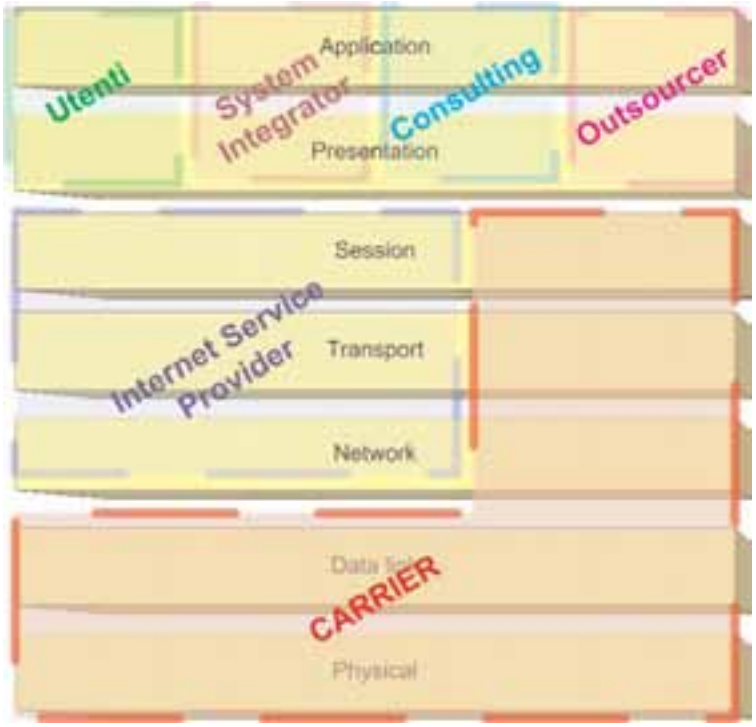


Figura 2-1 - Schema dei livelli della pila ISO/OSI

Ogni **livello** della pila è gestito da soggetti diversi che offrono servizi specifici. Proviamo a percorrere la pila per descrivere i diversi soggetti.

I **livelli 1 e 2** (a cominciare dal basso) sono dominio del **carrier** telefonico, proprietario del collegamento fisico, che installa le diverse tratte pianificando i suoi investimenti sulla base di una previsione di traffico. Il **carrier** è proprietario sia dei **back-bone** che collegano due punti di snodo con connessioni di elevata capacità, sia dell'**ultimo miglio**, che rappresenta la tratta finale e più costosa, dalla centrale telefonica fino alle utenze finali.

I rischi connessi a questo livello sono legati ad operatori che non sono in grado di offrire servizi sicuri e affidabili.

I **livelli da 3 a 5** sono gestiti dagli **Internet Service Provider** (ISP), che forniscono connessione ad Internet comprando l'accesso alle infrastrutture dei carrier e rivendendo la connessione, per così dire, al dettaglio. L'ISP fornisce anche una serie di servizi accessori che consentono all'utente di concentrarsi solo sul contenuto della comunicazione. Fra questi, di solito, troviamo la gestione del server di posta, registrazione di domini Internet, gestione dei server **web** o **ftp**, video streaming, video conferenza, e anche servizi di sicurezza quali la configurazione di reti sicure tramite tecniche di **tunnelling**.

I rischi connessi al service provider nascono dalla scarsa presenza di competenze specifiche in questo settore. È una tipologia di operatore nata da poco che spesso non offre professionalità in grado di supportare le esigenze delle organizzazioni clienti. Altro rischio connesso è un'eccessiva delega da parte delle aziende che in questo modo intendono liberarsi dalle competenze tecniche. In realtà l'asset rete dovrebbe sempre essere controllato dai clienti, al limite affidandosi a terze parti in grado di monitorare chi eroga i servizi.

I **livelli 6 e 7** si sviluppano, normalmente, presso l'utente finale. Parte di essi può essere affidata a società di consulenza, system integrator e outsourcer. Il rischio in questo campo è incentrato sul modo in cui vengono progettate le applicazioni. Spesso il system integrator si concentra sugli aspetti funzionali dell'applicazione, delegando la sicurezza agli strati operativi di più basso livello.

2.3 LA SICUREZZA DELLE RETI[1]

Minacce alla sicurezza sono tutti quegli eventi che possono avere come conseguenza la perdita dei requisiti generici, tra loro interdipendenti, di sicurezza delle informazioni (**confidenzialità**, **disponibilità** e **integrità**, già definiti al precedente paragrafo 1.5).

Devono essere prese in considerazione tutte le minacce alla sicurezza e non solo quelle caratterizzate da un intento doloso. Dal punto di vista degli utenti, rischi quali le catastrofi ambientali o gli errori umani che causano la caduta della rete sono potenzialmente altrettanto dannosi che un attacco doloso.

La sicurezza di una rete o di un sistema d'informazione va pertanto intesa come la capacità di resistere ad eventi imprevisti o atti dolosi che compromettono la disponibilità, l'integrità o la riservatezza dei dati conservati o trasmessi, nonché dei servizi forniti e accessibili tramite la suddetta rete o sistema.

Lo scopo dei paragrafi successivi è descrivere i diversi tipi di minacce.

2.3.1 Quadro generale delle minacce alla sicurezza

Intercettazione delle comunicazioni

Le comunicazioni elettroniche possono essere intercettate e i dati in esse contenuti copiati o modificati. L'intercettazione può assumere diverse forme, dall'accesso fisico alle linee della rete (ad es. intercettazioni telefoniche) alla sorveglianza delle radiotrasmissioni. I punti più vulnerabili e sensibili ad un'intercettazione del traffico sono i punti di gestione e di concentrazione della rete come, nel caso della comunicazione tramite Internet, i router, i gateway, i commutatori e i server di rete.

---

[1] *Il paragrafo contiene contributi tratti da "Comunicazione della Commissione al Parlamento Europeo, al Consiglio, al Comitato Economico e Sociale e al Comitato delle Regioni -Sicurezza delle reti e sicurezza dell'informazione: proposta di un approccio strategico europeo", disponibile all'indirizzo: www.privacy.it/com2001-298.html*

Le intercettazioni illecite o dolose vanno tenute distinte dalle attività di intercettazione consentite dalla legge. Tutti gli Stati membri dell'UE autorizzano, in casi particolari, l'intercettazione delle comunicazioni per ragioni di tutela dell'ordine pubblico o per l'attuazione di provvedimenti dell'autorità giudiziaria.

Un'intercettazione illecita può configurarsi come una violazione del diritto alla vita privata di una persona oppure essere la premessa per un uso illegale dei dati intercettati, come una password o gli estremi di una carta di credito, per fini di lucro o per sabotaggio. La percezione diffusa di questo tipo di rischio costituisce uno dei principali ostacoli ad una più marcata diffusione del commercio elettronico in Europa.

Le difese contro le intercettazioni possono essere attuate dagli operatori (protezione della rete), come previsto, tra l'altro, dalla direttiva 97/66/CE, o dagli stessi utenti (cifratura dei dati trasmessi in rete).

Per gli operatori, proteggere la rete da eventuali intercettazioni è un compito complesso e costoso.

In passato, gli operatori delle reti di telecomunicazione solevano proteggere le reti collocando dispositivi fisici di controllo dell'accesso ed impartendo apposite direttive di sicurezza al personale. Il traffico veniva cifrato solo occasionalmente.

Oggi, per le reti senza filo, è oneroso provvedere ad un'adeguata cifratura delle radiotrasmissioni. Gli operatori di reti mobili cifrano le comunicazioni tra l'apparato mobile e la stazione di base.

Gli utenti possono decidere se cifrare o no i dati o i segnali vocali a prescindere dalle misure di sicurezza previste dalla rete. Un'adeguata cifratura rende i dati incomprensibili per chiunque eccetto il destinatario autorizzato, anche in caso di intercettazione.

Sono ampiamente disponibili in commercio software ed hardware di cifratura per tutti i tipi di comunicazione. Vi sono prodotti specifici destinati a cifrare le conversazioni telefoniche o le trasmissioni via fax. Anche la posta elettronica può essere cifrata mediante software dedicati, moduli di cifratura integrati nel programma di trattamento testi oppure nel software client di posta elettronica.

Il problema è che se l'utente cifra una e-mail o una comunicazione vocale il destinatario deve essere in grado di decifrarla. È indispensabile quindi che i software o gli hardware siano interoperabili. Parimenti, il destinatario deve conoscere la chiave di cifratura, il che significa che un dispositivo deve essere in grado di ricevere ed autenticare la chiave. Il costo della cifratura, in tempo e denaro, è elevato e gli utenti, non disponendo sempre delle informazioni necessarie in merito ai rischi e ai vantaggi, hanno difficoltà a scegliere in modo ottimale.

Uno dei sistemi di sicurezza più diffusi su Internet è il protocollo **Secure Socket Layer** (SSL), un sistema che cifra le comunicazioni tra il web server ed il browser dell'utente. La diffusione di questa tecnologia, e in particolare della sua versione più potente a 128 bit, è stata frenata in passato dalle disposizioni restrittive degli Stati Uniti in materia di controllo sulle esportazioni.

Il regime statunitense è stato modificato di recente a seguito dell'adozione di un regime più liberale in materia di controllo sulle esportazioni di prodotti e tecnologie di cifratura.

Le statistiche rivelano che il numero di server web protetti in Europa è largamente inferiore a quello degli Stati Uniti (cfr. figura).

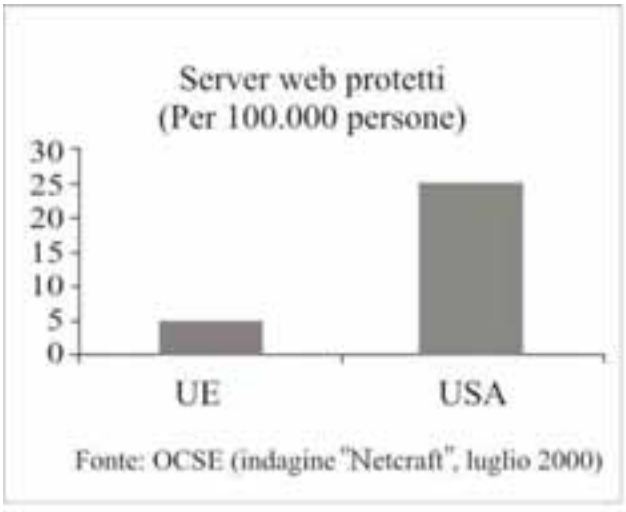


Figura 2-2 - Server dotati di misure di protezione

Operatori, utenti e produttori si devono confrontare con il problema della concorrenza e della non interoperabilità tra le norme esistenti. Ad esempio, in materia di protezione della posta elettronica due standard si contendono la supremazia sul mercato. L'importanza dell'Europa in questo campo è limitata.

Ne risulta una profusione di prodotti non europei che applicano questi standard e il cui utilizzo da parte degli utenti europei è subordinato alla politica in materia di controllo delle esportazioni americana. Alcuni Stati membri stanno valutando la possibilità di avvalersi di software di tipo open source.

Queste attività, tuttavia, si trovano ancora in una fase pilota, senza alcun coordinamento, e la volontà del mercato potrebbe prevalere sugli sforzi isolati delle autorità pubbliche. Per affrontare il problema nel modo migliore è necessaria una valutazione globale dei prodotti reperibili in commercio e delle soluzioni open source.

Accesso non autorizzato a computer e reti informatiche

L'accesso a computer e reti informatiche è normalmente autorizzato solo per i soggetti che superano un processo di autenticazione dell'utente, inteso come il riconoscimento dell'identità dichiarata.

Per molte applicazioni e servizi sono necessarie adeguate procedure di autenticazione: è questo il caso, ad esempio, della stipula di contratti on line, il controllo dell'accesso a determinati dati o servizi (ad es. per il telelavoro) e per l'autenticazione dei siti web (ad es. per i servizi di **home banking**).

Le modalità di autenticazione devono contemplare la possibilità dell'anonimato in quanto per molti servizi non è necessario conoscere l'identità dell'utente ma basta ottenere una conferma affidabile di taluni criteri (dette credenziali anonime), come ad esempio la capacità di pagamento.

L'accesso non autorizzato ad un computer o ad una rete di computer ha in genere finalità dolose e mira a copiare, modificare o distruggere i dati. Dal punto di vista tecnico si tratta di un'intrusione e può avvenire in diversi modi: uso di informazioni confidenziali inter-

ne, decifrazione di password mediante i cosiddetti **dictionary attacks**, attacco frontale (avvalendosi della tendenza degli utenti a scegliere password prevedibili), **ingegneria sociale** (avvalendosi della tendenza della gente a divulgare informazioni a persone apparentemente affidabili) o intercettazione di password. Spesso questo tipo di attacco è sferrato dall'interno dell'organizzazione.

L'accesso non autorizzato è talvolta motivato dalla sfida intellettuale piuttosto che dalla prospettiva di procurarsi un guadagno economico, anche se un fenomeno nato come semplice attività di disturbo ha messo in luce la vulnerabilità delle reti informatiche e spinto i pirati informatici mossi da intenti dolosi o criminali a sfruttare queste lacune. Proteggersi da un accesso non autorizzato ai propri dati personali, ad esempio finanziari o sanitari, è un diritto soggettivo. Per il settore pubblico e per le imprese il rischio va dallo spionaggio industriale all'alterazione dei dati pubblici o aziendali, fino alla corruzione dei siti web.

I metodi più comunemente utilizzati per difendersi dall'accesso non autorizzato consistono nell'installare una password e/o un firewall. Entrambi i sistemi offrono tuttavia una protezione limitata e devono essere integrati da altri dispositivi di sicurezza quali i dispositivi di riconoscimento di un attacco, di rilevamento delle intrusioni o i dispositivi a livello applicativo (come quelli che fanno uso di smart card). L'efficacia di questi sistemi dipende dal modo in cui le loro caratteristiche si contrappongono ai rischi che minacciano un determinato ambiente. È necessario pervenire ad un equilibrio tra protezione della rete e vantaggi legati alla libertà di accesso.

La rapida evoluzione tecnologica e le nuove minacce che questa comporta per le reti rendono necessaria una revisione permanente ed indipendente dei dispositivi di protezione. Fintantoché gli utenti e i fornitori non saranno pienamente consapevoli della vulnerabilità delle loro reti le soluzioni potenziali rimarranno inesplorate. Il grafico nella pagina che segue illustra l'impiego dei prodotti di protezione delle reti nell'Unione Europea (le statistiche si basano su un'indagine svolta nel febbraio 2001 nell'ambito delle analisi comparative dell'iniziativa eEurope 2002).

Figura 2-3 - Utilizzo di prodotti di sicurezza nell'ambito dell'UE

Caduta della rete

Gran parte delle reti sono ormai informatizzate e controllate da computer. In passato, la caduta della rete era spesso dovuta ad una disfunzione del sistema informatico che la controllava e gli attacchi erano rivolti soprattutto verso questi computer. Attualmente, invece, gli attacchi che causano le più gravi interruzioni sfruttano le debolezze e le vulnerabilità dei componenti della rete (sistema operativo, router, commutatori, server di nomi, ecc.).

Le aggressioni di questo tipo effettuate mediante la rete telefonica non hanno causato problemi di rilievo in passato ma sono piuttosto frequenti su Internet. Ciò è dovuto al fatto che i segnali telefonici di controllo sono separati dal traffico e possono pertanto essere protetti; su Internet, invece, gli utenti possono contattare i principali com-

puter che gestiscono il traffico. In futuro, tuttavia, le reti telefoniche potrebbero essere più vulnerabili a questi attacchi perché conterranno elementi costitutivi di Internet e i loro piani di controllo saranno divulgati ad altri operatori.

Gli attacchi di questo tipo possono assumere diverse forme:

- **attacchi rivolti al server dei nomi di dominio**: il funzionamento di Internet si basa su un sistema di nomi di dominio (Domain Name System - DNS) grazie al quale gli indirizzi di rete **significativi** per l'utente (ad es. europa.eu.int) vengono tradotti in nomi in forma astratta (ad es. IP 147.67.36.16) e viceversa. Se parte del DNS non funziona alcuni siti web non possono essere localizzati e i sistemi di recapito della posta elettronica potrebbe cessare di funzionare. La corruzione a livello dei root server del sistema DNS o di altri server di nomi di primo livello potrebbe paralizzare la rete. All'inizio del 2004 sono state evidenziate lacune nel software utilizzato dalla maggior parte dei server di nomi di dominio
- **attacchi rivolti ai router:** il routing su Internet è estremamente decentrato ed ogni router comunica regolarmente ai router contigui quali reti conosce e come raggiungerle. La vulnerabilità sta nel fatto che queste informazioni non possono essere verificate perché, per esigenze di progettazione, ogni router ha una conoscenza minima della topologia della rete. Ognuno di essi può quindi spacciarsi come la via migliore verso una determinata destinazione in modo da intercettare, bloccare o modificare il traffico diretto a tale destinazione
- **attacchi di tipo Denial of Service (diniego di servizio)**: questo tipo di attacchi paralizza la rete sovraccaricandola di messaggi artificiali che riducono o impediscono le possibilità di accesso legittimo da parte degli utenti. Sono fenomeni simili al blocco degli apparecchi fax attuato da messaggi lunghi e ripetuti. In particolare, il **flooding** consiste nel tentativo di sovraccaricare i server web o la capacità di trattamento dei fornitori di servizi Internet con messaggi generati automaticamente.

Le interruzioni hanno causato danni ad una serie di prestigiosi siti web. Alcuni studi hanno stimato in diverse centinaia di milioni di euro i danni provocati dagli attacchi più recenti, senza contare il pregiudizio intangibile in termini di immagine. Le imprese si avvalgono sempre più spesso di siti web per promuovere le proprie attività e quelle che dipendono da Internet per le forniture **just in time** sono particolarmente vulnerabili a questo tipo di attacchi.

Per difendersi dagli **attacchi ai server DNS** basta in genere estendere i protocolli DNS, ricorrendo ad esempio ad estensioni DNS protette con cifratura a chiave pubblica. Questa soluzione richiede tuttavia l'installazione di nuovo software sulle apparecchiature client e non è stata utilizzata molto spesso. Inoltre, l'efficacia della procedura amministrativa necessaria per ampliare la fiducia tra domini DNS deve essere migliorata.

Gli **attacchi al sistema di routing** sono invece molto più difficili da arginare. Internet è stato concepito all'insegna della flessibilità di routing per ridurre le probabilità di cessazione del servizio in caso di disfunzione di una parte dell'infrastruttura di rete. Non esistono mezzi efficaci per proteggere i protocolli di routing, soprattutto sui router della dorsale.

Il volume di dati trasmessi impedisce di filtrare con precisione il traffico perché una tale verifica paralizzerebbe la rete. Per lo stesso motivo, la rete effettua solo funzioni di filtraggio e di controllo dell'accesso poco sofisticate. Le funzioni di sicurezza più specifiche (autenticazione, integrità, cifratura) sono implementate alle estremità della rete, vale a dire sui terminali e i server che fungono da punti terminali. È dunque in tal sede che occorre agire per premunirsi contro attacchi di tipo Denial of Service.

Esecuzione di software maligni (malicious software) che modificano o distruggono i dati

I computer funzionano con le applicazioni software. Tali applicazioni, tuttavia, possono essere utilizzate anche per disattivare un computer o cancellare o modificare i dati che vi sono contenuti. Come indicato in precedenza, se il computer in questione fa parte del sistema di gestione della rete, una sua anomalia di funzionamento può

ripercuotersi su molti altri componenti della rete stessa.

Il virus è un tipo di software **maligno** che riproduce il proprio codice aggregandosi ad altri programmi in modo tale che il codice **virale** sia eseguito ogni volta che viene attivato il programma informatico infetto.

I software maligni possono tuttavia assumere altre forme: alcuni danneggiano solo il computer sul quale vengono copiati mentre altri si propagano verso gli altri computer della rete. Esistono, ad esempio, programmi (minacciosamente chiamati **logic bombs** o **bombe logiche**) che rimangono inerti fino al momento in cui vengono innescati da un determinato evento, come ad esempio una data (molto spesso venerdì 13). Altri programmi sono in apparenza benigni ma, una volta attivati, lanciano un attacco distruttivo (e per questo sono chiamati **cavalli di Troia**). Altri ancora, i cosiddetti **worm** (vermi), non infettano gli altri programmi ma si autoduplicano in copie che, riproducendosi a loro volta, finiscono col saturare il sistema.

I virus possono essere estremamente distruttivi, come dimostrato dagli elevatissimi danni provocati dai recenti virus **I Love You**, **Melissa** e **Kournikova**. Il grafico che segue illustra, per ogni Stato membro UE, l'aumento dei virus di cui sono stati vittime gli utenti Internet tra l'ottobre 2000 e il febbraio 2001. L'11% circa degli utenti europei di Internet ha subito un'infezione da virus informatico sul proprio PC domestico.

La principale difesa sono i **software antivirus**, disponibili in diverse forme. I software che funzionano come scanner di virus e disinfettanti hanno la capacità di individuare e distruggere tutti i virus conosciuti. La loro principale lacuna è che non individuano facilmente i nuovi virus, anche se vengono regolarmente aggiornati.

Un'altra contromisura è rappresentata dai software di verifica dell'integrità (gli **integrity checker**). Per infettare un computer il virus deve modificare un elemento del sistema e la verifica di integrità consente di individuare qualsiasi alterazione della struttura, anche se causata da un virus sconosciuto.

Per quanto evoluti siano i prodotti antivirus, i problemi dovuti ai software maligni sono in aumento. Le ragioni principali sono due:

in primo luogo, la struttura aperta di Internet consente ai pirati di informarsi a vicenda e di mettere a punto strategie di aggiramento delle barriere di protezione. In secondo luogo, Internet si espande e tocca nuovi utenti, molti dei quali non sono consapevoli della necessità di proteggersi. Il livello di sicurezza dipende dall'uso effettivo e generalizzato del software di difesa antivirus.

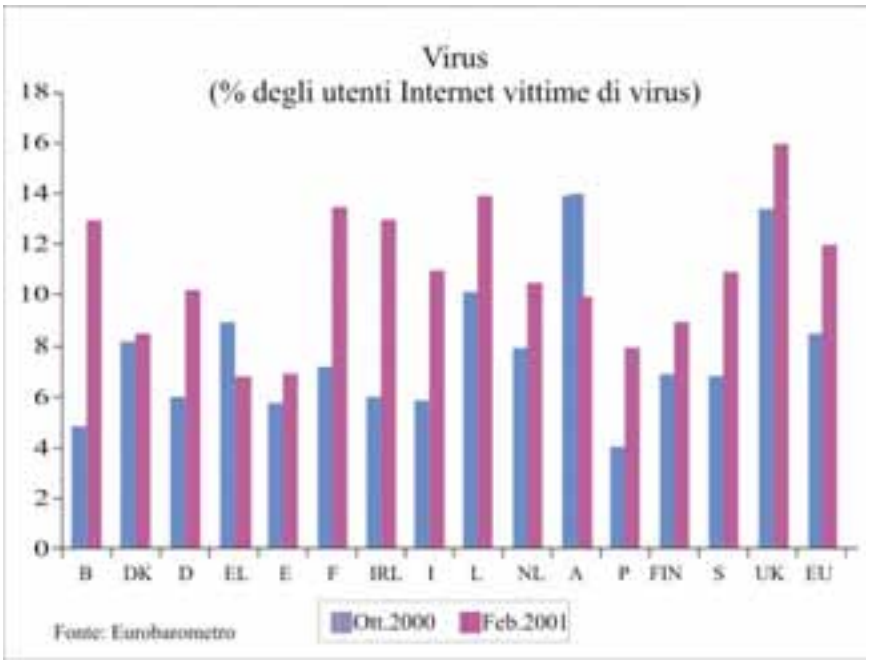


Figura 2-4 - Incidenza dei virus nell'UE tra Ottobre 2000 e Febbraio 2001

Usurpazione di identità

Al momento di stabilire un collegamento alla rete o di ricevere dati, l'utente deduce l'identità del suo interlocutore in funzione del contesto in cui avviene la comunicazione. La rete presenta una serie di indicatori al riguardo, ma il rischio principale di attacco è rappresentato dagli **iniziati**, da coloro cioè che conoscono il contesto della comunicazione. Digitando un numero o un indirizzo Internet sulla tastiera del computer l'utente deve raggiungere la destinazione prevista. Se questo può bastare per molte applicazioni, non è così per le importanti transazioni commerciali o per le comunicazioni di tipo medico, finanziario o ufficiale, che richiedono un maggiore livello di autenticazione, integrità e riservatezza.

L'**usurpazione dell'identità** di persone o organismi può causare inconvenienti di diverso tipo. I clienti potrebbero scaricare software maligno da un sito web che si fa passare per una fonte affidabile e potrebbero anche rivelare informazioni riservate alla persona sbagliata. Un'usurpazione di identità può avere come conseguenza la nullità di un contratto, ecc. Forse il danno maggiore è proprio il fatto che la mancanza di un'autenticazione frena nuove iniziative economiche. Molti studi confermano che il motivo principale che dissuade le imprese dall'operare su Internet sono proprio i timori riguardo alla sicurezza. Se vi fosse la certezza dell'identità dell'interlocutore il livello di fiducia nelle operazioni economiche su Internet aumenterebbe.

L'introduzione di un'autenticazione legata all'adozione del sistema SSL rappresenta indiscutibilmente un passo avanti in materia di riservatezza dei dati in rete. Le reti virtuali private (VPN) usano il sistema SSL e il protocollo IPSec per trasmettere su reti Internet non protette e canali aperti mantenendo un determinato livello di protezione. Queste soluzioni hanno tuttavia un'utilità limitata in quanto si affidano a certificati elettronici che non forniscono piena garanzia di non essere stati contraffatti.

Spetta a un terzo, spesso chiamato **autorità di certificazione** o, nella direttiva UE sulla firma elettronica (vedi All. 1-B), **prestatore di servizi di certificazione**, la funzione di prestare tali garanzie. Il problema legato alla diffusione di questa soluzione è simile a quello incontrato in materia di cifratura, ossia la necessità di un'interoperabi-

lità e di una gestione delle chiavi. Questo problema non si pone per le reti VPN, per le quali possono essere sviluppate soluzioni proprietarie ma per le reti pubbliche rimane uno degli ostacoli principali.

La direttiva sulle firme elettroniche detta le norme destinate a facilitare l'autenticazione elettronica all'interno dell'UE. Essa fornisce un quadro di riferimento che consente al mercato di crescere ma prevede anche incentivi per le imprese che sviluppano firme più sicure destinate ad un riconoscimento giuridico. La direttiva è attualmente in fase di recepimento negli Stati membri, tra cui l'Italia si trova in una posizione d'avanguardia.

Incidenti ambientali ed eventi imprevisti

Molti incidenti in materia di sicurezza sono dovuti ad eventi imprevedibili ed involontari quali:

- **catastrofi naturali** (tempeste, inondazioni, incendi, terremoti)
- **terzi estranei** a qualsiasi rapporto contrattuale con l'operatore o l'utente (ad es. interruzione dovuta a lavori di costruzione)
- **terzi aventi un rapporto contrattuale con l'operatore o l'utente** (ad es. guasti dell'hardware o del software dei componenti o dei programmi consegnati)
- **errore umano dell'operatore** (compreso il fornitore del servizio) **o dell'utente** (ad es. problemi di gestione della rete, installazione errata del software).

Le **catastrofi naturali** possono causare interruzioni nella disponibilità di una rete. Purtroppo è proprio in occasione di eventi di questo tipo che il funzionamento delle linee di comunicazione è assolutamente indispensabile. Guasti dell'hardware e inadeguata progettazione del software sono causa di vulnerabilità che possono portare ad un'immediata interruzione della rete o essere sfruttate da pirati informatici. Anche una gestione poco oculata della capacità della rete può causare una congestione del traffico che rallenta o paralizza i canali di comunicazione.

In tale contesto la ripartizione delle responsabilità tra le parti interessate riveste un'importanza cruciale. Nella maggior parte dei casi gli utenti non saranno responsabili della situazione ma le loro possibilità di esigere un risarcimento saranno scarse se non addirittura nulle.

Gli operatori delle reti di telecomunicazioni sono consapevoli dei rischi degli **incidenti ambientali** e da tempo costruiscono reti ridondanti e dispositivi di protezione delle loro infrastrutture. La maggiore pressione concorrenziale potrebbe avere conseguenze ambivalenti sul comportamento degli operatori. Da un lato, i prezzi potrebbero spingere gli operatori a ridurre tali ridondanze ma, d'altro lato, il maggior numero di operatori presenti sul mercato per effetto della liberalizzazione, consente agli utenti di trasferirsi verso un altro operatore qualora la rete utilizzata non risultasse più disponibile.

Le pertinenti disposizioni del diritto comunitario obbligano tuttavia gli Stati membri a prendere tutte le misure necessarie per garantire la disponibilità delle reti pubbliche in caso di guasto catastrofico o di catastrofe naturale (cfr. direttiva 97/33/CE sull'interconnessione e direttiva 98/10/CE sulla telefonia vocale, Codice delle Telecomunicazioni). Il numero crescente di reti interconnesse fa sì che non si conosca con certezza il livello di sicurezza di questo settore.

La concorrenza dovrebbe spingere i **produttori di hardware e di software** ad accrescere il livello di sicurezza dei prodotti. Ma la pressione della concorrenza non è tale da generare investimenti in materia di sicurezza, tanto più che questa non sempre è un elemento determinante nella decisione di acquisto. Le lacune in materia di sicurezza vengono spesso alla luce troppo tardi, quando il danno è fatto. Preservando un comportamento di concorrenza leale sul mercato delle tecnologie dell'informazione si creeranno migliori presupposti per lo sviluppo della sicurezza.

I rischi di errori umani e tecnici potranno essere ridotti mediante azioni di formazione e di sensibilizzazione. L'istituzione di un'adeguata politica della sicurezza a livello di ogni singola azienda potrebbe contribuire a contenere i rischi.

Nuove sfide

La sicurezza delle reti e dell'informazione è destinata a diventare un fattore determinante dello sviluppo della società dell'informazione dato che le reti svolgono un ruolo sempre più importante nella vita economica e nella vita sociale. Al riguardo, due sono i fattori principali che vanno presi in considerazione: l'aumento dei danni potenziali e l'emergere di nuove tecnologie.

Le reti e i sistemi informativi contengono sempre più spesso dati sensibili e preziose informazioni commerciali, con conseguenti maggiori incentivi per attacchi di pirateria informatica. Gli attacchi possono avvenire ad un basso livello ed avere conseguenze irrilevanti sul piano nazionale (corruzione di un sito web personale o riformattazione di un disco rigido ad opera di un virus). L'interruzione può tuttavia avvenire su scala molto più ampia ed interferire con comunicazioni estremamente sensibili, provocare gravi interruzioni dell'alimentazione di energia elettrica o causare gravi danni alle imprese tramite attacchi di tipo **denial of service** o violazioni della riservatezza.

È difficile valutare i danni reali e potenziali di una violazione della sicurezza delle reti. Non esiste sull'argomento un sistema di segnalazioni sistematiche, anche perché molte imprese preferiscono non ammettere di essere state vittima di attacchi informatici per timore di pubblicità negativa. Le prove finora raccolte sono quindi essenzialmente aneddotiche e i costi comprendono non solo i costi diretti (perdita di introiti, perdita di informazioni utili, spese di ripristino della rete) ma anche diversi costi immateriali, in particolare in termini di immagine, difficili da quantificare.

La sicurezza delle reti e delle informazioni è un problema evolutivo. La rapidità dei cambiamenti tecnologici pone continuamente nuove sfide; i problemi di ieri sono risolti ma le soluzioni di oggi sono già superate. Il mercato sforna nuovi applicativi, nuovi servizi e nuovi prodotti praticamente tutti i giorni. Vi sono tuttavia taluni sviluppi che rappresenteranno senza dubbio importanti sfide per i responsabili della sicurezza dei settori pubblico e privato:

- sulle reti saranno trasmesse opere digitali (opere multimediali, software scaricabile, mobile agents) recanti, integrate, le caratteristiche di sicurezza. Il concetto di disponibilità, considerata

oggi come la possibilità di utilizzare una rete, tenderà ad avvicinarsi a quello di uso autorizzato, come ad esempio il diritto di utilizzare un videogioco per un determinato periodo di tempo, il diritto di creare una singola copia di un software, ecc.

- in futuro gli operatori delle reti IP tenteranno di accrescere il livello di sicurezza ricorrendo ad una supervisione sistematica delle comunicazioni che lascerà filtrare solo il traffico autorizzato. Tali misure dovranno tuttavia essere compatibili con le pertinenti disposizioni in materia di protezione dei dati personali
- gli utenti opteranno per collegamenti permanenti ad Internet e ciò moltiplicherà le possibilità di attacco e la vulnerabilità dei terminali non protetti, consentendo ai pirati di sottrarsi ai dispositivi di individuazione
- si assisterà alla diffusione delle reti domestiche a cui saranno collegati numerosi apparecchi e dispositivi. Ciò aumenterà le possibilità di pirateria e la vulnerabilità degli utenti (ad esempio, i segnali di allarme potranno essere disattivati a distanza)
- la diffusione su larga scala delle reti senza filo (ad es. rete locale senza filo o wireless local area network, servizi mobili della terza generazione) porrà il problema di un'efficace cifratura dei dati trasmessi via radio. Sarà pertanto sempre più difficile imporre per legge un basso livello di cifratura dei segnali
- le reti e i sistemi di informazione saranno onnipresenti, in configurazione mista fissa e mobile, e rappresenteranno **l'intelligenza ambiente**, vale a dire una serie di funzioni autogestite ed attivate automaticamente che prenderanno decisioni in precedenza prese dall'utente. La sfida consisterà nell'evitare un livello inaccettabile di vulnerabilità e nell'integrare l'elemento sicurezza nell'architettura dei sistemi.

2.4 UN ESEMPIO DI RETE SICURA: LA RETE UNITARIA DELLA PA[2]

All'inizio degli anni '90, anche per la mancanza di un organismo che rendesse armonico il contesto delle telecomunicazioni nelle Pubbliche Amministrazioni, esisteva una pluralità di reti dati nate dalle differenti esigenze che nel corso degli anni si erano presentate. Nel 1997 si è proceduto a razionalizzare tale scenario in un'unica rete, omogenea per qualità, sicurezza e costi, che ha rappresentato per le Amministrazioni Centrali la piattaforma di sviluppo delle applicazioni.

La R.U.P.A. (Rete Unitaria della Pubblica Amministrazione) oggi collega con circa 20.000 accessi la totalità delle sedi delle pubbliche amministrazioni centrali. Al suo backbone sono ad oggi collegate anche la totalità delle reti delle Regioni alla data attive per un totale complessivo di 90 Enti interconnessi tra PA Centrali e PA Locali.

2.4.1 L'infrastruttura tecnologica: il disegno della rete

Il disegno dell'architettura della RUPA è stato concepito, nelle sue fasi di progettazione e realizzazione, osservando alcuni principi che si ritenevano condizioni necessarie per assicurare alla rete adeguati standard di sicurezza. Due sono stati i criteri fondamentali cui il disegno della RUPA è stato improntato:

- utilizzazione di linee guida derivate da esperienze precedenti nella realizzazione di strutture con caratteristiche simili
- adozione di un modello di risk analysis che evidenziasse macroscopicamente le aree di rischio potenziale e le adeguate contromisure.

---

[2] *Il paragrafo contiene contributi tratti da:*

- *"CNIPA - Sistema Pubblico di Connettività - Organizzazione della sicurezza" (Emesso da: gdl Organizzazione e Qualificazione - Coordinato da: Mario Terranova - Edizione 1.4 del 26/11/2003).*
- *"CNIPA- Sistema Pubblico di Connettività - Scenario introduttivo" (Emesso da: gdl SPC - Coordinatore: Francesco Pirro - Edizione 3.2 del 07/04/2004).*
- *"Autorità per l'Informatica nella Pubblica Amministrazione - La sicurezza dei servizi in rete - requisiti, modelli, metodi e strumenti"- Versione 1.0 del 14/11/2001.*

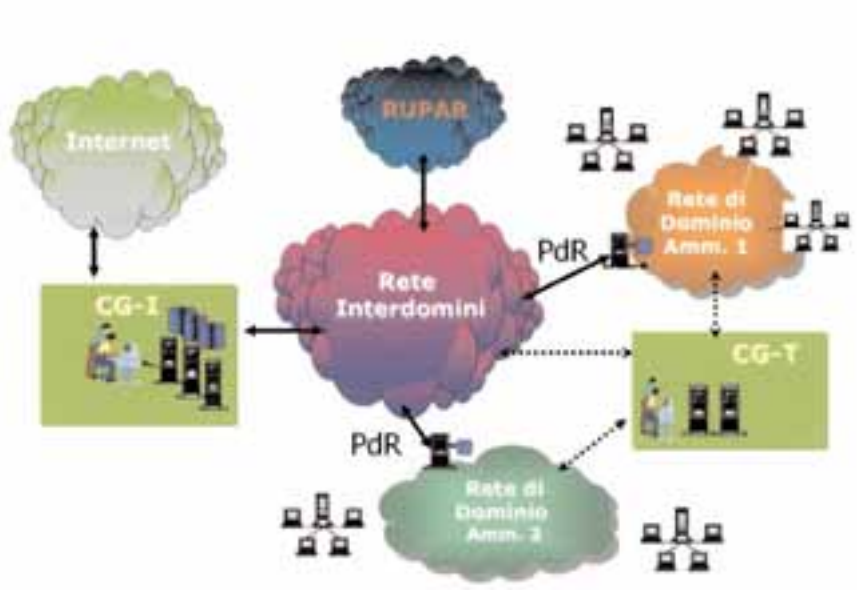


Figura 2-5 - L'architettura generale della RUPA

Le linee guida utilizzate nella progettazione dell'infrastruttura del Centro di Gestione, organo centrale di supervisione e gestione, hanno inteso enfatizzare le caratteristiche di disponibilità dell'intero sistema, in particolare:

- è stata prevista l'installazione, in modalità ridondata, di tutti i principali componenti per garantire il funzionamento nel caso d'avaria
- i componenti sono stati selezionati in base alle caratteristiche intrinseche di fault resiliency
- la rete interna insiste su una struttura a matrice
- sono stati adottati, per tutti i componenti, criteri di conformità a standard (de iure o de facto) per garantirne l'interoperabilità

- tutti i componenti utilizzati sono stati sottoposti ad un processo di misurazione dello stato di funzionamento.

Oltre alle caratteristiche tecniche suddette si è utilizzato, per la parte di gestione, un processo di Risk Analysis che ha consentito, a sua volta, di individuare le azioni atte a compromettere l'integrità del sistema (minacce), la vulnerabilità del sistema alle minacce, nonché l'effetto che l'evento di una qualsiasi violazione ha sul sistema.

2.4.2 Gestione della sicurezza

È particolarmente importante sottolineare la potenzialità dell'infrastruttura di sicurezza messa in atto per il monitoraggio della componente relativa ai servizi. Il Centro di Gestione ha un altissimo livello di controllo per i messaggi scambiati fra le Amministrazioni e presenta elevatissime caratteristiche di sicurezza per ciò che concerne gli aspetti di riservatezza, crittografia ed anti-intrusione.

Lo stato del livello d'accesso ed uso della rete (sulla RUPA circolano ogni giorno 37 gigabyte di dati distribuiti tra migliaia di messaggi di posta elettronica e 5 milioni di pagine WEB visitate quotidianamente dagli utenti della rete) è costantemente controllato da due strategie concorrenti di monitoraggio e verifica:

- le attività di monitoraggio e verifica prevedono la conduzione su base periodica di una serie di test dello stato di vulnerabilità della rete e dei suoi dispositivi. I test imitano tecniche note di intrusione e collaudano le configurazioni adottate secondo schemi d'attacco definiti ad hoc
- il test di vulnerabilità è parte del processo di certificazione dei cambiamenti dell'infrastruttura di rete e del processo di mantenimento delle prestazioni del sistema.

Le attività di monitoraggio insistono sul controllo costante dell'utilizzo dell'infrastruttura e segnalano l'insorgere di comportamenti anomali mediante l'uso di sensori installati in diversi segmenti della rete (reazione ad eventi).

Il test di vulnerabilità è effettuato attraverso un insieme di procedure che analizzano automaticamente la rete e i segmenti gestiti dal Centro, predisponendo un catalogo dei componenti (indirizzi IP) e dei servizi disponibili (porte). In un momento successivo altre procedure applicano ai componenti del catalogo una serie di azioni, appartenenti ad un insieme definito da regole, che verificano il comportamento del componente stesso a seguito di una richiesta di servizio.

Le due strategie sono complementari: il monitoraggio controlla costantemente lo stato della rete, mentre i test di vulnerabilità verificano la soglia di intervento dei sensori e forniscono le linee guida per la configurazione del singolo sensore. Le segnalazioni dei sensori individuano la localizzazione delle situazioni di attacco e indirizzano la conduzione di test specifici su particolari componenti.

Tali misure si sono rilevate di effettiva efficacia ed hanno permesso alla rete RUPA, sin dalla sua creazione, di respingere con successo attacchi di virus che, per altre realtà, hanno rappresentato una perdita considerevole sia in termine finanziario sia di immagine.

Nell'anno 2001 la RUPA ha subito oltre 99 milioni di attività ostili, di cui 95 milioni di attacchi (respinti) indirizzati verso i siti Web pubblicati sulla RUPA, e nel 2002, fino a settembre, circa 79 milioni. Nel 2003, solo fino a Marzo, sono stati respinti oltre 15 milioni di attacchi indirizzati verso i siti web pubblicati sulla RUPA.

Gli attacchi di Nimda sono iniziati il 14 settembre 2001 in Internet. Sulla rete si ha la rilevazione del primo allarme grave alla fine del 18 settembre; il picco avviene il 19 settembre con ben 9 milioni di attacchi, tutti respinti.

Gli attacchi del worm SQL SLAMMER, rilevati a gennaio 2003, non hanno causato impatti grazie alla corretta e tempestiva applicazione delle contromisure tecnologiche ed architetturali.

Ad aprile 2003, si registra il tentativo bloccato di Denial of Service verso una rilevante Amministrazione Centrale (invio di oltre 100.000 pacchetti ostili al minuto).

2.4.3 Evoluzioni della rete

La Rete Unitaria, così come è oggi strutturata e utilizzata, prossimamente andrà a evolversi e a innestarsi all'interno del nuovo modello di infrastruttura della PA: il Sistema Pubblico di Connettività (SPC), istituito dal D. lgs. 28 febbraio 2005 n.42.

Il sistema SPC nasce dalla necessità di permettere alla pluralità di attori presenti in un mercato competitivo, come quello della fornitura di servizi telematici, di concorrere all'innovazione tecnologica realizzando un sistema di **fiducia**, con regole di interconnessione comuni, che permetta a tutte le PA di essere connesse tra loro con gli adeguati standard di qualità e sicurezza e che garantisca l'integrità e l'omogeneità dello sviluppo del sistema telematico in linea con l'evoluzione della tecnologia.

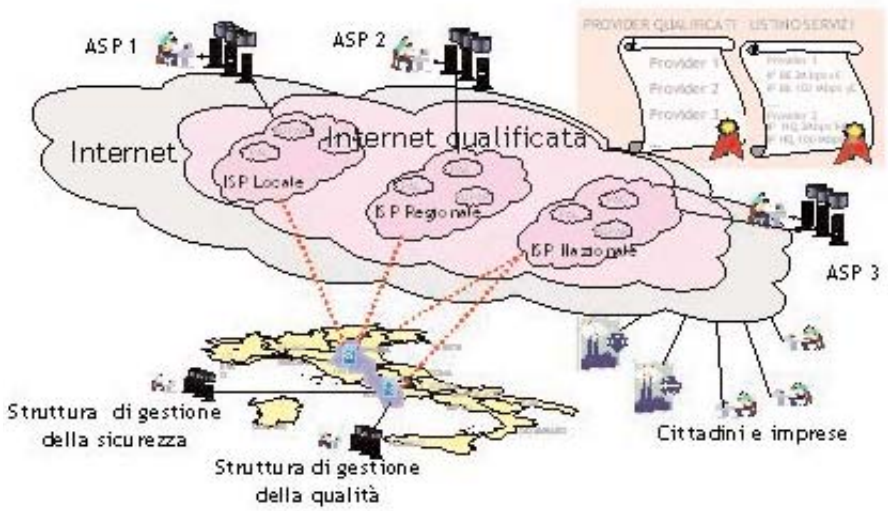


Figura 2-6 - SPC: infrastruttura, regole e modello organizzativo

Il sistema SPC presenta lineamenti architetturali che prevedono un modello di rete multi-fornitore nella quale ogni operatore, fornitore dei servizi SPC, ha come clienti un determinato numero di Amministrazioni. La qualità e la sicurezza di ciascun fornitore sarà garantita attraverso una procedura di qualificazione secondo regole prestabilite e concordate.

I principali obiettivi che si intendono raggiungere con l'adozione del SPC sono:

- fornire dei **servizi di interconnessione** i cui principi fondamentali, in merito a omogeneità sicurezza e qualità, siano chiaramente **definiti** ma, grazie a queste caratteristiche, siano ampiamente **configurabili ed adattabili** alle caratteristiche ed alle specifiche esigenze di ciascuno degli Enti interconnessi
- garantire la **possibilità estesa di interconnessione** permettendo a tutti i soggetti presenti in Internet l'interazione con gli Enti e le Pubbliche Amministrazioni
- fornire, pur salvaguardando gli investimenti ad oggi effettuati, un'infrastruttura di **connessione condivisa ed omogenea** tra tutte le reti della PA
- fornire **servizi ed infrastrutture**, per le Amministrazioni interessate, che permettano anche l'interconnessione all'interno del Domino dell'Amministrazione stessa
- realizzare un **modello di servizi multi-fornitore allineato e coerente** con gli attuali scenari di mercato
- garantire, anche tramite la qualificazione degli operatori fornitori dei servizi, un **sistema di qualità** sia in termini di prestazioni sia di disponibilità nonché assicurare un sistema di raccolta ed analisi dei dati per un controllo costante della qualità dei servizi
- garantire **misure di sicurezza** in grado di assicurare la continuità e la disponibilità dei servizi sia tra le Amministrazioni stesse sia verso i cittadini per minimizzare le possibilità di disservizi.

Quest'ultimo obiettivo (garanzia della sicurezza e garanzia della qualità del servizio) rappresenta l'elemento caratterizzante del SPC.

La necessità di realizzare un Sistema nel quale la comunicazione tra le diverse Amministrazioni avvenga con caratteristiche di qualità e sicurezza garantite **end to end**, in un contesto multi-fornitore, implica, oltre alla realizzazione dell'infrastruttura di interconnessione e controllo, anche la definizione di opportune **regole** che devono essere rispettate da tutti gli attori coinvolti. Infatti, per le peculiarità proprie dell'architettura di una rete distribuita all'interno della quale operano organizzazioni e strutture diverse sia per tipologia di servizio sia per processi ed organizzazione, è necessaria la creazione di livelli di **governo**, centrali e locali, che siano in grado di indirizzare, armonizzare e coordinare le strutture operative in modo da costituire ed operare come un'unica organizzazione virtuale.

L'organizzazione del Sistema di Sicurezza del SPC, ispirata ai modelli proposti dall'International Standard Organisation (ISO), sarà articolata su più livelli distinguendo le responsabilità e gli ambiti di intervento in due aree principali:

- un'area di **governo** per la definizione di politiche e direttive
- un'area **operativa** per l'attuazione ed il controllo delle misure e delle procedure atte a garantire la qualità e la sicurezza delle comunicazioni.

Tali aree includeranno i gruppi di seguito elencati.

La **Struttura di Coordinamento** è principale responsabile della sicurezza del sistema. Si tratta di un organismo federato presieduto dal Presidente del CNIPA, costituto da tredici componenti di cui sei rappresentanti delle Amministrazioni Centrali e sei delle Amministrazioni locali. È suo compito definire, in funzione delle esigenze di fruitori ed erogatori del servizio, le politiche di sicurezza ed emanare le relative direttive e raccomandazioni per salvaguardare sia la sicurezza del sistema di interconnessione sia quella delle altre reti collegate. La Struttura di Coordinamento avrà anche il compito di gestire le procedure di qualificazione dei fornitori di servizi.

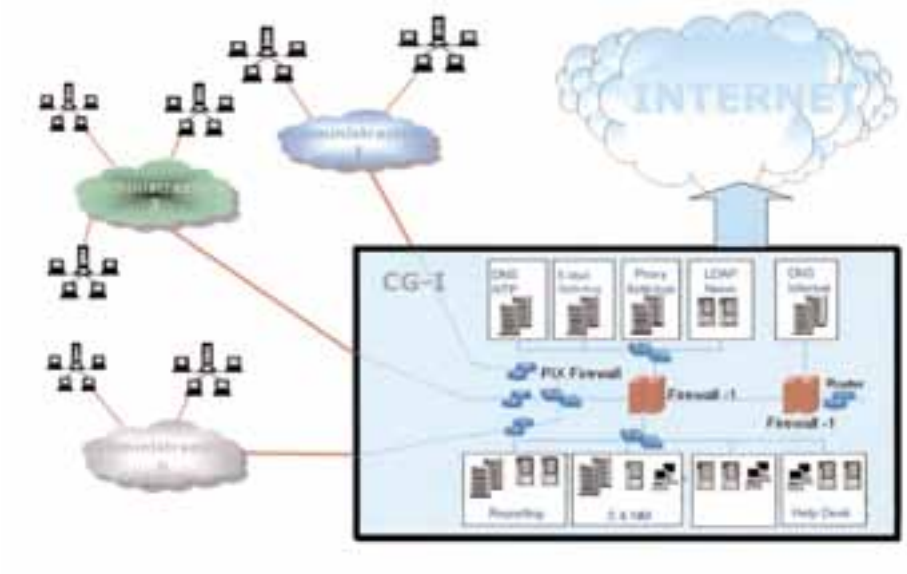


Figura 2-7 - Il CG-I e le categorie di servizi - Il CG-I connette tutte le Amministrazioni Centrali e consente loro di accedere ad Internet attraverso un canale veloce e sicuro.

Il **Comitato strategico** è una struttura comune che si occupa dell'indirizzo strategico globale della sicurezza, curando anche l'assegnazione dei relativi fondi. Il Comitato è composto da esperti di sicurezza e di telecomunicazioni, nonché da rappresentanti del Ministero per l'Innovazione e le Tecnologie e degli utenti.

Il **Centro di Gestione della Sicurezza** cura l'attuazione di quanto emanato dalla Struttura di Coordinamento in termini di realizzazione ed applicazione delle direttive e delle raccomandazioni per la salvaguardia della sicurezza. È suo compito anche l'individuazione delle linee guida per la stesura del piano della sicurezza di tutti i soggetti del SPC.

L'**Unità Locale di Sicurezza** è una struttura locale, una per ogni rete collegata al sistema, che ne gestisce gli aspetti di sicurezza. Tutte le Unità di Sicurezza devono essere collegate tra loro, con i fornitori di servizi e con il CERT, per permettere la maggiore efficienza possibile nello scambio di **informazioni sicure** in caso di risposta ad attacchi e/o eventi anomali.

Il **CERT SPC** svolge un ruolo fondamentale nella prevenzione e nella risposta agli incidenti di sicurezza. Esso mette a disposizione di tutte le altre strutture avvisi, linee-guida, check-list e tutto quello che può essere utile per la corretta gestione dei sistemi.

Nell'ambito del SPC è fatto largo uso di certificati digitali per scopi diversi. Il **Gestore Tecnico della PKI** è una Certification Authority che si fa carico dell'emissione dei certificati, della gestione delle varie directory in cui questi sono organizzati e di quanto è necessario per garantire la disponibilità e l'accessibilità delle informazioni di autenticazione degli utenti e dei sistemi.

3 - La normativa legale pertinente

3.1 QUADRO NORMATIVO GENERALE DI RIFERIMENTO

3.1.1 Generalità

Il quadro normativo relativo al sistema delle reti teleinformatiche è semplice e complesso nello stesso tempo. Mentre, infatti, gli strumenti legislativi effettivamente emanati dallo Stato italiano sono, per le aziende e l'utenza private, relativamente pochi, numerosi sono invece quelli per il settore pubblico unitamente ad altri elementi complementari, quali le direttive europee, alcuni documenti di prestigiosi organismi internazionali (vedi OCSE) e, soprattutto, documenti e circolari emanati dal Ministero per l'Innovazione e le Tecnologie, dall'AIPA, dal CNIPA (che, com'è noto, ha sostituito l'AIPA).

In generale si può osservare che, mentre nel settore pubblico le norme intese a promuovere l'utilizzo della rete e a regolamentarne la sicurezza sono state, particolarmente nel corso degli ultimi anni, numerose e idonee a promuovere, accanto al progresso tecnologico, la consapevolezza della sicurezza e le relative soluzioni, in ambito privato il cammino da fare sembra ancora lungo. Per altro, molto di quanto operato nell'ambito pubblico potrebbe servire di stimolo e guida per le imprese e anche, fatte le debite proporzioni, per l'utenza privata.

L'illustrazione del quadro normativo in questione è, nel presente documento, articolata secondo due vettori. Il primo evidenzia la valenza, diciamo così, giuridica del documento, distinguendo tra docu-

menti di organismi non strettamente governativi anche se di consolidata reputazione, raccomandazioni della UE, leggi dello Stato e, in fine, documenti rilevanti per l'autorevolezza delle fonti (AIPA, CNIPA ecc.). Il secondo individua, invece, i destinatari dei diversi documenti e norme, distinguendo tra Pubblica Amministrazione, imprenditoria privata e cittadini singoli.

Nel paragrafo che segue si è cercato di estrarre dalle diverse fonti normative quanto potesse esser utile a definire un profilo obbligatorio (cogente) di misure di protezione, riferito ai diversi soggetti protagonisti dello scenario nazionale del sistema reti. Va, al riguardo, osservato che pur avendo un quadro normativo che ha registrato nel corso dell'ultimo decennio un rilevante incremento in termini di numero e consistenza delle contromisure previste, sia sul piano organizzativo che tecnico, i soggetti dovrebbero non limitarsi a tali suggerimenti, che sono da considerarsi piuttosto come uno zoccolo duro obbligatorio, da integrare in base a un opportuno processo di analisi dei rischi.

L'elenco delle fonti è riportato nell'Allegato 1 e comprende, per completezza, quanto riguarda il settore della firma elettronica e digitale che tuttavia, per la peculiare fattispecie funzionale, non è da considerarsi vera e propria componente strutturale di protezione delle reti. Stante il carattere essenzialmente informativo-pratico di questo documento, non sono state riportate le normative riassorbite in provvedimenti più recenti (tipico è il caso delle norme precedenti al D. lgs. 30 giugno 2003, n. 196 - Codice in materia di protezione dei dati personali - e in quest'ultimo ricomprese).

3.1.2 Documenti dell'OCSE e delle Nazioni Unite

I documenti dell'Organizzazione per la cooperazione e lo Sviluppo Economico (OECD in inglese, OCDE in francese) costituiscono, anche per il credito di cui godono presso gli organi normativi dell'UE, una fonte di riferimento di elevato valore sul piano sociale ed etico.

Rilevante, ai fini del presente documento, è la Raccomandazione del Consiglio in data 25 luglio 2002, intitolata ***"Linee Guida dell'OCSE sulla sicurezza dei sistemi e delle reti d'informazione:***

verso una cultura della sicurezza" di cui si riassume di seguito il contenuto.

Sotto il comune denominatore della promozione della cultura della sicurezza si enunciano nove principi:

1. **Sensibilizzazione** - Le parti interessate devono essere consapevoli della necessità di tutelare la **sicurezza dei sistemi e delle reti d'informazione** e delle azioni che possono intraprendere per rafforzare la sicurezza.
2. **Responsabilità** - Le parti interessate sono responsabili della **sicurezza dei sistemi e delle reti d'informazione**.
3. **Risposta** - Le parti interessate devono operare tempestivamente e in uno spirito di cooperazione per prevenire, rilevare e rispondere agli incidenti di sicurezza.
4. **Etica** - Le parti interessate devono rispettare i legittimi interessi delle altre parti.
5. **Democrazia** - La **sicurezza dei sistemi e delle reti d'informazione** deve essere compatibile con i valori fondamentali di una società democratica.
6. **Valutazione dei rischi** - Le parti interessate devono procedere a valutazioni dei rischi.
7. **Concezione e applicazione della sicurezza** - Le parti interessate devono integrare la sicurezza quale elemento essenziale dei **sistemi e delle reti d'informazione**.
8. **Gestione della sicurezza** - Le parti interessate devono adottare un approccio globale della gestione della sicurezza.
9. **Rivalutazione della sicurezza** - Le parti interessate devono esaminare e rivalutare la sicurezza dei sistemi e delle reti d'informazione e introdurre adeguate modifiche nelle loro politiche, pratiche, azioni e procedure di sicurezza.

Non è secondario osservare che (siamo nel 2002!) il sottotitolo del documento recita: *"Verso una cultura della sicurezza"*!

Sulla stessa linea del documento dell'OCSE è la risoluzione delle Nazioni Unite A/RES/58/199 del 23.12.2003 intitolata "Creation of a global culture of cyber-security and the protection of critical information infrastructures"

La risoluzione invita gli stati membri a considerare undici principi di sicurezza, ampiamente basati su quelli adottati dal G8 nel marzo del 2003.

La tabella 3-1, redatta dal NISCC (National Infrastructure Security Coordination Centre), indica i principi indicati dalla risoluzione N.U. con i riferimenti a quelli proposti nel documento OCSE in precedenza indicati. Come si può notare, rispetto al documento OCSE, ampiamente orientato alla società, agli operatori e agli utenti (principi 2, 4 e 5), la risoluzione delle Nazioni Unite appare più specificamente rivolta ai Governi e alle forze dell'ordine (principi 6, 7 e 9).

3.1.3 Direttive e altri documenti UE

Negli ultimi anni il Governo italiano non ha mancato di attuare con lodevole tempestività le direttive UE in materia di reti e sicurezza informatica. Notevole è la risoluzione del Consiglio (Trasporti/Telecomunicazioni) in data 11 dicembre 2001 *"Resolution on network and information security"*. Nel documento si richiede ai paesi membri, per la fine del 2002, di:

- promuovere la cultura della sicurezza con **campagne educative** presso amministrazioni, aziende private, ISP ecc.
- promuovere **best practices** di sicurezza basate su standard internazionali anche e soprattutto presso aziende medie e piccole
- promuovere la **sicurezza nei corsi di informatica**
- potenziare i **computer emergency response team**
- promuovere la conoscenza e l'adozione dello **standard di sicurezza Common Criteria** (CC) recepito nella norma ISO-15408
- promuovere lo studio e l'adozione di **dispositivi biometrici**
- promuovere lo scambio d'informazioni e **cooperazione tra paesi membri**.

Argomenti	Principi della risoluzione UN 58/199	Riferimento ai principi OCSE
Avvisi e reazione agli incidenti	1. Disporre di strutture sulla rete per fornire avvisi circa le vulnerabilità informatiche, le minacce e gli incidenti.	3. Risposta
	5. Realizzare e mantenere reti di comunicazioni per situazioni di crisi, collaudandole periodicamente per assicurarne l'efficienza nei momenti d'emergenza.	
Promozione della consapevolezza e formazione	2. Promuovere la consapevolezza per agevolare la comprensione, da parte di tutte le parti coinvolte, dell'estensione e della natura delle proprie infrastrutture informatiche critiche e del ruolo che ciascuna parte ha nella protezione delle stesse.	1. Sensibilizzazione
	8. Condurre attività formativa ed esercitazioni per aumentare il grado di reattività e collaudare piani di continuità e di crisi in caso di attacchi alle infrastrutture informatiche, incoraggiando i corrispondenti ad effettuare analoghe attività.	
Analisi del rischio	3. Esaminare le infrastrutture e identificare le loro interdipendenze, in modo da incrementare il loro grado di protezione.	6. Valutazione dei rischi
		8. Gestione della sicurezza
		9. Rivalutazione della sicurezza
Tecnologia della sicurezza	11. Promuovere ricerche e sviluppi nazionali e internazionali e favorire l'applicazione di tecnologie di sicurezza coerenti con gli standard internazionali.	7. Concezione e applicazione della sicurezza
	4. Promuovere la collaborazione tra le diverse parti, sia pubbliche che private, per condividere e analizzare le informazioni relative alle infrastrutture critiche al fine di prevenire, investigare, reagire relativamente ad attacchi e danni concernenti tali infrastrutture.	
Condivisione delle informazioni e collaborazione internazionale	10. Impegnarsi in idonee collaborazioni internazionali al fine di porre in sicurezza sistemi informatici critici, anche tramite lo sviluppo e il coordinamento di sistemi di avviso e allarme, disseminazione e condivisione di informazioni riguardanti vulnerabilità, minacce e incidenti e coordinando attività investigative relative ad attacchi a tali sistemi informatici, in accordo con le leggi locali.	3. Risposta
Aspetti legali e di investigazione criminale	9. Avere leggi adeguate nella forma e nella sostanza e personale adeguatamente formato per consentire agli Stati di investigare e perseguire attacchi ai sistemi informatici critici e coordinare tali attività, quando del caso, con gli altri Stati.	
	6. Assicurare che le norme relative alla disponibilità dei dati tengano in considerazione l'esigenza di proteggere i sistemi informatici critici.	
	7. Facilitare il tracciamento degli attacchi ai sistemi informatici critici e, quando appropriato, la comunicazione delle informazioni relative a tali tracciamenti agli altri Stati.	
Considerazioni sociali e politiche		2. Responsabilità
		4. Etica
		5. Democrazia

Tabella 3-1 - Confronto tra il documento OCSE e la Risoluzione delle Nazioni Unite

Molto interessante anche la Comunicazione della Commissione al Parlamento Europeo, al Consiglio, al Comitato economico e sociale e al Comitato delle Regioni del giugno 2001 intitolata ***"Sicurezza delle reti e sicurezza dell'informazione: proposte di un approccio strategico europeo"***.

In questo documento si passano in rassegna le diverse minacce e attacchi (conosciuti all'epoca, oggi occorrerebbe aggiungerne qualcuno) che possono riguardare le reti e i conseguenti rimedi. Si tratta di un utile documento di pianificazione della sicurezza, di cui si è tenuto conto anche nella stesura dei paragrafi successivi di questa sezione.

Il 12 luglio 2002 veniva emanata la ***"Direttiva 2002/58/CE relativa al trattamento dei dati personali e alla tutela della vita privata nel settore delle comunicazioni elettroniche"***. Questa norma, che sostituisce integralmente la precedente direttiva 97/66/CE, riflette le esigenze di aggiornamento intervenute a seguito dell'evoluzione, in un quinquennio, delle tecnologie e, di conseguenza, dei maggiori rischi di violazione della privacy a carico degli utenti. La norma introduce, tra l'altro, i termini di **rete e servizio di comunicazioni elettroniche** conseguenti alla convergenza tra i servizi di fonia e dati.

La direttiva in questione è stata ampiamente recepita, assumendo efficacia cogente per il territorio italiano, nel ***"Decreto legislativo 30 giugno 2003, n. 196 - Codice in materia di protezione dei dati personali"***, di cui al paragrafo successivo che commenta le leggi italiane.

3.1.4 Leggi dello Stato Italiano e norme correlate

Veniamo ora a considerare le fonti legislative nazionali.

L'atto inaugurale dell'attenzione del legislatore italiano in materia di scenari teleinformatici è costituito dalla Legge 23 dicembre 1993, n. 547 ***"Modificazioni e integrazioni alle norme del codice penale e del codice di procedura penale in tema di criminalità informatica"***. Con tale norma veniva inserita la fattispecie del crimine informatico, fino a quel momento non prevista dal nostro ordinamento. La

norma, nel suo contesto, introduceva anche il principio secondo cui il crimine di intrusione indebita in un sistema si intendeva effettivamente consumato soltanto nell'ipotesi in cui il sistema violato fosse protetto da misure di sicurezza. A titolo di cronaca, la norma introduceva anche, per la prima volta, il concetto di documento informatico.

Nel 1996 vedeva la luce la prima norma sulla privacy, la Legge n. 675/96 ***"Tutela delle persone e di altri soggetti rispetto al trattamento dei dati personali"***. Tale norma introduceva per prima l'obbligatorietà di misure di protezione per i sistemi e le reti coinvolte nel trattamento dei dati personali. La specifica effettiva di tale base minima di protezione veniva emanata con apposito regolamento il 28.7.1999. Le due norme sono state integralmente riassorbite, ampliate e rielaborate nel recente Decreto legislativo 30 giugno 2003, n. 196, di cui si dirà in seguito.

Con la Legge n. 59 del 15 marzo 1997, art. 15, viene istituita la Rete Unitaria della Pubblica Amministrazione. Tale realizzazione rappresenta un esempio di eccellenza per le reti italiane in generale e, in particolare, per l'aspetto della sicurezza.

Nel 2001 veniva emanato il D. lgs. n. 231/2001 - ***"Disciplina della responsabilità amministrativa delle persone giuridiche, delle società e delle associazioni anche prive di personalità giuridica, a norma dell'articolo 11 della legge 29 settembre 2000, n. 300"***, da citare, ai nostri fini, per alcuni riferimenti che il testo riporta alla Legge 547/93, di cui in apertura del paragrafo.

La norma si applica a tutte le persone giuridiche e alle società e associazioni anche prive di personalità giuridica, ad esclusione dello Stato, degli enti pubblici territoriali, degli altri enti pubblici non economici, nonché agli enti che svolgono funzioni di rilievo costituzionale.

Tale decreto introduce nell'ordinamento italiano il concetto di responsabilità delle società nei casi in cui persone fisiche commettano dei reati anche nell'interesse o a vantaggio della società stessa. Per quanto ricade nell'ambito di questo documento, l'articolo 24 della norma richiama espressamente tale responsabilità in caso di frode informatica in danno dello Stato o di un ente pubblico.

In tema di adempimenti, la disciplina in oggetto non definisce

specifiche tecniche, ma individua piuttosto principi generali: la responsabilità della società per i reati commessi dai propri dipendenti è esclusa nel caso in cui la società stessa abbia adottato prima della commissione del reato un modello di organizzazione, gestione e controllo idoneo a prevenire reati della specie di quello verificatosi. Se ne deduce un obbligo da parte della società di dotarsi di un sistema di controllo atto a prevenire le possibilità di operare frodi informatiche attraverso l'utilizzo dei propri sistemi e delle proprie reti.

Sotto la pressione di una crescente esigenza di certificazione di sicurezza per i sistemi informatici l'11 aprile 2002 veniva emanato il DPCM ***"Schema nazionale per la valutazione e la certificazione della sicurezza delle tecnologie dell'informazione, ai fini della tutela delle informazioni classificate, concernenti la sicurezza interna ed esterna dello Stato"*** che provvedeva ad aggiornare ed ampliare il quadro normativo in materia di certificazione di sicurezza del trattamento delle informazioni nell'ambito del segreto di Stato: l'estensione ai soggetti privati sarebbe seguita, come si vedrà, l'anno successivo.

Infatti, con il DPCM del 30 ottobre 2003 (G. U. n.98 del 27 aprile 2004), approntato dal Ministro per l'Innovazione e le Tecnologie di concerto con i Ministri delle Comunicazioni, delle Attività Produttive e dell'Economia e delle Finanze, è stato istituito lo Schema Nazionale per la valutazione e certificazione della sicurezza di sistemi e prodotti nel settore della tecnologia dell'informazione. Lo Schema Nazionale definisce l'insieme delle procedure e delle regole nazionali necessarie per la valutazione e la certificazione di sistemi e prodotti ICT, in conformità ai criteri europei ITSEC e alla relativa metodologia applicativa ITSEM o agli standard internazionali ISO/IEC IS-15408 (Common Criteria). Nell'ambito dello Schema Nazionale di valutazione e certificazione è stato istituito l'Organismo di Certificazione della Sicurezza Informatica (O.C.S.I.), che ha il compito principale di gestire lo Schema Nazionale. L'Istituto Superiore delle Comunicazioni e delle Tecnologie dell'Informazione (ISCTI) del Ministero delle Comunicazioni è l'Organismo di Certificazione della Sicurezza Informatica (O.C.S.I.) nel settore della tecnologia dell'informazione. L'OCSI è nel pieno delle sue funzionalità a partire dal 17 febbraio 2005, data di emanazione del Decreto del Ministro per l'innovazione e

le tecnologie e del Ministro delle comunicazioni, recante le "Linee guida provvisorie per l'applicazione dello schema nazionale per la valutazione e certificazione di sicurezza nel settore della tecnologia dell'informazione".

Su di un versante diverso ma complementare, potremmo dire **di contenuti** anziché **d'infrastruttura**, veniva emanato il 9 aprile 2003 il ***Decreto legislativo, n. 68 - "Attuazione della direttiva 2001/29/CE sull'armonizzazione di taluni aspetti del diritto d'autore e dei diritti connessi nella società dell'informazione"***.

Le nuove norme prevedono, tra l'altro, l'estensione delle sanzioni per illeciti prima non previsti, quali l'elusione delle misure tecnologiche per la protezione dei dati e la loro diffusione on-line (art.23).

Il 29 luglio del 2003 veniva pubblicato sulla Gazzetta Ufficiale quella che costituisce, nel panorama complessivo della normativa presentata in questo capitolo, la sola fonte che prescrive misure concrete di sicurezza organizzative, logiche e fisiche, per la protezione delle reti e dei sistemi in ambito privato. Si tratta del ***Decreto legislativo 30 giugno 2003, n. 196 - "Codice in materia di protezione dei dati personali"***, che riassorbe, integra e amplia tutta la normativa italiana precedente, attuando le direttive europee nel frattempo emanate.

Tale norma, infatti, pur riferendosi ai cosiddetti dati personali e a fattispecie particolari di questi, di fatto costituisce l'unica fonte che obbliga enti ed aziende private alla realizzazione di un profilo di protezione consistente. Ciò prescindendo da quanto in ambito privato, soprattutto da parte delle maggiori aziende, non sia stato già autonomamente realizzato.

Il Decreto è fortemente orientato alle reti, integrando nei due concetti di **rete** e **servizio di comunicazioni elettroniche** ambedue gli aspetti di fonia e dati, in un'ottica di neutralità tecnologica che consente di applicare le disposizioni a tecnologie analogiche, digitali e wireless. Esso recepisce e attua la direttiva europea 2002/58/CE (**direttiva privacy nelle comunicazioni elettroniche**) che fa parte di un fondamentale gruppo di cinque direttive (**pacchetto del 2000**), citate in Allegato 1 che, nel loro insieme, regolamentano, nei diversi aspetti, le reti e i servizi di comunicazione elettronica.

L'attuazione della norma propone alle aziende, soprattutto alle medie e alle piccole entità, un'occasione senza precedenti per affrontare il tema della protezione teleinformatica in modo completo, data la poca convenienza, salvo situazioni particolari, di operare profili di protezione separati per dati personali e non (la protezione si progetta e si realizza più facilmente se la si orienta all'infrastruttura teleinformatica nel suo insieme).

La legge prevede le seguenti funzionalità di sicurezza (Art. 34):

- autenticazione degli utenti
- adozione di procedure di gestione delle credenziali di autenticazione
- utilizzazione di un sistema di autorizzazione
- aggiornamento periodico dell'individuazione dell'ambito del trattamento consentito ai singoli incaricati e addetti alla gestione o alla manutenzione degli strumenti elettronici
- protezione degli strumenti elettronici e dei dati rispetto a trattamenti illeciti, ad accessi non consentiti e a determinati programmi informatici
- adozione di procedure per la custodia di copie di sicurezza e il ripristino della disponibilità dei dati e dei sistemi
- tenuta di un aggiornato documento programmatico sulla sicurezza
- adozione di tecniche di cifratura o di codici identificativi per determinati trattamenti di dati idonei a rivelare lo stato di salute o la vita sessuale effettuati da organismi sanitari.

L'adozione delle misure di sicurezza sopra indicate riguarda, in parte, la generalità dei dati personali, in alcuni casi solo particolari tipologie o situazioni (dati sensibili, dati giudiziari). In alcuni casi, la robustezza dei meccanismi adottati è graduata in funzione della criticità delle informazioni trattate.

Oltre a quanto sopra, la norma prevede specificatamente per il settore delle **Comunicazioni elettroniche**, distribuiti in vari articoli e

segnatamente al Titolo X della Parte II, vari adempimenti riferibili a misure organizzative di sicurezza.

Al fine di estendere al settore privato la possibilità di effettuare certificazioni di sicurezza di prodotti e sistemi in un'ottica ITSEC e Common Criteria il 30 ottobre 2003 veniva emanato il DPCM **"Definizione di uno Schema nazionale per la valutazione e certificazione della sicurezza di sistemi e prodotti nel settore della tecnologia dell'informazione"**.

Questa norma conferisce all'Istituto Superiore delle Comunicazioni e delle Tecnologie dell'Informazione (organo del Ministero delle Comunicazioni), la gestione dello schema di certificazione ITSEC e Common Criteria per l'ambito privato. In tal modo, appena l'Istituto avrà concluso l'iter per ottenere il mutuo riconoscimento con gli altri Paesi che da tempo hanno attuato i predetti schemi di certificazione, si colmerà una lacuna che costringe i costruttori italiani a rivolgersi all'estero per ottenere tali certificazioni.

3.1.5 Documenti ministeriali, AIPA, CNIPA

I documenti che seguono costituiscono fonti autorevoli di prescrizione (è il caso della DPCM che segue) e d'indirizzo normativo-operativo.

Il 16 gennaio 2002 la Presidenza del Consiglio dei Ministri-Dipartimento per l'Innovazione e le Tecnologie emanava l'importante Direttiva ***"Sicurezza Informatica e delle Telecomunicazioni nelle Pubbliche Amministrazioni Statali"***.

La disposizione affronta due aspetti: il censimento dell'infrastruttura di sicurezza esistente all'interno delle Pubbliche Amministrazioni (attuata tramite un questionario allegato) e la prescrizione, sempre rivolta alle PA, di adeguarsi a un profilo **minimo** di protezione, notevolmente articolato e dettagliato, indicato anch'esso in un apposito allegato.

La norma, tra l'altro, annunciava l'istituzione, nell'ambito di un'iniziativa congiunta con il Ministero delle Comunicazioni, di un Comitato Tecnico Nazionale sulla Sicurezza Informatica e delle Telecomunicazioni nelle Pubbliche Amministrazioni, istituito nei mesi

successivi.

Il comitato in questione ha prodotto nel marzo del 2004, in linea con la propria missione, un documento intitolato ***"Proposte in materia di sicurezza informatica e delle telecomunicazioni per la pubblica amministrazione"***.

Il documento, dopo un iniziale quadro storico della normativa in materia di sicurezza informatica vigente per le PPAA, propone nella Parte I un modello per un sistema di governo della sicurezza ICT nella PA, basato sulla istituzione di un Centro Nazionale per la Sicurezza Informatica (CNSI) con funzioni di prevenzione, rilevamento, reazione e indirizzo.

Si propone la realizzazione di un CSIRT (Computer Security Incident Response Team), oggi in corso di realizzazione presso il CNIPA, e si sottolinea l'importanza dell'attività di analisi del rischio, della formazione del personale specialistico e utente e dell'istituto della certificazione di sicurezza.

Nella Parte II si riesamina, in termini maggiormente operativi, l'aspetto dell'analisi dei rischi, definendo i criteri di conformità di una eventuale metodologia da standardizzare presso le PPAA e si conclude con un esame del processo di Business Continuity e di Disaster Recovery.

Nel maggio 2004 il CNIPA ha pubblicato il documento *"Linee guida per l'utilizzo della firma digitale"*, con il fine di supportare gli utenti e le aziende circa l'utilizzo della firma digitale. Il documento, molto interessante e concretamente utile all'utente (cittadino, azienda, PA), fa il punto circa la normativa esistente (firma forte, debole) e su come ottenere ed operare i kit per la firma digitale.

3.2 I SOGGETTI E L'ADEMPIMENTO DELLE NORME

3.2.1 Generalità

L'ampia produzione di documenti legislativi e di orientamento in materia di protezione delle reti, di cui si è cercato di dare una lista sintetica ma, per quanto possibile, completa nella prima parte di questo capitolo, copre esurientemente la sfera pubblica mentre lascia spazio per riflessioni e miglioramenti nell'ambito delle utenze private, che potrebbero beneficiare dell'esperienza maturata nell'ambito della P.A. al riguardo.

Infatti gli obblighi la cui mancata ottemperanza comporta sanzioni sono sostanzialmente limitati al disposto del D. lgs. 196/2003 (artt. 33-36) che tuttavia è orientato a una tipologia specifica d'informazioni, anziché ad una visione infrastrutturale.

La Legge 547/93, dal proprio canto, ha il merito di istituire il reato informatico, senza tuttavia prospettare misure obbligatorie preventive, ma solo quelle necessarie per giustificare l'ipotesi di reato e la natura effettivamente criminosa di azioni intrusive.

3.2.2 Le principali responsabilità a carico dei soggetti: diritti, doveri ed adempimenti

Gestori di rete di comunicazione elettronica

Sia il Codice della Privacy (D. lgs. 196/2003) che il Codice delle Comunicazioni Elettroniche (D. lgs. 259/2003) presentano una comune definizione **di rete di comunicazioni elettroniche**: *"i sistemi di trasmissione e, se del caso, le apparecchiature di commutazione o di instradamento e altre risorse che consentono di trasmettere segnali via cavo, via radio, a mezzo di fibre ottiche o con altri mezzi elettromagnetici, comprese le reti satellitari, le reti terrestri mobili e fisse, a commutazione di circuito e a commutazione di pacchetto, compresa Internet, le reti utilizzate per la diffusione circolare dei programmi sonori e televisivi, i sistemi per il trasporto della corrente elettrica, nella misura in cui siano utilizzati per trasmettere i segnali, le reti televisive via cavo, indipendentemente dal tipo di informazione trasportato."*

I soggetti che gestiscono tali reti, come si vedrà non facilmente distinguibili dalla categoria dei gestori di servizi di comunicazione elettronica, hanno, in sintesi, oltre a quelli previsti dagli artt. 33-36 del Codice della Privacy, per il disposto degli artt. 121-133 della stessa norma, i seguenti doveri:

(a) divieto di accesso alle informazioni contenute nei terminali degli abbonati e utenti

(b) limitazioni temporali drastiche per la memorizzazione nei propri archivi dei messaggi trasmessi

(c) limitazioni temporali per la memorizzazione dei dati di traffico per la fatturazione o esigenze giudiziarie

(d) obblighi di trasparenza e chiarezza per gli abbonati per quanto concerne i dati di traffico

(e) disponibilità e flessibilità del servizio di identificazione della linea chiamante

(f) limitazioni e garanzie circa l'utilizzo dei dati relativi all'ubicazione dell'utente

(g) disponibilità del servizio di blocco del trasferimento di chiamata

(h) garanzie e limitazioni circa l'inserimento dei nominativi negli elenchi degli abbonati

(i) limitazione dell'attività di spamming nei confronti del soggetto emittente (nessun controllo è previsto a carico del gestore della rete di comunicazione elettronica)

(j) auspicio per la realizzazione di codici di deontologia e di buona condotta.

È interessante osservare che, tra i punti sopra indicati, sono previste sanzioni solo per i punti (a) (peraltro dalla Legge 547/1993), (b), (f), (h), e (i).

Come si può ancora una volta notare, la norma tende ad obbligare i soggetti a tenere determinati comportamenti specifici, piuttosto che a proporre misure di sicurezza infrastrutturali, indipendenti dalla tipologia dei dati trattati e trasmessi.

Gestori di servizi di comunicazione elettronica

Il Codice della privacy all'art. 4 definisce i servizi di comunicazione elettronica come segue: *"ogni informazione scambiata o trasmessa tra un numero finito di soggetti tramite un servizio di comunicazione elettronica accessibile al pubblico"* con l'esclusione del servizio di radiodiffusione.

La categoria dei gestori di tali servizi, come si può intuire, è difficilmente distinguibile da quella precedente, stante la forte integrazione funzionale e operativa della componente rete e della componente servizi. È ragionevole ipotizzare, di conseguenza, che tutti gli obblighi descritti nel precedente paragrafo siano in toto riferibili anche a questa categoria.

Utenti aziende

Le aziende sono obbligate ad attuare misure minime di sicurezza per il disposto degli artt. 33-36 del Codice della Privacy e quindi esclusivamente in relazione al possesso e al trattamento di dati soggetti alla norma. Le Legge 547/1993, d'altra parte, non obbliga, ma semplicemente prevede la necessità di **adeguate misure di sicurezza** perché il reato di indebita intrusione sia ravvisabile e perseguibile.

Anche in questo caso si può affermare che l'approccio **strutturale** è inesistente, almeno per quanto riguarda l'obbligatorietà.

Di fatto, almeno le maggiori aziende e organizzazioni sullo scenario italiano hanno predisposto misure di sicurezza infrastrutturali di una certa portata. Ciò non di meno, negli ultimi anni non sono mancati casi clamorosi rivelatori di ampie falle al riguardo.

La carenza maggiore che sembra potersi rilevare non è tanto connessa all'acquisto di componenti hardware e software per la protezione, quanto piuttosto alle risorse umane dedicate alla gestione e all'ottimizzazione di tali componenti (struttura organizzativa). La consapevolezza che una gran parte dell'efficacia delle misure di protezione hardware e software installate dipende da una corretta e quotidiana gestione di tipo organizzativo legata a persone adeguatamente professionalizzate non è ancora affermata nei responsabili dell'azienda e dei budget.

Utenti privati

La pericolosità per la collettività della impreparazione in materia di sicurezza da parte degli utenti privati appare sottostimata. L'universo degli utenti privati, ormai massicciamente connesso in rete spesso in modalità **always on** stante il rapido diffondersi delle connessioni ad alta velocità, non rientra neanche nell'ambito dell'applicazione della normativa privacy la quale, come si è visto, è l'unica che pone qualche obbligo, seppure in un ambito di tipologia di dati peculiare.

La responsabilità degli utenti privati nella diffusione (in genere inconsapevole) dei virus è l'aspetto più rilevante da osservare: tuttavia non è l'unico. La maggior parte dei computer **personali** contiene, oltre alle informazioni del proprietario, anche dati relativi a corrispondenti e affini. Inoltre, un personal computer in rete non protetto si presta facilmente come **sponda** per attacchi nei confronti di terzi.

3.2.3 Il rapporto con l'autorità giudiziaria e investigativa

Il rapporto con l'autorità giudiziaria

L'autorità giudiziaria, per le proprie esigenze investigative, si giova soprattutto della collaborazione dei gestori delle reti e dei servizi. La collaborazione, efficace e normalmente fruttuosa ai fini delle esigenze della Giustizia, è prevista dalla legge e le aziende percepiscono un compenso per tale attività.

A tal fine, le aziende hanno realizzato un apparato tecnico-organizzativo di una certa complessità a dimostrazione del fatto che, se esistono le opportune motivazioni, anche le aziende divengono sensibili alle esigenze organizzative della sicurezza.

Il rapporto con l'autorità investigativa

Molto spesso da parte dei responsabili delle aziende che subiscono un crimine informatico si registra un atteggiamento di scetticismo nei confronti della reale possibilità di intervento delle forze di Polizia nei reati ad alta presenza di tecnologia. A ciò si aggiunge generalmente una scarsa propensione delle imprese a denunciare i crimini

informatici subiti per evitare la pubblicità negativa che potrebbe derivarne.

Le strutture italiane hanno acquisito una notevole efficienza ed affidabilità mostrando un grande impegno nell'aggiornamento tecnico-professionale, attuato anche attingendo da know-how esterni all'istituzione. Gli interventi investigativi vengono ora attuati con modalità poco **intrusive** e generalmente senza provocare alcun rallentamento alle normali attività gestionali e produttive dell'azienda. Ovviamente tali qualità investigative possono essere evidenziate e sfruttate dai cittadini solo quando questi reparti specialistici vengono coinvolti, attraverso la denuncia, o semplicemente chiedendo un consiglio per cercare di prevenire possibili crimini.

La Polizia Postale e delle Comunicazioni fornisce le seguenti indicazioni di comportamento da parte dei soggetti che rilevino abusi effettivi o sospetti:

- ad ogni sospetto di abuso chiamare[1] immediatamente una forza di polizia specializzata. È necessario agevolare l'intervento degli investigatori informatici, chiamati dall'azienda, aiutandoli a realizzare un'indagine preliminare interna che tende in primo luogo ad accertare l'effettiva presenza di un crimine
- non prendere iniziative prima dell'arrivo degli investigatori per ridurre al minimo i rischi di cancellazione/contaminazione accidentale delle prove
- predisporre un team di supporto all'investigazione composto da personale altamente fidato. È necessario aiutare l'investigatore ad individuare gli elementi costitutivi del crimine in questione, onde poter delineare la fattispecie delittuosa presente
- ridurre al minimo i rischi di ulteriori perdite ma contemporaneamente cercare di acquisire elementi utili per la scoperta del colpevole. Queste due attività sono spesso in antagonismo

[1] *Per l'elenco delle sezioni territoriali della Polizia delle Comunicazioni si veda l'omonima voce al sito www.poliziadistato .it .*

logico tra loro essendo il sistema migliore per interrompere un attacco quello di spegnere il sistema e procedere al ricaricamento delle copie di sistema pulite e dei programmi applicativi. Tuttavia, tale operazione nella maggior parte dei casi riduce le possibilità di identificazione dell'intruso

- mantenere un'assoluta riservatezza sull'indagine. Le strutture aziendali dovrebbero collaborare con gli organi investigativi ma le informazioni sull'investigazione in atto dovrebbero essere trasmesse al minor numero di persone possibili per limitare una fuga di notizie all'interno e all'esterno dell'organizzazione. Tali informazioni andrebbero quindi fornite solamente a chi ne debba per forza venire a conoscenza
- tutte le comunicazioni (quelle indispensabili) collegate all'indagine in corso dovrebbero essere effettuate non utilizzando i sistemi informatici (e-mail, intranet ecc.) al fine di evitare qualsivoglia intercettazione da parte dell'insider o dell'intruso
- in caso di sospetti su possibili autori **insider**, né l'investigatore né tanto meno gli impiegati della società dovrebbero affrontare o parlare con tali sospetti per non dar loro modo di nascondere o cancellare le prove.

3.3 FATTISPECIE DI VIOLAZIONE DELLE NORME

3.3.1 Reati informatici

Il termine reato informatico ha assunto, nel corso degli anni, un significato molto, forse troppo ampio: viene infatti oggi comunemente definito come tale ogni reato condotto con l'ausilio di mezzi informatici e, quindi, delle reti.

È chiaro che un'accezione così ampia del termine mal si presta ad individuare soluzioni e a redigere norme. Se infatti appare legittima la definizione di reato informatico nel caso di una introduzione non autorizzata in un sistema altrui, meno accettabile risulta tale definizione per una frode commerciale o un reato di pedofilia condotta con l'ausilio delle reti. Sarebbe come classificare reato ai sensi del Codice

della Strada un furto perpetrato con l'ausilio di un'automobile.

Vale la pena ancora una volta rilevare come questa accezione per così dire **estesa** del termine coincida con una visione non strutturale del sistema **rete**, quanto piuttosto con una visione di contenuti e comportamenti supportati dalla rete stessa.

Ai nostri fini e, augurabilmente, più in generale, anche in linea con la sostanza della Legge 547/1993 che in definitiva istituisce tale tipologia di reato, il reato informatico è quello che arreca danno a un sistema informatico **in toto** o a un suo componente (ivi compresi i dati gestiti). Per le persone fisiche e giuridiche, i reati informatici, nell'accezione ristretta sopra illustrata, sono di fatto quelli previsti dalla citata Legge 547/1993, che stabilisce anche le condizioni per cui tali reati sono perseguibili.

3.3.2 Inadempienze dei soggetti

Ad oggi, le inadempienze possibili da parte di persone giuridiche (aziende) quanto a omissione di protezione delle reti, si limitano alla violazione dei disposti del D. lgs. 196/2003. Le sanzioni relative sono indicate nell'art. 169 della norma. Nessuna inadempienza possibile sembra ravvisabile allo stato attuale da parte di persone fisiche.

3.4 I PRINCIPALI REQUISITI DEI CONTRATTI DI OUTSOURCING

Oggigiorno le imprese devono adattarsi rapidamente alle continue sollecitazioni che ricevono dallo specifico contesto competitivo in cui operano e adottano un ciclo di vita dei prodotti/servizi sempre più rapido; basti riflettere sul fatto che in passato un modello di automobile, quale la Ford **"T"**, poteva essere venduto con piccole modifiche per 30 anni mentre oggi un modello di automobile ha una vita massima di 2-3 anni prima di un forte restiling o del definitivo abbandono. Tale costante adattamento alle mutevoli esigenze dei propri clienti determina un costante adeguamento delle attività aziendali necessarie alla produzione del bene o del servizio. Le imprese operano

in una situazione di costante cambiamento che deve essere governato pena la sopravvivenza dell'impresa stessa.

In questo contesto competitivo le aziende hanno riprogettato il loro funzionamento concentrando la loro attenzione non più sulle strutture e gli organigrammi ma sui processi, ovvero *sull'insieme delle attività strutturate e misurate, progettato per produrre uno specifico output per un mercato o un cliente particolari* [2]. Si riclassificano le attività sulla base della specifica **Catena del Valore**[3] dell'impresa, si progettano le leve di miglioramento per ciascun processo individuato ovvero le tecnologie ed i ruoli necessari al loro funzionamento. Si pianificano e si effettuano le varie tipologie di investimento necessarie alla transizione dallo stato attuale a quello desiderato.

Nella maggior parte dei processi le leve principali di tale ridefinizione dell'impresa sono costituite dalle tecnologie dell'informazione che costituiscono il **sistema nervoso** dei nuovi modelli aziendali. La flessibilità e la specializzazione diventano i cardini su cui progettare un'organizzazione aziendale che, spesso, vede coinvolti fornitori e clienti nella propria Catena del Valore che diviene così interaziendale. Ciò avviene mediante l'esternalizzazione (outsourcing) di componenti aziendali che a volte condizionano il funzionamento dell'intera azienda. È il caso dell'esternalizzazione (o delega all'esterno) di servizi aziendali preposti alla gestione delle tecnologie dell'informazione e delle comunicazioni (ICT Outsourcing).

Il crescente ricorso alla pratica di terziarizzazione dei processi aziendali pone all'azienda problemi non trascurabili, quanto alla sicurezza delle informazioni trattate, sia sul piano delle strategie di protezione da adottare, sia sul piano di ottemperare alla normativa vigente, in particolare al Codice della privacy.

Un contratto di **Information and Communication Technology Outsourcing** può essere totale (full outsourcing) oppu-

---

[2] *Davemport, T.H. "Innovazione dei processi", Franco Angeli, Milano, 1994, p.25.*

[3] *Porter, M.E. "Competitive Advantage", Free Press, New York, 1985, tr.it. "Il Vantaggio Competitivo", Edizioni Comunità.*

re selettivo (selective outsourcing). In entrambe le tipologie è essenziale specificare i requisiti ed i criteri relativi alla gestione delle tematiche di sicurezza e di riservatezza, delle informazioni e delle immobilizzazioni tecniche, trasferite all'outsourcer caratterizzandoli con puntuali livelli di servizio coerenti con le **politiche di sicurezza** dell'impresa committente.

Occorre quindi che per ogni servizio di gestione della sicurezza trasferito siano stabiliti, garantendo comunque la necessaria flessibilità al contratto, precisi obblighi delle due parti. Le tipologie di servizi di gestione della sicurezza, che saranno nel seguito trattate in dettaglio, possono riassumersi in:

- Identity and Access Management (riguarda i processi operativi di gestione degli utenti abilitati ad accedere ai vari servizi ICT consentiti dall'infrastruttura)
- Secure Content Management (riguarda i processi operativi che consentono di prevenire lo **spam** nei servizi di e-mail, di ispezionare e filtrare il contenuto e di proteggere dai virus informatici i messaggi scambiati con l'esterno)
- Security Monitoring and Management
- Physical Security Management
- Secure Communication Services (identificano quei processi e tools necessari a individuare false identità, tentativi di accesso a messaggi riservati, riutilizzo non autorizzato di messaggi trasmessi, falsificazione del mittente o dell'origine, modifica del contenuto, mancata consegna di un messaggio)
- Auditing and Reporting
- Compliance Management Services (verifica della aderenza ai requisiti richiesti)
- Security Training.

Nei più recenti contratti di ICT outsourcing i livelli di servizio associati a ciascuno dei servizi elencati sono misurati con modalità che tengono conto non solo della singola componente o dello specifico

aspetto processuale ma, soprattutto, della percezione dell'utente finale in termini di funzionalità ed ergonomicità.

Si osserva, in generale, una scarsa attenzione da parte delle aziende committenti, che esternalizzano il processo, a curare, nei documenti contrattuali, una sezione che specifichi i criteri minimi di sicurezza da adottare, ivi compreso un aspetto di verifica e controllo.

3.5 AREE DI POSSIBILE INTEGRAZIONE NORMATIVA

Come si è potuto considerare nei precedenti paragrafi, il **corpus normativo** oggi esistente, per quanto riguarda l'ambito della PA, appare da qualche anno in fase di progressivo adeguamento sotto il profilo delle esigenze di sicurezza, conseguendo un ulteriore importante consolidamento con l'avvenuta approvazione, recente, del Decreto legislativo di attuazione del Sistema Pubblico di Connettività. La stessa cosa non può dirsi per quanto riguarda l'ambito privato (aziende e utenze personali) dove le normative cogenti sono oggi sostanzialmente orientate a fattispecie specifiche d'informazioni trattate (D. lgs. 196/2003) ed ad alcuni comportamenti (L. 547/93). Mancano disposizioni regolamentari preventive orientate alla infrastruttura di rete.

Tali disposizioni dovrebbero essere emanate nei confronti sia di chi realizza le reti, di chi le gestisce e di chi le utilizza, secondo un criterio di competenza funzionale (ruolo) e di rilievo economico (utenti), senza tuttavia escludere nessuno: ciò in relazione alla topologia **totalmente connessa** che caratterizza il sistema **reti**.

In sostanza se per la Pubblica Amministrazione, con l'emanazione del Decreto legislativo sul Sistema Pubblico di Connettività, diventa obbligatorio utilizzare provider che rispettino regole atte a garantire la sicurezza nelle transazioni informatiche è auspicabile che queste stesse regole opportunamente adattate possano costituire la base per un **codice etico** da rispettare da parte di tutti i soggetti abilitati a fornire i servizi di trasmissione dati. Tale condizione costituirebbe un significativo elemento di garanzia per tutti i soggetti fruitori siano essi i cittadini, le aziende od i soggetti privati in genere.

3.6 CONCLUSIONI

L'attuazione sistematica ed efficiente di un adeguato livello di protezione per le reti dati (intese nei loro diversi componenti) dipende da una serie di fattori, non solo normativi e legali, che cerchiamo di seguito d'individuare, per successivamente esaminare, per alcuni di essi, in modo maggiormente approfondito, eventuali spazi e margini di miglioramento del quadro complessivo e dell'aspetto normativo in particolare.

Tali fattori sono anzitutto il grado di consapevolezza e di iniziativa da parte degli utenti; in secondo luogo, il programma di sensibilizzazione eventualmente predisposto da parte di enti governativi ed infine il quadro normativo e l'eventuale struttura a supporto e le metodologie, eventualmente condivise e standardizzate.

È opportuno notare come questo insieme di componenti, oltre ad una prima vista a livello nazionale, trovi riscontro in un corrispondente quadro europeo, in corso di istituzione e consolidamento.

3.6.1 Consapevolezza e iniziativa da parte degli utenti

Occorre, per correttezza, premettere che uno studio di sufficiente livello scientifico e consequenziale attendibilità, sia a livello nazionale che europeo, che fotografi il livello di consapevolezza di istituzioni, enti, aziende e privati in materia di protezione delle reti, non è, ad oggi, disponibile.

Tutto quanto è stato pubblicato nel corso degli ultimi anni si basa su generalizzazioni ed estrapolazioni di perimetri settoriali e su valutazioni di tipo indiretto, quali la presenza di addetti al tema della sicurezza nelle aziende, denunce di virus e di attacchi di vario tipo, indagini telefoniche, condotte su campioni spesso non significativi.

Le presenti note non presentano credenziali maggiori, pur basandosi sull'esperienza delle aziende che hanno partecipato alla reda-

zione del documento e che hanno dalla loro l'operatività concreta quotidiana sul mercato.

A riprova di quanto affermato, l'UE ha recentemente avvertito l'esigenza di pianificare, nel corso dei prossimi mesi, un'indagine conoscitiva presso tutti i paesi membri intesa ad accertare il grado di consapevolezza, da parte delle aziende e delle organizzazioni, dell'importanza della sicurezza delle reti con particolare riferimento agli aspetti della gestione del rischio e della continuità delle operazioni. Giova peraltro rilevare che tale indagine si limita al settore delle aziende private, escludendo la pubblica amministrazione.

L'impressione è che il grado di consistenza del binomio consapevolezza-iniziativa, da parte di tutti, grandi e piccoli protagonisti, sia ad uno stadio iniziale, che necessita di un notevole incremento perché possa generare risultati tangibili ed efficaci.

Tale basso livello di consapevolezza si riflette in una limitata disponibilità a conformarsi alle norme (peraltro, per il settore privato, non molte, come si è visto) attualmente in vigore. Una difficoltà di rilievo consiste nel fatto che la maggior parte dei dirigenti di organismi pubblici e privati sembrano continuare a considerare gli oneri per la sicurezza delle reti come un costo privo di motivazioni e ritorni, sia sul piano funzionale che etico.

Può essere utile, al riguardo, richiamare il parallelismo che esiste tra il tema della protezione delle reti ed altri aspetti concettualmente affini quali la sicurezza stradale e la salute pubblica. Sono temi che, seppure più maturi storicamente e organizzativamente, e soggetti a finanziamenti e iniziative, ancora pongono seri problemi di strategia e di attuazione.

Il danno derivante a una comunità da un'epidemia è oggi comunemente riconosciuto non solo sul piano etico (salvaguardia della vita umana) ma anche sul piano dei costi sociali. Ne deriva un'adeguata attività sia di sensibilizzazione, sia legislativa e sanzionatoria, sia di strutturazione organizzativa a livello politico e amministrativo.

Diversa è la situazione per quanto concerne la sicurezza delle reti, dove esistono ancora, per l'ambito privato, notevoli margini per una maggiore concentrazione degli sforzi da parte delle associazioni di

categoria in sintonia e in analogia con quanto, in ambito pubblico, è in corso di svolgimento da parte degli organi governativi.

3.6.2 Quadro legislativo

Nel corso del presente capitolo si è potuto constatare (si veda il paragrafo 3.1.4) che, in Italia, per quanto concerne l'ambito privato, il quadro normativo che prevede obblighi per la protezione delle reti è esclusivamente costituito da alcuni disposti del D. lgs. 196/2003. Occore al riguardo notare:

- che il D. lgs. 196/2003 riguarda esclusivamente il dominio della privacy e dei cosiddetti dati personali
- che detta norma, di fatto, riguarda sostanzialmente solo le aziende e gli enti, non obbligando i privati
- che gli **utenti privati**, nella loro numerosità e impreparazione, stante l'ormai crescente e presto generalizzato utilizzo di connessioni ad Internet ad alta velocità **always on**, costituiscono, nel sistema totalmente interconnesso in cui oggi viviamo, una elevata criticità.

Non sarebbe fuor di tempo e di luogo ipotizzare un dispositivo legislativo specifico che, comprendendo e sviluppando quanto contenuto negli articoli 31-36 del D. lgs. 196/2003, ne estendesse la competenza oltre lo specifico dominio dei dati personali e prevedesse:

- misure minime di sicurezza a orientamento infrastrutturale piuttosto che in relazione a specifiche criticità dei dati (tale aspetto può essere considerato condizione per un livello incrementale di protezione)
- misure minime di sicurezza per diversi livelli di utenza quali privati, connectivity e application provider, aziende, enti, PA ecc.

D'altra parte il Decreto legislativo che ha formalizzato l'istitu-

zione del Sistema Pubblico di Connettività potrebbe costituire una valida fonte di criteri e misure di sicurezza da applicare alle reti anche per quanto riguarda l'utenza privata ivi includendo sia le aziende e le organizzazioni che le singole persone.

In ambito aziendale, la prassi di una certificazione di sicurezza ICT va rapidamente guadagnando terreno e fautori. Al riguardo, la norma generalmente adottata è lo standard BS 7799, convertito per la sola parte 1 in norma ISO /IEC 17799:2000.

4 - L'analisi e la gestione del rischio: principi e metodi

4.1 IL SISTEMA DI GESTIONE DELLA SICUREZZA

Prima di iniziare qualsiasi esposizione sull'**analisi e gestione del rischio**, ma anche sulle **misure di protezione delle reti**, è opportuno evidenziare la difficoltà di approntare un **efficace** sistema di protezione senza considerare alcuni presupposti che caratterizzano il **sistema di gestione della sicurezza**.

Ci sono diversi standard e linee guida che descrivono i componenti di un buon sistema di gestione della sicurezza, fra cui:

- i nove principi dell'OCSE (vedi paragrafo 3.1.2)
- lo standard ISO17799/BS7799, particolarmente il documento BS 7799:2000 parte 2
- lo *"Standard of Good Practice"* dell'Information Security Forum (vedi Allegato 2.2).

Questo, ovviamente, oltre a tutti gli altri standard e linee guida che trattano l'argomento in modo meno diretto, fra cui: il COSO Report sull' *"Enterprise Risk Management"*; la metodologia ISACA per l'IT Audit, denominata CobiT; gli standard ITSEC e *"Common Criteria"*, le linee Guida del CNIPA e altri.

Tutte queste **direttive** presentano, fortunatamente, delle **parti comuni** che possiamo sintetizzare, ad alto livello, come segue.

Sensibilizzazione

Tutta l'azienda deve essere adeguatamente sensibilizzata alla necessità di proteggere le proprie risorse iniziando dal top management per proseguire con tutta l'organizzazione e i vari ruoli. Per il raggiungimento dell'obiettivo è necessario conseguire un adeguato livello d'addestramento.

Organizzazione e governo

È necessario definire un modello organizzativo per la sicurezza distribuendo i compiti e le responsabilità. Il governo della sicurezza sarà efficace solo se mantenuto ad alto livello e se include, fra i suoi compiti, quello di definire la strategia, gli obiettivi aziendali specifici e i relativi sistemi di misurazione delle performance.

Analisi dei rischi

Come descritto al paragrafo 4.2, l'analisi dei rischi è fondamentale per acquisire conoscenza delle minacce e delle vulnerabilità che incombono sull'organizzazione e per poter dirigere sforzi e risorse (per definizione limitati) a difesa delle aree più a rischio.

Politiche e procedure

A seguito di un'analisi dei rischi è importante definire le politiche e le relative procedure. Ciò avviene solitamente a tre livelli: **generale**, che descrive l'organizzazione, il sistema di governo, gli obiettivi e i principi; **utenti**, nel quale ambito si regola il comportamento degli utenti nell'uso quotidiano delle tecnologie; **tecnico**, ove il personale ICT viene guidato circa le azioni da intraprendere in fase di implementazione e manutenzione della tecnologia.

Costante monitoraggio e allineamento del sistema di protezione

Il sistema di gestione della sicurezza dovrà essere disegnato in

modo da assicurare un adeguato monitoraggio, operativo e di governo, per permettere all'organizzazione di reagire e allineare l'intero sistema rispetto ai cambiamenti che dovessero verificarsi nell'ambito del dominio dei rischi.

4.2 ANALISI DEI RISCHI

4.2.1 L'importanza dell'analisi dei rischi

È possibile, oggi, affermare che la vita economica e sociale non può più essere separata dalle correlate risorse informative e, quindi, dalle relative reti di comunicazione.

A differenza del mondo fisico, le informazioni e le reti sono soggetti a rischi inerenti di più ampia natura, spesso latenti ed in continua evoluzione. D'altra parte riscontriamo che:

- le reti sono sempre più complesse ed il loro modificarsi genera nuovi rischi
- la protezione **completa** implicherebbe un utilizzo restrittivo e rallentato delle risorse
- la tecnica di protezione è fortemente dipendente dal relativo rischio
- i costi per implementare un livello di sicurezza, che vada oltre il necessario o l'ottimale o che si estenda ad elementi a basso impatto, possono diventare proibitivi per la maggior parte delle organizzazioni.

Di conseguenza è importante effettuare un'analisi dei rischi ai fini di:

- definire quali siano le minacce informatiche che si presentano alle organizzazioni
- valutare l'impatto nel caso in cui le minacce si concretizzino
- definire ed implementare contromisure adeguate a mitigare il rischio con un impegno commensurato ai potenziali impatti.

In definitiva l'analisi dei rischi pone le basi perché si possano scegliere le contromisure senza **provare a indovinare**, e si possano bilanciare tali contromisure rispetto ai rischi e ai costi delle stesse.

Il processo di analisi dei rischi è uno degli elementi fondamentali del Sistema di Gestione della sicurezza. È inoltre richiesta, direttamente o indirettamente, da normative comunitarie e nazionali (vedi capitolo 3), e dai principali standard di riferimento, quali ad esempio:

- Standard ISO 17799 - BS7799
- ISF Standard of Good Practice
- CobiT (*"Control Objectives of IT Governance"* dell' ISACA)
- GMITS (*"Guidelines for the Management of IT Security"*; parte di questa serie di documenti è conosciuto anche come standard ISO 13335).

L'analisi dei rischi informatici assume ulteriore importanza se si considera che essa trova collocazione sempre più rilevante all'interno di contesti più ampi di analisi e gestione dei rischi aziendali, quali i contesti di Corporate Governance e il documento **Basilea II**. Quest'ultimo si rivolge agli organismi bancari-finanziari e prevede un programma di gestione di tutti i rischi di business (dai rischi di credito ai rischi finanziari e di mercato) e operativi, inclusi quelli correlati ai sistemi informativi (information risk).

La sempre crescente importanza assunta dall'analisi dei rischi informatici rispetto al contesto più globale della gestione di tutti i rischi aziendali trova giustificazione nel fatto che l'Information Technology sempre più supporta il business e i relativi processi aziendali.

Di conseguenza il rischio informatico (ossia il rischio derivante da assenza di protezione dei sistemi informatici) influenza e condiziona sempre più le altre categorie di rischi (rischio finanziario, di mercato, rischi operativi, ecc.).

Infine è importante condurre a priori, ciclicamente e in maniera dinamica/continuativa (vedere paragrafo 4.2.3), un'attività di analisi dei rischi che mantenga aggiornato il sistema di protezione in funzione dell'effettiva e reale esigenza riscontrata, consentendo, nel contempo, l'ottimale utilizzo delle risorse disponibili.

4.2.2 Considerazioni generali sulle diverse metodologie di analisi dei rischi

Le metodologie esistenti in merito alla conduzione di un'analisi dei rischi sono molteplici e spesso si presentano con differenti obiettivi o caratteristiche, anche se si basano su alcuni concetti, elementi e passaggi procedurali comuni.

Nessuna è particolarmente migliore dell'altra: è importante comprendere quale tipologia di approccio sia più idoneo utilizzare, considerandone le caratteristiche a livello di:

- approfondimento dell'analisi
- modalità di assegnazione dei valori (sistema di misurazione dei rischi)
- ripetibilità e frequenza del processo di analisi.

Livello di approfondimento

Se si considera il livello di approfondimento con cui si conduce un'analisi dei rischi si può classificare un approccio come **concettuale**, ossia rivolto al management e orientato all'organizzazione e ai processi, oppure **operativo**, ossia rivolto allo specialista o responsabile dei sistemi informatici, e orientato quindi alla singole tecnologie e al contesto, appunto, operativo.

Una valutazione di tipo **concettuale** - ad alto livello - dei rischi consente normalmente di:

- individuare il profilo di rischio a livello strategico e organizzativo
- definire le minacce all'organizzazione e quindi individuare le macro aree di criticità o contesti di rischio su cui intervenire nel tempo
- definire un piano di interventi immediati a livello **enterprise**
- definire la politica generale della sicurezza.

Una valutazione di questo tipo consegue l'importante obiettivo di aumentare la percezione e la consapevolezza (awareness) dei vertici aziendali circa l'importanza di definire ed implementare un piano di gestione della sicurezza. Ottiene inoltre **commitment** a garanzia del piano della sicurezza e, soprattutto, consente di indirizzare l'impegno verso le aree più critiche (ambienti tecnologici, singoli sistemi, rete aziendale) per le quali realizzare un'analisi dei rischi più approfondita.

Un'analisi di tipo **operativo** è più orientata alla valutazione dettagliata e approfondita della sicurezza delle singole tecnologie, sistemi e specifici ambiti di rete e si prefigge normalmente i seguenti macro obiettivi:

- comprensione delle vulnerabilità, minacce e rischi a cui sono esposte le singole tecnologie (singole piattaforme applicative, sistemi, reti, ecc.) e le informazioni trattate
- definizione di architetture e standard tecnologici di sicurezza
- revisione delle policy e procedure di gestione dei sistemi
- proposta di percorsi operativi per la correzione delle debolezze riscontrate, corrispondenti all'assenza di controlli di sicurezza necessari
- ottenimento di conformità rispetto a best practice tecnologiche di sicurezza.

Modalità di assegnazione dei valori

Nello scegliere una metodologia è importante considerare il sistema di misura (metrica) adottato per i diversi elementi considerati dal modello della metodologia stessa, in relazione agli obiettivi prefissati.

Una misurazione di tipo **quantitativo**, che si basa su elementi monetari e statistici, permette di definire un budget d'investimento in modo più immediato, ma può essere complessa da applicare e non riesce interamente ad evitare valutazioni di tipo soggettivo.

Per applicare quest'approccio occorre che tutti gli elementi di rischio siano quantificati (es. costo del ripristino di una risorsa, ma anche danno per perdita d'immagine, ecc.). Per fare questo è necessa-

rio avere accesso ad informazioni d'elevata qualità, difficilmente reperibili.

In realtà in seno a tale tipologia d'approccio esistono due varianti che possiamo definire con l'aggettivazione ulteriore (rispetto a quantitativo) di vero e apparente. La prima riguarda i casi in cui si utilizzi un numero che esprima una quantità reale. È il caso del danno direttamente quantificabile in unità monetaria.

Il secondo caso, che definiamo **quantitativo apparente** ovvero **semiquantitativo**, si verifica allorché ci si trovi nella necessità (per esigenze computazionali spesso legate all'utilizzo di un elaboratore) di convertire in indici numerici misure di carattere qualitativo.

È il caso, ad esempio, di un valore di criticità, espresso inizialmente in termini qualitativi, ad esempio con la quaterna **alto**, **medio**, **basso**, **nullo**, che viene tradotto con una corrispondente quaterna di valori numerici (ad esempio, 3, 2, 1 e 0) per consentire un prodotto logico con un'altra misura (ad esempio, un livello di esposizione al rischio).

L'approccio **quantitativo puro**, che appare certamente più preciso rispetto a quello qualitativo, non è, in generale, di facile applicazione per due motivi.

Il primo è che spesso non sono disponibili i valori (chi può definire, con certezza, il valore di un bene materiale, magari al netto del valore d'ammortamento, che non sia gestito da una procedura contabile al necessario livello analitico, e come regolarsi in caso di danno d'immagine?).

Il secondo è che, mancando una buona base di oggettività per tali valori, si finisce per effettuare stime, spesso lontane dalla verità, conferendo una forma numerica a quella che, in realtà, è di fatto una valutazione qualitativa.

Le metodologie **qualitative** in generale non richiedono dati statistici, presentano una scala di valori generalmente espressa, ad esempio, come **basso**, **medio**, **alto**, **vitale**, **critico**.

Tali approcci, apparentemente più superficiali e meno precisi, in realtà si rivelano spesso più onesti, anche perché, in generale, la filiera logica dei modelli di analisi del rischio conclude il suo percorso con

l'individuazione delle contromisure, che sono definibili, quanto a robustezza, in termini discontinui, rendendo, in tal modo, vano e non indispensabile l'approccio di tipo quantitativo, ammesso che sia in realtà possibile attribuire valori esatti credibili alle diverse entità in gioco.

L'aspetto di maggior rilievo che il progettista si trova a dover fronteggiare in proposito alla metrica è il **bilanciamento**, in termini di escursione, della scala di valori ammessi per i vari concetti e dei diversi sistemi di metrica adottati per essi, siano detti sistemi di carattere qualitativo o quantitativo.

È evidente, infatti, che relazioni e funzioni che implichino concetti misurati secondo scale di valori tra loro poco congruenti, possono portare a risultati poco consistenti.

Determinare un sistema di verifica per la valutazione della congruità e della rispondenza dei diversi sistemi di metrica è uno dei temi aperti della materia trattata. Potremmo, però, concludere che il sistema quantitativo è più indicato per le analisi di tipo concettuale, in contesti di business e quello qualitativo per le analisi di tipo operativo dove è l'efficacia delle contromisure a prevalere sulla giustificazione dei costi.

Ripetibilità e frequenza del processo di analisi

A seconda della **ripetibilità/frequenza del processo di analisi** dei rischi, si possono distinguere le metodologie esistenti fra approcci **statici** e approcci **dinamici/continuativi**.

Gli approcci statici:

- realizzano una fotografia dello stato attuale della sicurezza
- richiedono revisioni periodiche, con scadenze temporali diverse, a seconda del livello di profondità dell'analisi:
  - una volta l'anno nel caso di analisi di tipo concettuale/organizzativo
  - ogni 3-4 mesi nel caso di analisi a livello operativo/tecnologico.
- hanno differenti obiettivi a seconda del livello di profondità dell'analisi:

  - definizione di politiche e infrastruttura organizzativa di gestione della sicurezza, nel caso di analisi di tipo concettuale/organizzativo
  - definizione di architetture e standard tecnologici/controlli di sicurezza a fronte della valutazione delle vulnerabilità e minacce a cui sono esposte le tecnologie (livello di analisi di tipo tecnologico).

- coinvolgono tutte le organizzazioni, di qualsiasi dimensione, in particolar modo nel caso in cui si effettua un primo giro di valutazione del rischio
- normalmente sono gestiti sotto la responsabilità di funzioni aziendali specifiche, in genere in ambito ICT (ICT Manager, Security Officer, Comitato per la Sicurezza, ecc.); quindi le altre funzioni aziendali sono coinvolte passivamente.

Gli approcci dinamici/continuativi:

- non fotografano la situazione della sicurezza in un dato momento, ma danno gli elementi per analizzare e gestire continuamente e dinamicamente il rischio
- la valutazione e gestione dei rischi diventa parte integrante dei processi di implementazione, manutenzione e monitoraggio dei sistemi informativi
- si basano spesso su misure del rischio di tipo quantitativo (attraverso utilizzo di tool come **Balance Scorecard** e di **Key Performance Indicators**)
- integrano la gestione dei rischi informatici all'interno dell'impianto di gestione di tutti i rischi aziendali e, in particolare, delle normali attività operative (implementazione, change management, operatività)
- comportano un decentramento in termini di responsabilità nella gestione dei rischi, con il coinvolgimento di tutte le funzioni aziendali a più livelli, e richiedono un commitment che parte dal Top-Management per coinvolgere tutta l'organizzazione

- coprono tutti i livelli di profondità dell'analisi; conducono analisi sia a livello concettuale che a livello operativo/tecnologico.

La tendenza attuale rileva una sempre più crescente diffusione di approcci e modelli di analisi e gestione dei rischi di tipo dinamico e continuativo, orientati al business aziendale e integrati con tutte le restanti attività di analisi dei rischi aziendali (rischi operativi, di credito, finanziari, ecc.)

Si rimanda all'Allegato 2 per approfondimenti su alcune delle metodologie più conosciute a livello nazionale e internazionale.

4.2.3 Gli elementi comuni alle principali metodologie

A prescindere dalla metodologia utilizzata, esistono molti elementi e passaggi del processo di analisi dei rischi comuni a tutte le metodologie. Difatti una valutazione dei rischi, indipendentemente dalla metodologia adottata, deve consentire di:

- definire il contesto entro cui svolgere le analisi, cioè definendo cosa si vuole proteggere dal rischio
- individuare, classificare e valorizzare i beni da proteggere
- individuare e valutare gli agenti ostili, minacce ed attacchi e vulnerabilità
- definire quali minacce vanno fronteggiate
- calcolare il rischio finale, valutarne i livelli accettabili e definire le contromisure che permettono di mantenere il rischio entro questi livelli.

La maggior parte delle attuali metodologie di analisi presenta tutti gli elementi descritti, ma può differenziarsi su concetti e terminologie, spesso non chiaramente definiti e, non di rado, difformi dall'accezione prevalente, consolidata negli standard di riferimento. Tali sono, ad esempio, i termini ed i concetti di protezione, pericolo, minaccia, attacco, danno e, quindi, di rischio.

Appare quindi fondamentale, in questo paragrafo, puntualizza-

re l'accezione prevalente dei seguenti principali concetti e le relative definizioni:

- Perimetro d'intervento
- Risorsa informativa (censimento e classificazione)
- Attributi di protezione
- Censimento delle minacce
- Censimento delle vulnerabilità
- Probabilità di accadimento (esposizione alla minaccia)
- Misurazione degli impatti
- Definizione delle contromisure
- Mitigazione del rischio conseguente alle contromisure individuate.

Perimetro d'intervento e risorse informative

La prima attività da svolgere è quella di definire chiaramente il **perimetro d'intervento** e quindi l'organizzazione interessata e le informazioni gestite.

Da qui bisogna procedere ad eseguire un **censimento** analitico **delle informazioni** contenute nel perimetro d'intervento. Il dettaglio del censimento dipende dagli obiettivi e dalla tipologia (concettuale/operativa) di analisi dei rischi che s'intende eseguire.

Ai fini di un'analisi concettuale può essere sufficiente censire i dati a livello di processo (fatturazione, pagamenti, personale) o di **sistema applicativo**, mentre per un'analisi operativa è necessario considerare anche le tecnologie di riferimento (le reti di comunicazione e relativo hardware/software utilizzati per il trattamento).

In ogni caso bisogna mettere in relazione tutti i singoli elementi che compongono l'informazione, quindi dati, software e tecnologie ed i relativi processi che definiscono i metodi **validi** di accesso all'informazione. Ovviamente tutti questi elementi devono poi essere **classificati** per categoria omogenea relativamente alla quale valutare minacce e vulnerabilità.

Le reti informatiche si trovano alla base del sistema di comunicazione e trattamento (input, output e aggiornamento) di tutte le informazioni e quindi si potrebbe obiettare che sono da proteggere a prescindere dalle informazioni che trattano. Questo può effettivamente essere vero in alcune circostanze (esempio per i back-bone di una società di telecomunicazione). In ogni caso bisogna essere coscienti di cosa si debba proteggere e di quante risorse impegnare per la protezione dei diversi elementi dell'intero patrimonio informativo, in base alla loro criticità.

Obiettivi e attributi di protezione

Prima di proseguire oltre è importante definire gli obiettivi del sistema di protezione. Ciò ha un effetto su tutto il resto delle attività in quanto gli **obiettivi di business** di una società con finalità di profitto non sono paragonabili alle **mission** di enti governativi o **non profit** e di conseguenza neanche gli obiettivi di protezione.

In funzione degli obiettivi ci sono poi dei precisi attributi da definire e valutare separatamente. Questi influiscono sul processo di misurazione del rischio e relativa scelta delle tecniche di protezione.

Come già evidenziato precedentemente in questo documento (vedi il paragrafo 1.5), nell'attuale best practice si riscontrano tre attributi di sicurezza: **confidenzialità**, **disponibilità** e **integrità**.

Come accennato precedentemente, è opportuno che i tre attributi siano valutati separatamente, in quanto ognuno di loro presenta diversi scenari di rischio.

Censimento delle minacce

Il rischio è strettamente associato al concetto di **minaccia**, che ne costituisce, per così dire, un equivalente depurato dalle due caratteristiche di probabilità e danno consequenziale. Inoltre il rischio può essere visto come la possibilità che accada un evento negativo, che procuri danni a qualcuno o qualcosa. La minaccia, in effetti, è proprio tale evento.

Possiamo quindi definire **minaccia** come qualsiasi cosa che

possa farci perdere gli attributi di sicurezza di confidenzialità, disponibilità e integrità.

La minaccia è generalmente un evento indesiderato che può essere potenzialmente identificato a priori. Esso è classificabile come evento **interno** o **esterno**. Una minaccia si concretizza tramite **attacchi** variamente attuati.

Senza dubbio c'è una certa tendenza a proteggere il perimetro d'intervento maggiormente da minacce esterne, potenzialmente a causa della visibilità generata da questi eventi, rispetto a quelle interne. La verità è che i rischi interni rimangono la maggioranza e quindi non possono essere sottovalutati. Ad esempio, l'indagine CSI/FBI del 2003 evidenzia, con il 77% dei partecipanti, l'importanza delle minacce interne.

Le minacce interne e i relativi controlli (contromisure) dipendono fortemente dall'organizzazione e dalla natura del trattamento prevalente dell'informazione mentre quelle esterne possono essere fortemente influenzate dalle tecnologie utilizzate, indipendentemente da persone e processi.

Di conseguenza la determinazione delle minacce interne deve considerare l'ambiente organizzativo specifico mentre per quelle esterne si possono utilizzare soluzioni maggiormente standardizzate, riconducibili alle tecnologie al momento maggiormente in uso.

Censimento delle vulnerabilità

Un ulteriore concetto importante è quello di **esposizione** di un determinato soggetto **ad una determinata minaccia**. È opportuno trattare questo concetto assieme ad un altro correlato, anch'esso facente parte del novero delle qualità del soggetto, che è quello di **vulnerabilità**.

La vulnerabilità consiste in una condizione organizzativa o tecnologica che permettere alla minaccia di attuarsi. Le minacce sono presenti in ogni caso ma si annullano, in teoria, in assenza di vulnerabilità. Viceversa la minaccia ha maggiori probabilità di attuarsi in presenza di numerose o importanti vulnerabilità.

La vulnerabilità può essere organizzativa o di processo (mancanza di una vitale funzione aziendale, ad esempio di monitoraggio) o tecnica (debolezze tecniche di BIOS, sistemi operativi, database, e quant'altro).

Le vulnerabilità tecniche si determinano anche con l'ausilio di appositi **scanner**, prodotti automatizzati per la scansione continua delle debolezze tecniche, o tramite attività di **attack and penetration**.

Alla figura 4-1 sono stati sintetizzati le più comuni categorie di vulnerabilità, così come censite in un **security survey** condotto da PricewaterhouseCoopers e CIO Magazine nel 2003.

I principali fattori che contribuiscono alla proliferazione delle vulnerabilità sono:

- componenti difettosi
- distribuzione geografica
- dimensioni e complessità
- evoluzione tecnologica
- scarsa cultura sui problemi di sicurezza.

Il livello di vulnerabilità può essere ridotto attraverso l'implementazione di opportune contromisure di sicurezza, discusse nel capitolo 5 di questo documento. La vulnerabilità non può però mai essere ridotta a zero, perché le stesse contromisure presentano, a loro volta, delle debolezze.

Probabilità di accadimento

Come anche indicato altrove in questo documento, la definizione più accreditata di **rischio** lo identifica come il prodotto (logico o aritmetico) dell'**impatto** (danno arrecato) per la **probabilità** di attuazione di una particolare minaccia. La determinazione di tale probabilità può avvenire tramite l'espressione di un giudizio, ovvero conside-

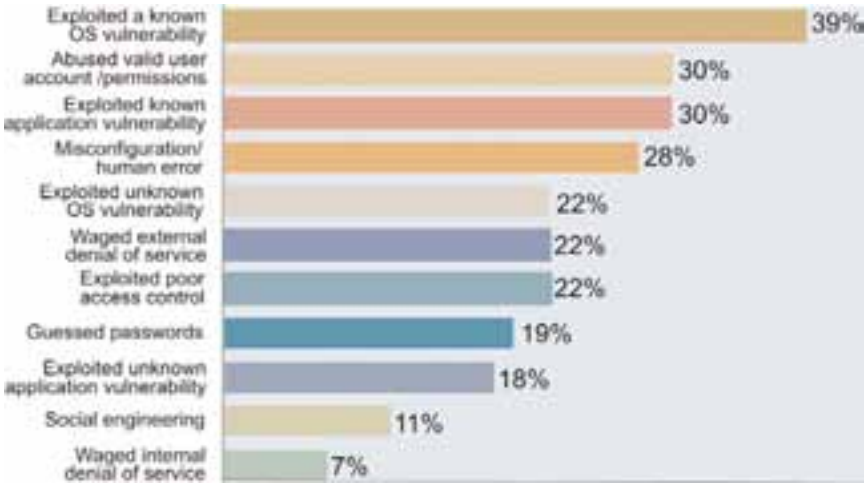


Figura 4-1 - Categorie di vulnerablità più comuni [1]

rando, ove disponibili, le serie statistiche relative ai vari incidenti ed attacchi, oppure tramite entrambe le cose.

Quello che è certo è che in questa fase bisogna valutare tutti gli elementi che contribuiscono al rischio e quindi minacce, attacchi e vulnerabilità. Nella tabella 4-1 si è messo in relazione, a fini esplicativi, alcuni esempi di minacce con relativi attacchi e vulnerabilità.

Misurazione degli impatti

Parte fondamentale di tutto il processo di analisi dei rischi è la determinazione dell'impatto, sulle risorse da proteggere e sull'azienda in genere, nel momento in cui una minaccia viene attuata con successo. L'impatto, come si è visto al punto precedente, è, dopo la probabilità di accadimento di una minaccia, la seconda componente del rischio.

[1] *Tratto da "Information security: a strategic guide for business" © PricewaterhouseCoopers 2003.*

Minacce	Attacchi	Vulnerablità
Un intruso riesce ad accedere alla rete privata dell'organizzazione	L'intruso accede al sistema tramite back door utilizzando una Wireless Local Area Network (Wlan)	- Network Service Set Identifier (SSID) non è stato adeguatamente mascherato - Un punto d'accesso non autorizzato è installato da un dipendente interno - Wired Equivalency Protocol (Wep) è debole e la relativa sessione di crittografia è interrotta
	L'intruso ottiene l'accesso tramite attacco bruto alla password	- Lunghezza minima della password insufficiente - Password deboli soggette ad attacchi da dizionario
	L'intruso ruba una password utente autorizzata	- La sequenza di autenticazione non crittografata permette intrusioni - Basso livello di monitoraggio - Trojan Horse installato in rete
	Un ex dipendente scontento rientra nei sistemi al fine di impossessarsi di informazioni classificate	- Account e password utente non cancellate tempestivamente dopo le dimissioni - Le password di accesso sui terminali dei server dial-in o i punti di accesso Wlan non sono revocati dopo le dimissioni
Perdite finanziarie dovute a operazioni fraudolente	Chi esegue l'attacco simula un'autentica operazione di servizi web	- Autenticazione e crittografia inadeguate nei canali applicativi di comunicazione
	L'intruso riesce ad accedere ai record delle carte di credito del cliente	- Controlli di accesso compromessi su database critico
Perdita di dati critici	Un attacco terroristico distrugge un centro dati	- Procedure di backup dati e di ridondanza inadeguate
	Un programma "cavallo di Troia" cancella un hard drive	- I dipendenti non sono stati sensibilizzati al rischio di scaricare software da fonti non di fiducia - Software antivirus non aggiornato
Servizi internet non disponibili, che determinano perdita di ricavi causa il tempo di fermo	Attacco "Denial of Service" tramite tecnica di "ping" sovraccarica i server di rete bloccandoli.	- Un router programmato malamente non riesce ad individuare i pacchetti malformati - Il sistema operativo del server non è aggiornato con i più recenti standard di sicurezza - Difese antivirus inadeguate
	Un intruso riconfigura il router per impedire il traffico legittimo.	- Impossibilità di resettare la password amministrativa di default sul sistema
	Ripetute richieste di applicazioni saturano le risorse del server	- Inadeguata progettazione delle applicazioni - Controlli di autenticazione inadeguati permettono che le chiamate fraudolente siano accettate come genuine

Tabella 4-1 - Correlazione tra minacce, attacchi e vulnerabilità [2]

[2] *Vedi nota 1.*

La condizione per cui un sistema metrico (vale a dire **atto a misurare**) possa trovare applicazione ad un concetto è, ovviamente, che tale concetto si presti ad essere misurato. Ciò si verifica sempre con le qualità, mentre per le entità possono verificarsi due casi. Il primo è quello in cui l'entità stessa, per sua natura, è misurabile (è il caso del danno); il secondo è il caso per cui l'entità, in sé e per sé, non è misurabile, ma lo diviene per il tramite della misurazione delle sue qualità (è il caso del soggetto, di cui si misura la criticità).

Si rimanda al precedente paragrafo 4.2.2 per un esame più completo degli approcci quantitativi e qualitativi di misurazione.

Misurazione e mitigazione del rischio

In termini formali il rischio, come si è visto, è definito come il prodotto (matematico o logico) tra la **probabilità di accadimento** dell'evento e il **danno arrecabile** (R=Pa*D). In effetti, se almeno uno dei due termini del prodotto tende a zero, si è inclini a percepire il rischio come basso.

Per le misurazioni di tipo qualitativo è invece necessario determinare un sistema di misurazione che permetta di misurare le due componenti del rischio in modo fra di loro omogeneo, tramite un sistema di **gradi** opportunamente tarato.

Risulta inoltre utile, nella pratica, considerare due aspetti del rischio. Il primo, definito come **rischio assoluto** o **intrinseco** e il secondo, definito come **rischio residuo**. Quest'ultimo concetto, a differenza del primo, tiene conto dell'effetto delle contromisure previste.

Definizione delle contromisure

Nel corso del processo di valutazione del rischio ci si trova, all'atto pratico, nella necessità di individuare un **livello accettabile di rischio** e di confrontarsi con il budget effettivamente disponibile.

Con il termine **contromisure** si indicano quindi le misure organizzative e tecnologiche che sono in grado di contrastare e abbattere il livello del rischio, riducendolo a un livello individuato come **accettabile**.

Nel processo di analisi dei rischi può accadere che le contromisure siano definite in modo generico, da assoggettare ad ulteriore analisi e definizione in un'ottica più operativa. È invece sempre importante definire le modalità attuative, i tempi e le responsabilità in un apposito piano operativo di attuazione.

Note conclusive

Si è voluto, in questa sezione del documento, individuare, i vari componenti di un modello generale di analisi del rischio. Lo scopo prefisso è quello di individuare una mappa possibilmente chiara di tutti i componenti di un modello generico, in modo da rendere più agevole la comprensione delle schede dei vari modelli disponibili oggi sul mercato alcuni dei quali sono descritti nell'Allegato 2.

4.2.4 Gestione dei rischi

L'analisi dei rischi, precedentemente descritta, consente di definire le opportune contromisure da adottare. L'effettiva adozione, ossia implementazione delle contromisure, così come la gestione e il monitoraggio nel tempo dell'effettivo stato della sicurezza, rientra nell'ambito della **gestione dei rischi**.

Perché si possa contrastare realmente i rischi individuati ed associati all'utilizzo di infrastrutture per la gestione, trattamento e scambio dei dati, occorre adottare misure di sicurezza che siano **controllabili** ed **efficaci**.

La sicurezza delle informazioni deve essere pertanto vista come caratteristica globale, in grado di fornire, dinamicamente con l'evolversi temporale delle necessità e delle tecnologie, il desiderato livello di riservatezza, integrità e disponibilità delle informazioni e dei servizi.

Un'illustrazione ad alto livello di astrazione delle attività previste per lo svolgimento completo del processo di **gestione dei rischi** è riportata nella seguente figura 4-2.

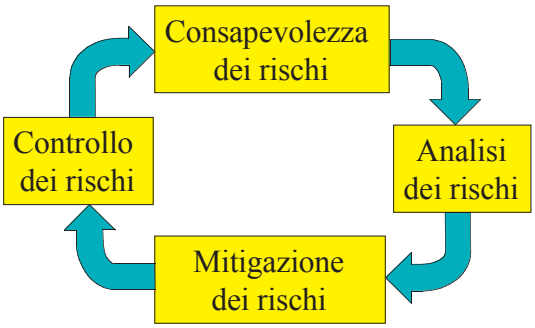


Figura 4-2 - Ciclo di vita della gestione dei rischi

Dall'illustrazione risulta chiaro come il processo di gestione dei rischi debba essere **continuativo** e **ripetibile**.

L'effettiva salvaguardia della sicurezza delle informazioni attraverso un'attenta gestione dei rischi richiede l'integrazione all'interno dell'organizzazione, incaricata di creare, aggiornare, eliminare e mantenere tali informazioni, di un adeguato **Sistema di Gestione della Sicurezza** (SGS) sviluppato secondo le tre dimensioni del problema:

- processi
- organizzazione
- tecnologie.

La mancata analisi di una delle tre dimensioni sopra illustrate, ovvero una loro considerazione frammentaria e limitata al di fuori di un **framework omogeneo** di **valutazione complessiva** dell'attuale stato della sicurezza delle informazioni, comporta la potenziale inefficacia delle azioni correttive intraprese, perché valutate secondo una visione ristretta o incompleta della problematica indirizzata.

In linea generale le problematiche da dover affrontare sono le seguenti:

- identificare e definire i processi aziendali e i contesti di rischio ad essi associati

- assicurare l'aderenza alle normative e standard di sicurezza nazionali ed internazionali (ad esempio D. lgs. 196/2003)
- formalizzare una strategia per la gestione della sicurezza
- decidere le linee guida che l'azienda ha intenzione di adottare in tema di gestione della sicurezza
- preservare gli investimenti fatti o in fase di rilascio immediato per la sicurezza dei Sistemi Informativi.

La gestione dei rischi è essenzialmente **funzione di**:

- missione aziendale
- conformità a leggi e norme
- disponibilità economica.

Uno scopo fondamentale di un Sistema di Gestione della Sicurezza è quello di attuare un ragionevole compromesso tra il **costo della sicurezza** e i **costi della non sicurezza** e il suo obiettivo principale consiste nel mantenere nel tempo uno stabile e ottimale livello di protezione.

In base alle considerazioni fin qui descritte, non si può considerare l'esecuzione di un'analisi dei rischi come unico elemento rilevante per un completa gestione dei rischi, ma occorre:

- implementare effettivamente contromisure adeguate e stabilire un ciclo iterativo che ne verifichi l'efficacia
- mantenere aggiornata la misurazione del rischio, ripetendo periodicamente il processo o implementando sistemi dinamici di gestione del rischio
- considerare l'intera sfera del sistema di gestione della sicurezza (vedi 4.1).

Questo modo di vedere il problema nella sua globalità ha determinato l'attuale tendenza di far convergere modelli di analisi dei rischi in sistemi di gestione dei rischi, principalmente attraverso

moderne metodologie di analisi e misurazione **dinamica**. Tali metodologie considerano anche i cambiamenti che hanno impatto sulle risorse informative ed il risultato delle attività di monitoraggio degli incidenti/attacchi che influisce nell'aggiornamento dei criteri di valutazione del rischio.

4.2.5 Analisi dei rischi a supporto del sistema di gestione della privacy

Il sistema di gestione della privacy è regolamentato in Italia dal D. lgs. 196/2003 (comunemente denominato *Codice della Privacy*).

Tale Codice garantisce che il trattamento dei dati personali si svolga nel rispetto dei diritti e delle libertà fondamentali, nonché della dignità dell'interessato, con particolare riferimento alla **riservatezza**, all'**identità personale** e al **diritto alla protezione dei dati personali**. Di conseguenza, impone alle aziende una serie di adempimenti, sia di tipo normativo sia di tipo tecnico-organizzativo, comprendenti l'adozione di misure specifiche di sicurezza.

Nell'ambito di tali adempimenti spicca l'adozione del **Documento Programmatico sulla Sicurezza**, previsto nel caso di trattamenti elettronici di dati personali **sensibili**.

Al fine di predisporre tale documento, che costituisce una delle misure minime di sicurezza previste dall'art. 34 del Codice e dal punto 19 del Disciplinare Tecnico - Allegato B del Codice stesso, occorre condurre, fra le altre attività, un'analisi dei rischi, avente come ambito di analisi il sistema dei trattamenti di dati personali gestito dall'azienda o dall'ente.

Da quanto sopra detto, con particolare riferimento ai principi e alla ratio della legge, si evince che l'enfasi, nell'applicazione dell'analisi dei rischi a supporto del sistema di gestione della privacy, è diversa rispetto al caso generale di analisi dei rischi a supporto del sistema di gestione della sicurezza aziendale, condotta rispetto all'intero patrimonio informativo aziendale.

Difatti emergono degli elementi di diversità fra i due casi che è interessante rilevare.

È diverso **l'obiettivo** che si vuole raggiungere: l'analisi dei rischi non è più tanto finalizzata a individuare (e quindi a ridurre) le conseguenze di possibili eventi dannosi per l'azienda che effettua l'elaborazione dei propri dati/processi di business, ma piuttosto è finalizzata a individuare le conseguenze di eventi dannosi per i soggetti a cui i dati si riferiscono; in pratica l'obiettivo è la protezione dei trattamenti dei dati personali dei soggetti tutelati dalla normativa sulla privacy.

È diverso **l'oggetto dell'analisi**: in un approccio di analisi dei rischi di carattere aziendale, ci si orienta su risorse e informazioni aziendali come oggetto di protezione. Nel caso dell'analisi dei rischi in ottica privacy è importante prendere in esame i dati limitatamente alla sfera personale dei soggetti interessati (e quindi le banche-dati o archivi contenenti tali dati) e correlarli ai trattamenti che ne vengono effettuati in seno all'azienda o all'ente titolare del trattamento stesso.

Di conseguenza cambia il modo di procedere nella conduzione del processo di analisi dei rischi:

- viene meno l'esigenza di valutare gli impatti
- viene meno l'esigenza di effettuare la classificazione delle informazioni, intesa come valutazione della criticità delle informazioni, in quanto è la normativa stessa a classificare e distinguere i dati inerenti la sfera personale su due livelli:
  - sensibili
  - non sensibili (anche detti dati personali comuni o ordinari).[3]

Resta comunque in capo alle aziende ed agli enti la non banale attività di identificare, al proprio interno e presso gli eventuali partner di outsourcing, l'esistenza di dati personali ordinari e sensibili, correlandoli ai pertinenti processi e applicazioni.

[3] *La normativa, indirettamente, individua, per differenza, un terzo tipo di dati: quelli che non ricadono nell'applicazione della norma stessa.*

5 - Misure per la protezione delle reti

5.1 MISURE TECNOLOGICHE

La tecnologia adottata oggi per le comunicazioni in rete deriva direttamente dall'attività di standardizzazione iniziata negli anni ottanta. L'organismo internazionale ISO/OSI definì a quel tempo, com'è noto, un modello di riferimento per le reti strutturato su sette livelli differenti, ognuno con un compito specifico: **Physical, Data link, Network, Transport, Session, Presentation**.

Per ogni livello della pila ISO/OSI, ad eccezione del primo (Physical), viene adottato in genere un protocollo che, utilizzando regole predefinite, consente di comunicare e trasferire dati tra interlocutori appartenenti alla stessa rete. Quando due o più sistemi hanno necessità di comunicare, **tutti** i livelli della pila ISO/OSI vengono coinvolti, dal livello **applicativo**, da cui normalmente si genera l'informazione da trasmettere, al livello fisico dove questa informazione viene convertita in segnali digitali per consentire la trasmissione fino a destinazione.

Potenzialmente le informazioni possono essere compromesse durante il transito in uno qualsiasi di questi livelli ed è per questo motivo che rendere **sicura** un'infrastruttura di rete significa adottare contromisure specifiche per **ogni livello** della pila ISO/OSI.

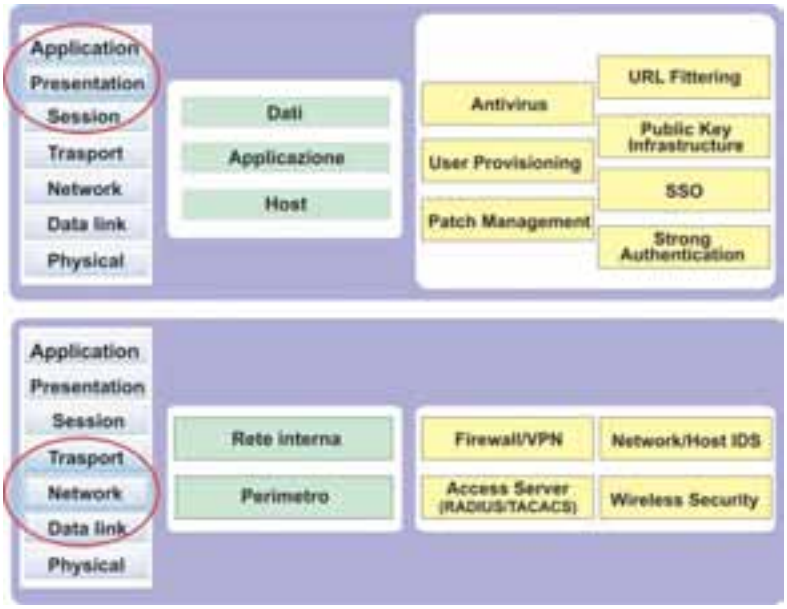


Figura 5-1 - Livelli ISO/OSI e tecnologie di protezione

La figura 5-1 illustra le principali tecnologie di protezione evidenziando, per ciascuna di esse, l'ambito (o asset) che sono in grado di proteggere. Nella realtà è abbastanza comune trovarsi di fronte a tecnologie in grado di realizzare sicurezza a più livelli (dalla rete alle applicazioni), ma per impostare una strategia di sicurezza efficace è bene comprendere fino in fondo gli ambiti di intervento di ciascuna tecnologia e soprattutto i rischi che ciascuna tecnologia è in grado di mitigare, considerando l'intero ciclo di vita dell'informazione.

5.1.1 Firewall e VPN

Il **firewall** costituisce, generalmente, lo strumento privilegiato per proteggere e controllare le comunicazioni che avvengono tra le diverse reti di un'organizzazione. Il firewall è un sistema hardware e/o software in grado di controllare il flusso di traffico, proveniente da reti **untrusted**, per le quali non è possibile determinare il livello di sicurezza, e diretto verso altri reti **trusted**, dove il livello di sicurezza è ben noto e garantito da opportune protezioni.

Le tecnologie firewall disponibili sul mercato sono estremamente varie e progettate specificamente per la tipologia di reti che devono proteggere: dalle reti WAN (ADSL, ISDN, Frame Relay) a quelle LAN (Ethernet, Token Ring, ecc.). Le tecnologie firewall moderne sono in grado di ispezionare i protocolli di comunicazione dai layer più bassi (livello fisico) a quelli più alti (livello applicativo), pur applicando la **maggioranza dei controlli a quei livelli che hanno un'implicazione diretta con la rete**.

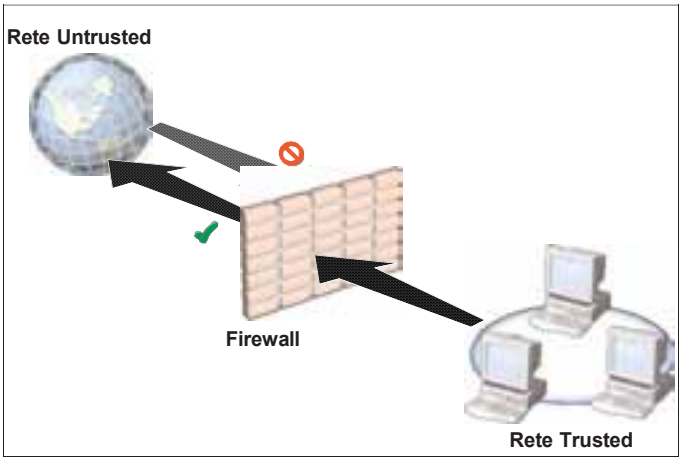


Figura 5-2- Firewall e reti

Per svolgere la sua funzione è necessario che **tutto** il traffico da proteggere transiti per il sistema firewall il quale, applicando le politiche di sicurezza impostate, consente o nega l'accesso alle risorse richieste.

Considerando l'infrastruttura di rete tipica di un'organizzazione sufficientemente informatizzata, quando si utilizza un sistema firewall è consuetudine parlare di **protezione perimetrale e protezione interna**.

La prima si riferisce alla messa in sicurezza delle comunicazioni che avvengono tra il perimetro esterno della rete (tipicamente Internet/Extranet) ed il resto dell'infrastruttura. La seconda si riferisce

invece alle contromisure necessarie per proteggere le comunicazioni che avvengono all'interno dell'organizzazione. Qui il firewall può essere adottato per segmentare ulteriormente la rete interna e per mettere in sicurezza reti aziendali particolarmente critiche.

La tabella seguente riassume le tecnologie firewall alla base dei principali prodotti del mercato.

Tecnologia Firewall	**Livello OSI**	**Caratteristiche**
Packet Filtering	Network (3)	Sicurezza limitata, prestazioni elevate, Network Address Traslation (NAT)
Application-Level Proxy	Application (7)	Sicurezza elevata, basse prestazioni
Circuit-level Proxy	Session (5)	Sicurezza media, prestazioni medie
Stateful Inspection	Da Network ad Application (2-7)	Compromesso tra sicurezza e prestazioni

Tabella 5-1 - Tecnologie prevalenti nei firewall

Le **VPN** (Virtual Private Network) sono realizzate con tecnologie che consentono di attuare su connessioni fisiche pubbliche canali virtuali **protetti** e, quindi, **privati**. Tali tecnologie fanno uso di protocolli specifici per la sicurezza delle transazioni, ad esempio **IPsec**, che utilizzano algoritmi crittografici sia ai fini dell'autenticazione delle parti, sia al fine di garantire la segretezza delle informazioni scambiate. Le funzionalità previste comprendono quella di gestione delle chiavi che avviene in modo trasparente agli utenti. Il traffico viene normalmente crittografato, per motivi di efficienza globale del sistema, tra router e router aziendale, escludendo le reti locali interne all'azienda stessa: in pratica, la funzione di VPN viene implementata su router, per così dire, **potenziati**, venendo ad aggiungersi a quella di routing ordinario. Le VPN possono anche essere implementate tra client e client.

5.1.2 Network/Host IDS

Un **Intrusion Detection System** (IDS) è un altro componente dell'infrastruttura tecnologica di protezione per sistemi e reti. A differenza di un firewall, che è considerato un sistema di protezione **atti-**

vo, un IDS è normalmente inteso come un dispositivo **passivo**, in grado di monitorare ed analizzare gli eventi che accadono sulla rete senza agire direttamente su di essi per contrastarli.

Un IDS raccoglie informazioni da host e segmenti di rete (DMZ, dorsali Internet, segmenti LAN, ecc.) allo scopo di identificare potenziali violazioni (attacchi esterni o interni all'organizzazione). Le tecnologie adottate dai moderni IDS si dividono in due categorie principali:

- **Pattern matching**. Il sistema analizza il flusso di pacchetti alla ricerca di sequenze associabili ad attacchi noti, che sono memorizzati in un database aggiornato regolarmente. In questo senso il funzionamento è molto simile a quello di un sistema antivirus ed è pertanto in grado di individuare solo attacchi noti
- **Statistical/Traffic anomaly based**. A differenza dei precedenti, l'individuazione delle violazioni avviene attraverso l'analisi degli scostamenti della quantità o tipologia di traffico rispetto a soglie pre-impostate e considerate **normali** o abituali per la realtà in esame. Questo genere di approccio consente di individuare anche attacchi non noti, ma è fortemente suscettibile alle variazioni di traffico transitorie che il più delle volte non sono riconducibili ad un attacco. Tali sistemi sono, pertanto, considerati meno affidabili rispetto ai precedenti.

Indipendentemente dalla tecnologia di analisi su cui l'IDS si basa è frequente distinguere due architetture comuni, legate alla tipologia di asset (beni) che devono essere monitorati: **network based** (analisi di segmenti di rete) e **host based** (analisi dei singoli sistemi).

- **Network IDS**. Un NIDS (Network IDS) analizza in tempo reale i pacchetti che attraversano la rete su cui agiscono, alla ricerca di sequenze che possano essere ricondotte a violazioni, attacchi sulla rete, o semplicemente un utilizzo sospetto delle risorse. Nel momento in cui rileva un potenziale attacco, l'IDS è in grado di inviare notifiche agli amministratori o responsabili della sicurezza i quali, dopo opportune valutazioni, intraprendono le azioni successive per contrastare l'incidente

- **Host based IDS**. Un HIDS (Host IDS) analizza in tempo reale il traffico diretto ad uno specifico sistema alla scoperta di attività maliziose o sospette. L'implementazione di questi IDS avviene pertanto direttamente sul sistema da monitorare. Tale approccio consente pertanto di analizzare anche aspetti intrinseci dell'host, quali i principali file e log di sistema.

Sebbene il funzionamento delle due tipologie possa apparire del tutto analogo, la scelta del sistema IDS deve essere ponderata e avvenire considerando svariati fattori, tra i quali:

- architettura di rete (numero e tipologia di segmenti di rete)
- livello di complessità e requisiti di sicurezza
- numero e tipologia di host/server da proteggere
- caratteristiche delle tecnologie di rete esistenti.

Affinché il sistema IDS possa dare il massimo dei benefici è necessario effettuare un'operazione di ottimizzazione delle politiche/parametri (**tuning**) che regolano il funzionamento del dispositivo ed assicurano il minor numero di falsi positivi (segnalazioni di attacchi non reali) e falsi negativi (mancata segnalazione di attacchi effettivi).

Infine, considerando l'enorme quantità di dati che i sistemi IDS sono costretti ad esaminare, è necessario valutare con attenzione le performance dei dispositivi hardware/software che compongono la soluzione IDS. Generalmente, per ottenere prestazioni migliori, è necessario adottare dei **security appliance** dedicati, in grado di analizzare elevate quantità di traffico nell'unità di tempo.

5.1.3 Access Server (RADIUS/TACACS)

Da un punto di vista generale, qualsiasi accesso esterno alla rete aziendale può costituire una minaccia per l'organizzazione. Tuttavia la necessità di avere costantemente a disposizione i dati aziendali, anche quando non è possibile fisicamente accedere al sistema informativo dall'interno, impone l'utilizzo di tecnologie in grado di fornire un accesso diretto ai sistemi interni con una connessione telefonica o similare, da qualsiasi punto del mondo ed indipendentemente dall'orario locale.

L'infrastruttura che realizza quanto descritto è comunemente conosciuta come **remote access** o **accesso remoto** ed è costituita da un set di tecnologie che in maniera trasparente connettono alla rete interna aziendale un computer situato in una locazione remota. Ciò è particolarmente utile per connettere il laptop di un dipendente alla rete dell'organizzazione e consentire l'utilizzo dei servizi aziendali (e-mail, file server, intranet, ecc.).

Affinché tale accesso non si trasformi in una vulnerabilità nella rete dell'organizzazione è fondamentale adottare tecnologie di protezione adeguate. Tra gli standard più diffusi per la protezione degli accessi remoti si citano: **RADIUS** (Remote Authentication Dial-In User Service) e **TACACS** (Terminal Access Controller Access Control System).

Integrate negli **access server** queste due tecnologie si occupano di verificare le credenziali degli utenti che accedono da remoto, attraverso l'utilizzo della combinazione **user name** e **password** o, nelle versioni più evolute, mediante tecnologie di autenticazione forte (**smart card**, **token**, **digital ID**, ecc.).

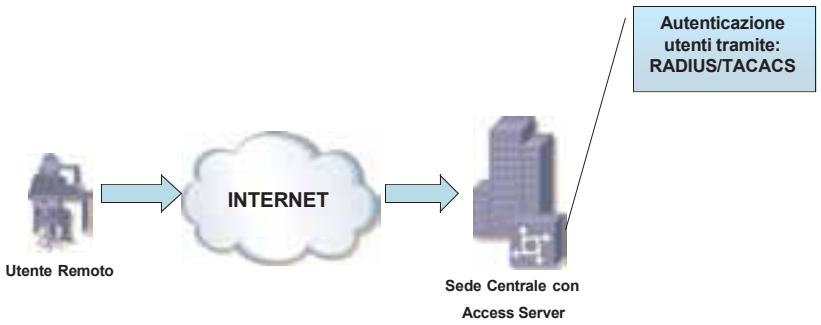


Figura 5-3- Remote Access Server

La tecnologia **RADIUS** è utilizzata da molti ISP per autenticare gli utenti. L'utente che si connette con una linea dial-in immette user name e password e il served RADIUS ne controlla la correttezza autorizzando l'utente all'accesso al sistema.

Negli ultimi tempi la tecnologia RADIUS è spesso usata anche all'interno delle organizzazioni, come sistema centralizzato di autenticazione per la gestione degli apparati di rete o l'accesso attraverso dispositivi wireless.

Il protocollo **TACACS** è diffuso nelle reti UNIX. Esso consente al server di accesso remoto di comunicare con un **authentication server** per verificare le credenziali di autenticazione per l'accesso alla rete.

Per evitare il furto di credenziali, entrambe le tecnologie generalmente crittografano le informazioni di autenticazione prima di inviarle sulla rete.

5.1.4 Wireless security

Per reti **wireless** si intendono quelle reti dove il collegamento tra qualunque elemento della rete avviene non per mezzo di connessioni via cavo ma per mezzo di **radiofrequenze**. Nella pratica, in una rete wireless gli elementi mobili (tipicamente i posti di lavoro, talvolta stampanti o altre periferiche) comunicano via radiofrequenza mentre gli elementi fissi (apparati di rete, sistemi server) sono collegati tramite cablatura fissa.

La rete wireless presenta, rispetto ad una rete fissa, una maggiore potenziale vulnerabilità, per le sue caratteristiche intrinseche di apertura. Per questo sono stati definiti una serie di meccanismi di protezione che hanno lo scopo di rendere la sicurezza di una rete wireless quanto più vicina a quella di una rete fissa.

Di seguito vengono elencati i protocolli di sicurezza in ordine crescente di livello di protezione:

- **Wired Equivalent Privacy (WEP):** è stato il primo meccanismo di protezione standard per reti basate sul protocollo 802.11, che definisce le modalità sia per la cifratura dei dati inviati tra il client mobile e l'Access Point (AP) che per l'autenticazione del dispositivo mobile. Il protocollo WEP ha evidenziato ben presto alcune debolezze, tra cui:
  - il protocollo di autenticazione non è bidirezionale (l'AP identifica il client, ma non viceversa)

- vengono identificati solo dispositivi, non utenti
- non è definita una modalità di gestione delle chiavi, che sono statiche e quindi si rendono necessarie operazioni di configurazione manuali per la loro gestione.

Per aumentare il grado di sicurezza, alcuni AP implementano una modalità di controllo per l'autenticazione del dispositivo, basato sul riconoscimento dell'identificativo dell'indirizzo di rete del dispositivo che si connette; questa tecnica è nota come **MAC address authentication** e fa uso di una tabella di indirizzi configurata sull'AP

- **IEEE 802.1x:** per ovviare ai limiti intrinseci del protocollo WEP sono stati definiti gli standard IEEE 802.1x, dove x è una lettera che ne identifica le caratteristiche. La famiglia di protocolli 802.1x consente l'autenticazione di un utente su rete wireless da parte di un sistema centrale di autenticazione. Viene utilizzato l'**Extensible Authentication Protocol** (EAP), usato anche nelle reti punto-punto, che consente di adottare schemi di autenticazione diversi, negoziabili tra client mobile ed AP durante la fase di connessione.

  Tra questi schemi il più noto è il **Transport Layer Security** (EAP-TLS), usato in ambienti che fanno uso, per autenticazioni remote, di certificati tipicamente memorizzati su carte elettroniche.

  Allo scopo di rendere il protocollo EAP ancora più sicuro è stato introdotto il Protected EAP (PEAP) che cifra le credenziali all'atto del login da parte dell'utente.

  Frequentemente alle reti basate sui protocolli 802.1x e EAP si associa un server di autenticazione che fa uso della tecnologia RADIUS: il vantaggio di questa soluzione sta nel poter autenticare qualunque tipo di dispositivo wireless che si connetta ad una rete.

La figura illustra una rete wireless, con server di autenticazione Radius:

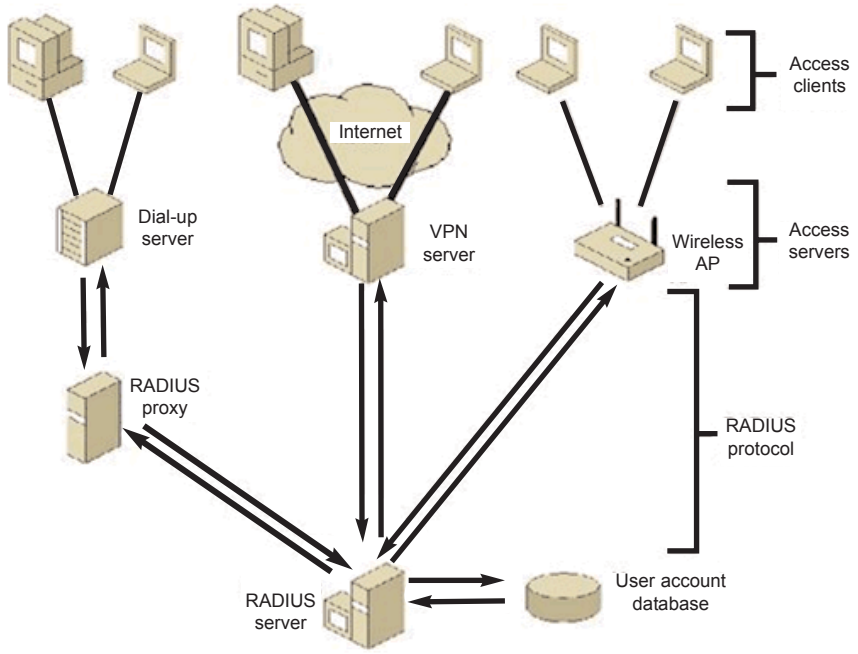


Figura 5-4- Rete wireless, con server di autenticazione Radius

5.1.5 Antivirus

Analogamente ai virus biologici anche quelli informatici, con il passare del tempo, hanno subito importanti evoluzioni, soprattutto per quanto riguarda i danni causati (il cosiddetto **payload** del virus). L'atteggiamento diffuso fino a qualche tempo fa era quello di considerare i virus come programmi in grado, nel peggiore dei casi, di alterare l'uso normale del proprio PC.

L'entità del danno subito variava dalla semplice visualizzazione di messaggi o immagini più o meno ironiche all'impossibilità di avviare o utilizzare correttamente il sistema, con la conseguente neces-

sità di un intervento specialistico. In quel periodo lo scambio di file avveniva prevalentemente attraverso i floppy disk, che pertanto costituivano il principale mezzo di propagazione dei virus.

La diffusione d'Internet a livello planetario, con le relative tecnologie di comunicazione, ha consentito invece il potenziale scambio di file e programmi con qualsiasi utente della Rete, annullando, di fatto, l'intermediazione fisica tra le persone. Tale fenomeno, se da un lato costituisce un indiscutibile vantaggio, ha tuttavia aumentato enormemente le possibilità d'infezioni, sia in termini di velocità nella propagazione che nel numero d'utenti contemporaneamente coinvolti.

Sulla scia di quest'importante innovazione sono apparsi i primi virus in grado di sfruttarla pienamente, generando nuove e preoccupanti minacce. Pensiamo ai danni causati dal virus Melissa che ha letteralmente inginocchiato i sistemi di posta elettronica di tutto il mondo con una velocità impressionante, grazie anche alla possibilità di reperire nuove vittime dalle rubriche dei PC già infetti. In realtà Melissa è una goccia in mezzo al mare; sulla stessa scia, infatti, virus come SirCam, Klez, Sobig introducono nuove preoccupanti tecniche che rendono le infezioni sempre più globali e con un payload più distruttivo: si passa dalla cancellazione alla diffusione non autorizzata di documenti riservati.

In teoria esistono varie tipologie di antivirus (**scanner**, **integrity checker**, **immunizzatori**, ecc.). All'atto pratico, il tipo quasi generalmente utilizzato appartiene alla tipologia **scanner** e si basa sulla capacità di questo tipo di software di riconoscere, all'interno dei supporti periodicamente esplorati e mantenuti sotto controllo, particolari **patterns** sospetti (**firme**), facenti parte di un data base di firme note. È evidente la necessità che i data-base delle firme di tali antivirus vengano periodicamente e tempestivamente aggiornati. La procedura di distribuzione degli aggiornamenti costituisce un'importante aspetto operativo, spesso trascurato, dell'infrastruttura di sicurezza

5.1.6 URL Filtering

L'utilizzo capillare di Internet all'interno delle organizzazioni, se da un lato rappresenta un'opportunità straordinaria per migliorare i processi interni ed esterni ed aumentare la produttività dei singoli, dal-

l'altro può comportare rischi intrinseci per i singoli utenti e per l'organizzazione stessa nel suo complesso.

Tra gli effetti più comuni derivanti da un uso improprio di Internet abbiamo:

- riduzione della produttività individuale
- dispendio di risorse informatiche (connettività, server, ecc.)
- aumento delle probabilità di infezione da parte di codici maligni
- aumento dei rischi di intrusioni interne/esterne
- esposizione a controversie legali dovute, ad esempio, ad un utilizzo **disinvolto** dei servizi Internet (pornografia, violazione di copyright, ecc.)

Un rimedio alle problematiche sopra evidenziate è rappresentato dall'utilizzo delle tecnologie di **URL Filtering**. Si tratta di soluzio-

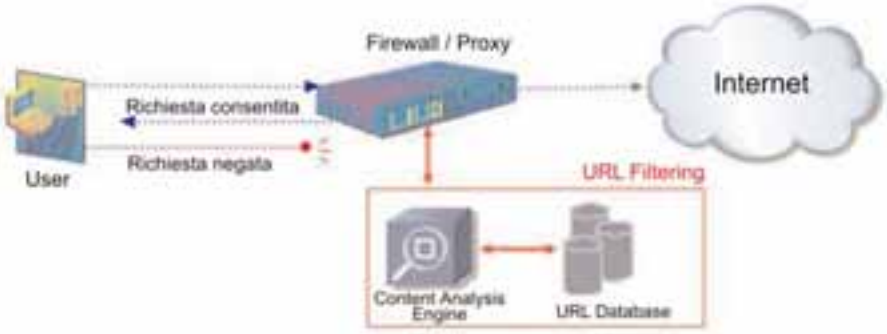


Figura 5-5- Architettura di una soluzione URL Filtering

ni hardware e/o software che, integrandosi con l'infrastruttura di rete esistente, consentono di filtrare i contenuti Internet richiesti dagli utenti, in base a delle politiche prestabilite.

Le tecniche comunemente adottate da questi strumenti sono principalmente due:

- **Black list.** L'indirizzo richiesto dall'utente viene confrontato con una lista di indirizzi non consentiti ed inseriti in precedenza. Se il confronto è positivo viene negato l'accesso alla risorsa
- **URL database.** Rappresenta la tecnica più sofisticata e consiste in un database di indirizzi Web che, aggiornato periodicamente, classifica i contenuti Internet in appositi gruppi. L'utente viene assegnato ad uno o più gruppi o configurato per essere escluso da alcuni di essi. In questo modo è possibile applicare restrizioni su categorie di siti, piuttosto che censire manualmente ciascun indirizzo.

5.1.7 Patch Management

Uno degli aspetti più impegnativi per garantire la sicurezza delle informazioni consiste nel gestire costantemente le **vulnerabilità** che affliggono la maggior parte dei software utilizzati.

È infatti estremamente improbabile che un sistema possa considerarsi esente da errori di sviluppo che, a vario titolo, possono compromettere la sicurezza dell'organizzazione. Oggigiorno la sfida di qualsiasi responsabile della sicurezza è proprio quella di intervenire rapidamente per risolvere le vulnerabilità appena scoperte.

Questa battaglia può essere vinta solo attraverso l'impegno dei produttori di software, che sono chiamati a rilasciare gli aggiornamenti di sicurezza (**patch**) nel più breve tempo possibile.

Ciò nonostante, l'impegno che l'organizzazione deve mettere in campo per gestire tale problematica cresce esponenzialmente all'aumentare dei sistemi utilizzati. Tale difficoltà spinge, il più delle volte, a non considerare affatto la problematica, che diventa pertanto un canale preferenziale per violare la sicurezza dei sistemi.

Una soluzione automatizza per la gestione delle vulnerabilità consente di ridurre notevolmente l'impegno previsto, aumentando significativamente la tempestività di applicazione delle patch.

Tali soluzioni, comunemente conosciute come applicazioni di **patch management**, forniscono funzionalità avanzate per l'analisi, la raccolta e la distribuzione degli aggiornamenti di sicurezza per applicazioni e sistemi operativi.

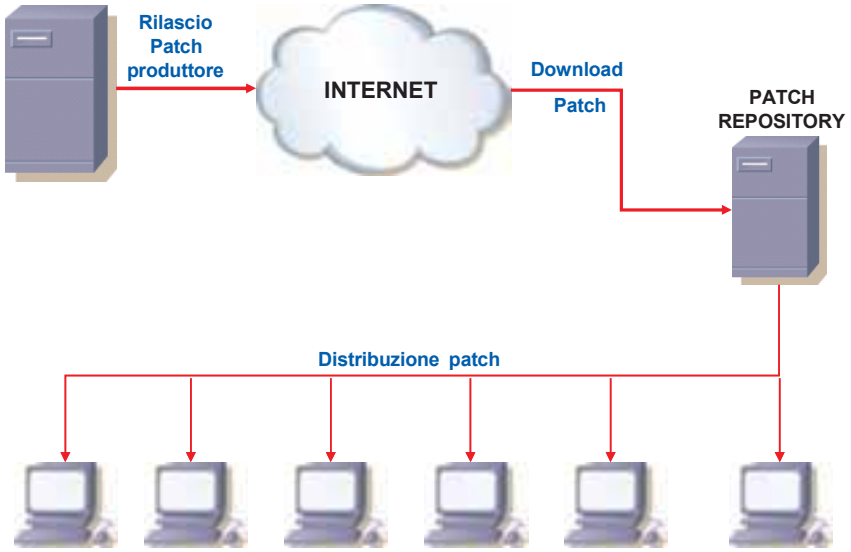


Figura 5-6- Architettura tipica di patch management

L'architettura tipica di un sistema di patch management consiste in un server centralizzato per il repository delle patch, scaricate automaticamente dai produttori dei sistemi operativi e delle applicazioni, corredato da una console centralizzata da cui gestire, in maniera automatica, gli aggiornamenti sull'intera rete aziendale. La piattaforma di patch management si occupa di distribuire le patch sui diversi sistemi.

L'utilizzo di una soluzione di patch management migliora la sicurezza dei servizi in azienda riducendo notevolmente i rischi legati alle vulnerabilità e snellendo notevolmente il processo di messa in sicurezza.

5.1.8 Crittografia e Public Key Infrastructure

Una **infrastruttura a chiave pubblica**, conosciuta anche come **PKI** (Public Key Infrastructure), è un sistema di **certificati digitali, autorità di certificazione** (CA) e **autorità di registrazione** (RA) che verifica, tramite l'utilizzo della crittografia a chiave pubblica, la legittimità delle varie parti coinvolte in una transazione elettronica. Gli standard PKI sono ancora in evoluzione, sebbene vengano già ampiamente implementati come un elemento necessario per la diffusione del commercio elettronico.

Le motivazioni che portano un'organizzazione a scegliere di realizzare, anche solo al proprio interno, un'infrastruttura a chiave pubblica sono molteplici:

- **protezione avanzata.** Un livello avanzato di autenticazione è reso possibile dalle smart card. La riservatezza e l'integrità dei dati trasmessi nelle reti pubbliche è garantita dalla protezione IP (IPsec) e la riservatezza dei dati memorizzati viene realizzata tramite sistemi di gestione dei files supportata da crittografia (ad esempio, EFS - Encrypting File System in ambito Windows 2000 e altri sistemi operativi Microsoft)
- **amministrazione semplificata.** L'organizzazione può rilasciare certificati anziché password. È possibile revocare i certificati in base alle esigenze e pubblicare gli elenchi dei certificati revocati (CRL, Certificate Revocation List)
- **funzionalità di cifratura.** È possibile scambiare file e dati in modo protetto su reti pubbliche, quali Internet. L'implementazione di un sistema di posta elettronica protetto è resa possibile dall'utilizzo delle estensioni S/MIME (Secure Multipurpose Internet Mail Extensions), mentre la protezione delle connessioni Web viene generalmente realizzata tramite SSL (Secure Sockets Layer) o TLS (Transport Layer Security).

Gli elementi che permettono ad un'organizzazione di implementare un'infrastruttura con chiave pubblica comprendono:

- **certificati**. Un certificato è essenzialmente una credenziale digitale rilasciata da un'autorità che garantisce l'identità del titolare del certificato. Un certificato associa una chiave pubblica

all'identità della persona, del computer o del servizio che dispone della chiave privata corrispondente. I certificati vengono utilizzati da diversi servizi e applicazioni di protezione con chiave pubblica, che forniscono l'autenticazione, l'integrità dei dati e servizi di comunicazioni sicure nell'ambito di reti **pubbliche**, quali Internet.

Il formato di certificato standard utilizzato è quello descritto dalla norma **X.509v3**. Un certificato X.509 include informazioni sulla persona o l'entità per cui è stato emesso, informazioni sul certificato, oltre a informazioni facoltative sull'autorità di certificazione emittente. Le informazioni sul soggetto possono includere il nome dell'entità, la chiave pubblica, l'algoritmo della chiave pubblica e un ID univoco opzionale del soggetto. Le estensioni standard per i certificati della versione 3 contengono informazioni relative agli identificatori della chiave, all'utilizzo della chiave, ai criteri del certificato, a nomi e attributi alternativi, ai vincoli del percorso di certificazione e informazioni relative alla revoca dei certificati, compresi i motivi della revoca

- **servizi certificati.** Un'autorità di certificazione ha il compito di stabilire e garantire l'identità dei titolari dei certificati. L'autorità di certificazione revoca anche i certificati nel caso non vengano più considerati validi e pubblica gli elenchi di revoche dei certificati (CRL, Certificate Revocation List) che verranno utilizzati dai verificatori dei certificati. La struttura PKI è composta da una sola CA principale. In pratica, tuttavia, la maggior parte delle società che gestiscono un'infrastruttura con chiave pubblica utilizzerà un certo numero di autorità di certificazione, organizzate in gruppi **trusted** noti come **gerarchie di certificazione**.

  Un elemento distinto di servizi certificati è costituito dalle pagine di registrazione Web CA. Tali pagine vengono predisposte quando si imposta una CA e consentono agli utenti di inviare le richieste di certificati mediante un browser Web. Inoltre, le pagine Web CA possono essere installate nei server in cui non è stata installata un'autorità di certificazione.

In questo caso le pagine Web vengono utilizzate per dirigere le richieste di certificati a una CA alla quale si desidera impedire, per qualsiasi motivo, l'accesso diretto da parte dei richiedenti

- **certificati e smart card.** I certificati possono essere memorizzati su smart card per facilitare l'accesso ad un sistema, per l'autenticazione via Web, per la protezione dei messaggi di posta elettronica e altre funzionalità di sicurezza che utilizzino la crittografia a chiave pubblica
- **criteri di chiave pubblica**. In alcuni sistemi è possibile utilizzare dei **criteri di gruppo** per distribuire automaticamente i certificati ai computer, stabilire gli elenchi di certificati attendibili e le autorità di certificazione trusted comuni, nonché gestire i criteri di recupero per eventuali sistemi di gestione file supportati dalla crittografia (come, ad esempio, EFS - Encrypting File System).

5.1.9 Single Sign On (SSO)

Il proliferare delle applicazioni, a volte legate anche ad esigenze transitorie, costringe il più delle volte l'utente ad eseguire svariate procedure di autenticazione. Così come delineato oltre, trattando di Identity Management, la gestione delle password può divenire complessa non solo per gli amministratori, ma anche per gli utenti che devono utilizzarle.

Uno dei requisiti richiesti, nel progettare sicurezza, è la semplicità d'uso. Aumentando la complessità di accesso ai dati ed alle applicazioni aumentano anche i rischi di perdita di confidenzialità ed integrità. Ciò accade, ad esempio, quando un utente, costretto a ricordare numerose password per accedere a diverse applicazioni, comincia a trascriverle non garantendone più la segretezza.

La soluzione che consente di adottare una procedura **unificata** per l'acceso a più applicazioni è comunemente indicata come **Single Sign On** (SSO). In sostanza la tecnologia alla base di un sistema SSO è costituita da un database di utenti e credenziali, da un numero variabile di interfacce verso applicazioni e sistemi (**agent**) e da una serie di funzionalità che assicurano l'esatta sincronizzazione delle informazio-

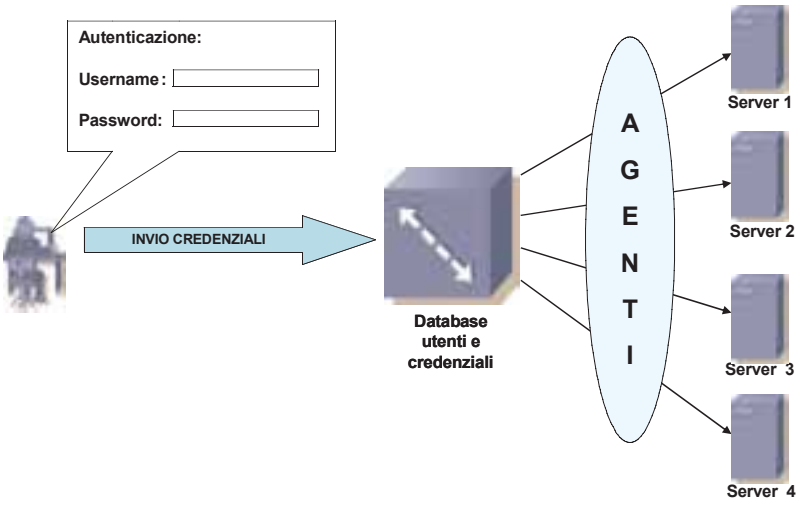


Figura 5-7 - Architettura tipica di Single Sign-On

ni di autenticazione (**password syncronization**) per ciascun sistema.

In presenza di ambienti molto eterogenei, caratterizzati dalla presenza di sistemi operativi ed applicazioni molto diverse tra loro, la soluzione di SSO può diventare estremamente complessa da realizzare. Inoltre, in simili circostanze, non sempre è possibile adottare un'unica soluzione, ma piuttosto bisogna ricorrere a personalizzazioni ed integrazioni di diverse tecnologie.

La combinazione tra SSO ed Identity Management (si veda più avanti il paragrafo 5.2.2) assicura la completa efficienza del binomio utente/applicazione, diminuendo notevolmente l'impegno giornaliero richiesto allo staff ICT per la gestione di queste problematiche. Inoltre, aggiungendo uno strato di controllo e di precisione maggiore, i due sistemi innalzano notevolmente il livello di sicurezza e, contemporaneamente, diminuiscono anche l'incidenza di errori umani.

5.1.10 Strong Authentication

L'identità di un utente remoto è generalmente verificata attraverso due funzionalità di sicurezza principali: l'**identificazione** e l'**autenticazione**. La prima è la fase in cui l'utente **dichiara** la propria

identità al sistema, mentre la seconda si riferisce alla tecnica con cui tale identità viene verificata. La sicurezza dell'asset a cui l'utente accede dipende fortemente dalla tecnica utilizzata per autenticarlo. L'utilizzo di sistemi deboli o non sufficienti a garantire l'identità dell'utente remoto possono esporre il target a numerosi rischi. Il sistema di autenticazione più diffuso è la **password**. La combinazione tra **identificativo** e **password** autentica l'utente al sistema.

Tuttavia questa tecnica fornisce una sicurezza molto limitata, essendo caratterizzata da diverse problematiche. La password, infatti, può essere trascritta e sottratta, smarrita, dedotta, condivisa e dimenticata e non è, pertanto, adatta nei sistemi in cui è necessario avere una ragionevole certezza **sull'effettiva identità** del soggetto che accede. Per superare tali limitazione ed innalzare i livelli di sicurezza sono nate le tecniche di **Strong Authentication** o **autenticazione a due fattori**. In questo caso, oltre all'identificativo, l'utente è in possesso di due elementi: uno da **ricordare** (password o pin) e l'altro da **possedere** (dispositivo fisico).

Solo avendo entrambi, l'autenticazione avviene con successo.

L'utente che viene autenticato può essere **locale** o **remoto**. Il primo realizza la connessione al sistema attraverso una postazione personale o aziendale raggiungibile attraverso una rete locale (LAN) o gestita dalla stessa entità in cui risiede il sistema da accedere. Per utente remoto, invece, s'intende qualsiasi tipologia di utente che accede al sistema attraverso una connessione esterna alla rete aziendale (Internet, VPN, extranet, dial-up, ecc.)

Esistono svariate soluzioni commerciali che implementano le tecniche di Strong Authentication, ognuna caratterizzata da ambiti di impiego e livelli di sicurezza diversi. La scelta del sistema più adatto deve considerare vari fattori, tra i quali:

- valore del bene da proteggere
- livello di sicurezza richiesto
- tipologia di utente da autenticare (locale o remoto)
- impatto tecnico sui sistemi dell'utente e sull'infrastruttura target

- tipologia di accesso remoto (Internet, VPN, RAS, Extranet, ecc.)
- facilità d'uso del sistema.

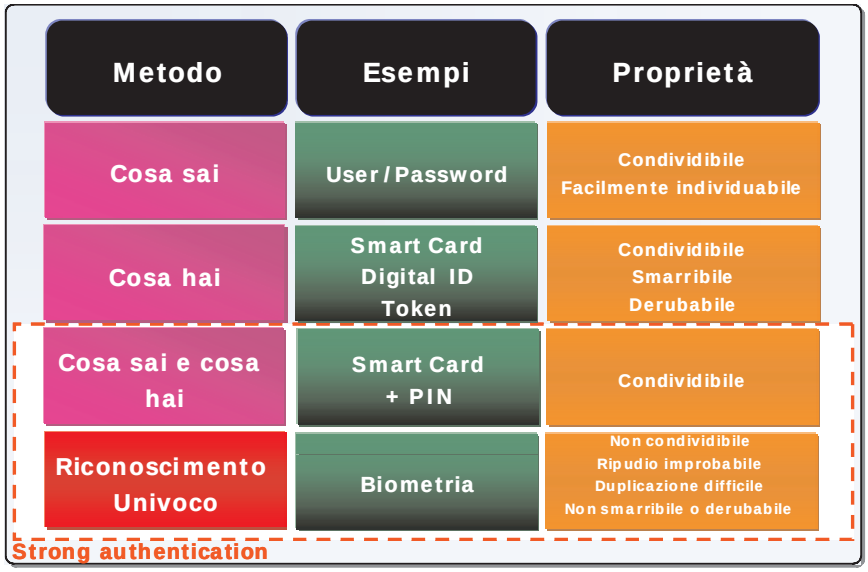


Figura 5-8 - Tecniche di autenticazione

La tipologia di utente che accede al sistema è un parametro fondamentale che dovrebbe essere considerato con attenzione durante la scelta di una soluzione di strong authentication. Alcune tecniche, infatti, sono più adatte all'utente remoto (in particolare quelli mobili) ed altre invece più idonee ad un utente aziendale interno (desktop o server).

La tabella alla pagina seguente riassume le principali soluzioni di autenticazione forte disponibili sul mercato.

Esistono varie tecnologie in grado di assicurare un elevato livello di sicurezza in fase di autenticazione. Vengono di seguito illustrate in sintesi.

Soluzione	Compatibilità VPN	Ambito d'mpiego consigliato	Livello di sicurezza	Impatto tecnico sulle postazioni	Impatto tecnico sugli utenti
One time password hardware (OTP)	Sì	Utente remoto con accesso ad applicazioni Web/VPN	Alto	Nessuno*	Medio
One time password software (OTP)	Sì	Utente remoto mobile con notebook, PDA, SmartPhone, palmare aziendale	Medio-alto	Alto	Alto
Digital ID	Sì	Utente locale o remoto con accesso ad applicazioni Web/VPN	Medio	Medio-alto	Basso
Smart Card/Token	Sì	Utente locale con postazione aziendale. Utente remoto con desktop/notebook aziendale	Medio-alto	Alto	Medio
Biometria	Poco diffusa	Utente locale con postazione aziendale	Alto	Alto	Alto

*Qualora l'utilizzo sia circoscritto ad applicazioni Web o a soluzioni compatibili.

Tabella 5-2- Quadro sinottico delle tecnologie di autenticazione forte

One time password (OTP)

I sistemi OTP sono basati sulla generazione di una password dinamica (normalmente ogni 60 secondi) associata ad un PIN conosciuto dall'utente. L'algoritmo che genera la password è casuale ed è pertanto altamente improbabile che i numeri generati possano ripetersi più di una volta. L'utente è dotato di un dispositivo con software, normalmente tascabile, che genera la password. Le credenziali vengono verificate da un server di autenticazione che applica lo stesso algoritmo, sincronizzato con il dispositivo in possesso dell'utente. La connettività con tale server deve essere garantita durante il processo di autenticazione. Questi sistemi, quando usati per l'accesso alle applicazioni Web o combinati ad un RAS, non necessitano di alcuna componente software sul client e sono, pertanto, particolarmente adatti lad-

dove non sia possibile controllare la configurazione del desktop che accede (postazioni di terze parti). Il livello di sicurezza raggiunto da questi sistemi è elevato, sebbene esistano tecniche sofisticate per aggirarli.

Figura 5-9 - Dispositivi OTP

Certificati digitali

L'utilizzo dei certificali digitali per l'autenticazione degli utenti è normalmente associato ad un client VPN (IPsec o SSL) o ad un browser Web attraverso l'utilizzo del protocollo SSL 3. Il certificato digitale deve essere emesso da una CA (Certification Authority) privata o pubblica (si veda il precedente paragrafo 5.1.8). Durante l'accesso

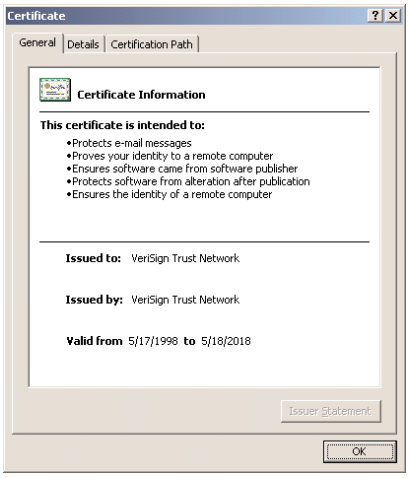


Figura 5-10 - Certificato digitale

viene verificato che la firma apposta sul certificato sia valida, attraverso il confronto con il certificato della **CA root** che l'ha firmato. In alcuni casi è possibile verificare altri parametri presenti nel certificato. Per questo motivo entrambi i certificati devono essere residenti sul client che effettua l'accesso. Il certificato utente può risiedere alternativamente anche su una smart card (conformemente al protocollo PKCS11) e rimosso con l'asportazione della stessa. I livelli di sicurezza sono elevati, anche se il certificato digitale deve essere conservato con cura. L'impatto tecnico sulle postazioni è abbastanza elevato, in quanto il certificato deve essere consegnato all'utente ed installato nel client (browser o altro client che effettua l'accesso) unitamente a quello della CA che l'ha emesso. Per un elevato numero di utenti è necessario implementare una Public Key Infrastructure (PKI) che può richiedere personale dedicato per garantirne la funzionalità.

Smart Card/Token

L'utilizzo di **smart card** e **token** è normalmente funzionale all'utilizzo di altre tecnologie, quali password dinamiche o certificati digitali, memorizzati su di essi. Il loro impiego richiede la presenza di determinati pre-requisiti tecnici, come lettori dedicati o periferiche USB. Per questi motivi sono generalmente adottati per le postazioni aziendali (desktop o notebook) di cui è possibile controllare completamente la configurazione. L'utilizzo può essere associato a più ambiti, dall'autenticazione alla firma digitale, alla crittografia dei dati. L'impatto tecnico è elevato ed il livello di sicurezza dipende fortemente dalla soluzione di mercato adottata.

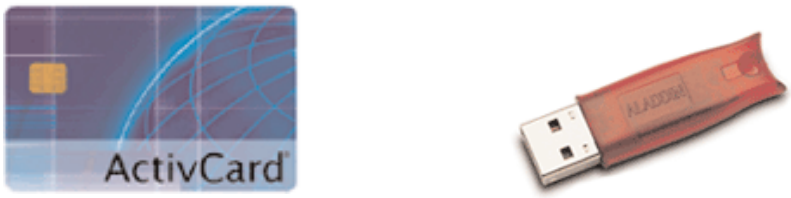


Figura 5-11 - Smart Card e Token USB

Biometria

La **biometria** utilizza, ai fini dell'identificazione dell'utente, parametri biologici o comportamentali specifici. Qualunque sia la tecnica adottata, dalla lettura delle impronte digitali al riconoscimento del volto, alla scansione della retina o altro è necessaria una forte collaborazione da parte dell'utente da autenticare. Inoltre, per completare la fase di registrazione iniziale (**enrollment**), è necessario il coinvolgimento iniziale di tutti gli utenti. Il loro impiego è solitamente circoscritto alle postazioni aziendali ed è poco indicato per l'utilizzo da parte di utenti remoti. L'impiego di dispositivi e lettori specifici causa un impatto tecnico elevato, rendendo difficile l'integrazione con soluzioni di accesso remoto.

Figura 5-12 - Tecniche biometriche

5.1.11 User provisioning

Il costante incremento degli accessi agli asset aziendali da parte di un bacino d'utenza sempre più eterogeneo ha aumentato notevolmente la complessità del processo di gestione delle utenze.

In ambienti particolarmente vasti e complessi operazioni di **creazione**, **dismissione** o **modifica** di un'utenza possono richiedere un dispendio notevole di energie in termini di risorse umane e temporali. Considerando, inoltre, che il processo di autenticazione costituisce un aspetto fondamentale per garantire la sicurezza delle informazioni, sul quale spesso si basano tutti gli altri, è fondamentale gestire in maniera efficace e tempestiva l'**identità elettronica** degli utenti.

I modelli di Identity Management (IdM) saranno discussi più oltre, nel paragrafo 5.2.2. Di seguito si accenna a due funzioni chiave di supporto, che intervengono in una soluzione IdM, il **provisioning** ed il **deprovisioning**.

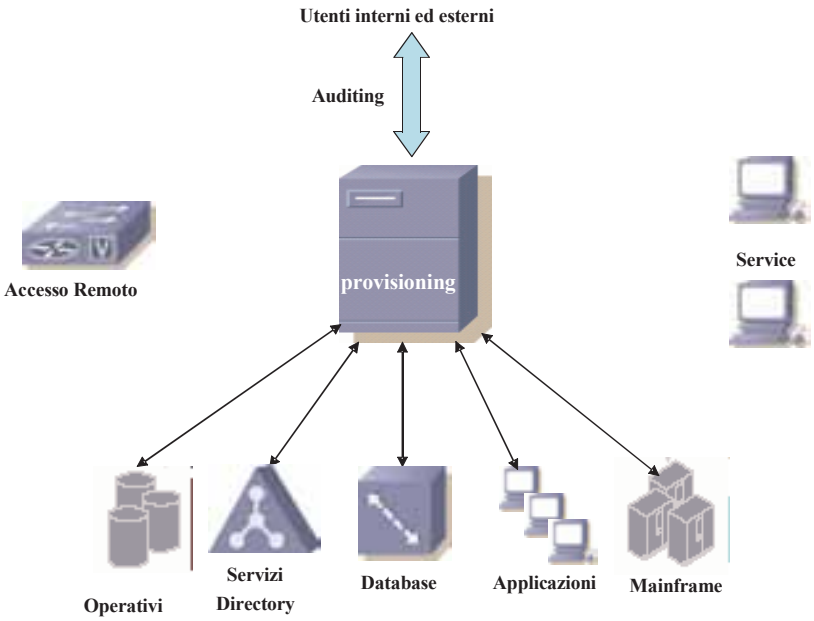


Figura 5-13 - Architettura di "Provisioning" per un sistema di Identity Management

La prima funzione si occupa di tutti gli aspetti legati alla creazione ed alla gestione del profilo utente, mentre la seconda si occupa della dismissione o sospensione degli utenti. Naturalmente quando parliamo di profili li intendiamo associati a svariati sistemi ed applicazioni a cui l'utente ha necessità di accedere e per i quali una gestione manuale e puntuale richiederebbe uno sforzo non accettabile. Le piattaforme software specifiche oggi sul mercato automatizzano e razionalizzano i due processi.

5.2 MISURE ORGANIZZATIVE E DI PROCESSO

5.2.1 Disaster Recovery e Business Continuity

Premesse e terminologia

Questa sezione illustra i punti salienti relativi alla continuità dei servizi ICT di cui le reti costituiscono un fattore abilitante, con l'obiettivo di inquadrare la tematica rispetto ai benefici, alle opportunità, ai costi e all'ambito di applicabilità.

La definizione formulata dal British Standards Institute (BSI©) per il concetto di Business Continuity Management è la seguente: *"processo di gestione olistico che identifica i potenziali impatti che minacciano un'organizzazione e definisce un approccio per realizzare la resilienza e la capacità di una risposta efficace che protegga gli interessi degli stakeholders*[1] *rilevanti, la reputazione, il marchio e le attività a valore aggiunto"*[2].

Nell'ambito del processo di Business Continuity Management quello di pianificazione e gestione del Disaster Recovery rappresenta la componente tecnologica dell'intero processo e costituisce l'argomento specifico di questa sezione.

Le fasi del piano di Disaster Recovery

Lo sviluppo di un piano di Disaster Recovery segue generalmente un percorso articolato nelle seguenti fasi.

Fase 1 - Classificazione dei processi critici

Il punto di partenza per lo sviluppo del piano di Disaster Recovery deve ravvisarsi nella prima fase del più complessivo proces-

---

[1] *Il termine sta ad indicare l'insieme di persone fisiche e giuridiche (azionisti ma non solo) che hanno relazioni con l'azienda e quindi interesse al buon andamento della stessa e alla trasparenza e correttezza della sua gestione.*

[2] *"holistic management process that identifies potential impacts that threaten an organization and provides a framework for building resilience and the capability for an effective response that safeguards interests of its key stakeholders, reputation, brand and value-creating activities".*

so di Business Continuity Management. Nel corso di questa fase si procede a definire il **perimetro di applicazione** del processo di gestione della continuità operativa e a classificare, per criticità decrescente, i diversi **processi** contenuti nel perimetro. La classificazione dei processi avviene in base al tempo massimo per cui è possibile tollerare la sospensione del processo (concetto di RTO, Recovery Time Objective). Normalmente si considera accettabile il principio per cui, per motivi economici, non è possibile garantire la continuità di tutti i processi. Si tratta quindi di individuare i processi di cui si deve garantire la continuità operativa.

Fase 2 - Definizione dei criteri e dei parametri del piano.

In questa fase, partendo dallo studio dei processi aziendali classificati, attraverso un'attività di correlazione dei processi inclusi nel piano con le relative applicazioni software, si perviene all'elencazione di tutte le **applicazioni informatiche** da includere nel piano di Disaster Recovery.

Fase 3 - Definizione dei requisiti del piano di Disaster Recovery.

Questa fase consiste nella definizione dei requisiti di fattibilità del piano in relazione agli obiettivi da perseguire e al perimetro d'intervento definito. In questa fase vengono forniti i criteri e le componenti strutturali del piano le quali, una volta discussi ed approvati dal management, consentono di procedere alle fasi realizzative successive su basi certe sia per quanto concerne le finalità, sia relativamente al contesto tecnico-organizzativo da considerare, sia sul piano del vantaggio economico. Da questa fase ci si attende la definizione dei punti sotto indicati:

- modalità ed entità di utilizzo dei sistemi nella fase di Disaster Recovery, sia a livello di impegno di risorse elaborative e di gestione delle stesse, sia a livello utente
- architetture di sistema e di rete alternative
- fonti e soluzioni per il reperimento e la disponibilità di sistemi e reti alternative

- eventuali polizze assicurative
- interfacce, interscambi e/o interconnessioni tra i vari sistemi di procedure
- verifica delle procedure di back-up per le applicazioni incluse nel piano
- definizione della struttura organizzativa di gestione della crisi.

Fase 4 - Progettazione di dettaglio del piano.

Questa fase consiste nella definizione, a livello dettagliato, delle **procedure e delle regole comportamentali** da seguire, da parte del personale coinvolto, sia in fase di gestione corrente che al momento della dichiarazione della crisi e, conseguentemente, di attuazione del piano.

Fase 5 - Implementazione del piano.

In questa fase si procede alla **redazione finale delle procedure**, al consolidamento dell'organizzazione necessaria per attuarle, all'acquisizione delle risorse software, hardware e logistiche necessarie.

Fase 6 - Test pre-operativo.

Questa fase consiste nell'effettuazione del **collaudo** dell'intero piano, prima del rilascio a livello operativo, e della relativa attività di **formazione**.

Fase 7 - Test operativi periodici e aggiornamento.

La fase si concretizza nell'effettuazione di **esercitazioni** periodiche di attivazione parziale e/o totale del piano, nonché nella definizione e messa in pratica dei criteri per la **manutenzione** ordinaria e straordinaria dello stesso.

La scelta delle risorse alternative

Nella redazione di un piano di Disaster Recovery l'aspetto maggiormente impegnativo, accanto a quello della definizione della criticità dei processi e ad esso connesso, è quello relativo alla scelta del tipo di soluzione da preferire per la rete e per il sistema, nel suo complesso, alternativi.

Per quanto concerne la rete, la soluzione maggiormente praticabile è quella di prevedere una soluzione alternativa, generalmente capace di gestire un traffico ridotto, rispetto al regime ordinario, con il fornitore abituale. Tale soluzione, evidentemente, deve prevedere nodi e instradamenti realmente indipendenti da quelli originari, che non siano soggetti a patire gli stessi eventi che dovessero danneggiare la rete originale.

Per quanto concerne gli altri componenti di sistema (host, server, workstation ecc.) e la relativa logistica, esistono, come è noto, soluzioni diverse, caratterizzate, in generale, dal fatto di avere costi crescenti quanto più bassi sono i tempi necessari per l'attivazione.

La figura che segue mostra, sinteticamente, le soluzioni possibili. Si chiarisce la terminologia utilizzata, ancorché ampiamente utilizzata.

Per **cold site** s'intendono locali con arredamento generico, ma senza apparecchiature e connessioni di rete. Per **warm site** una situazione parzialmente attrezzata: ad esempio con connessioni a rete esterna, ma priva di server e work-station. Per **hot site** s'intendono locali completamente attrezzati, con relativa rete interna ed esterna. **Mirroring** è un hot site in cui l'aggiornamento degli archivi avviene in tempo praticamente reale (al massimo con alcuni minuti di ritardo) rispetto al sito di elaborazione principale.

Da quanto sopra consegue che l'individuazione ottimale della soluzione delle risorse alternative impone un'accurata analisi della criticità dei processi inclusi nel piano di Disaster Recovery, considerando che i costi relativi possono variare considerevolmente. Quindi la definizione di soluzioni di disaster recovery dovrebbe poggiare sulla elaborazione di una opportuna strategia, seguita da studi di fattibilità che permettano l'identificazione delle migliori soluzioni per l'ottimizzazione dei costi e dei benefici.

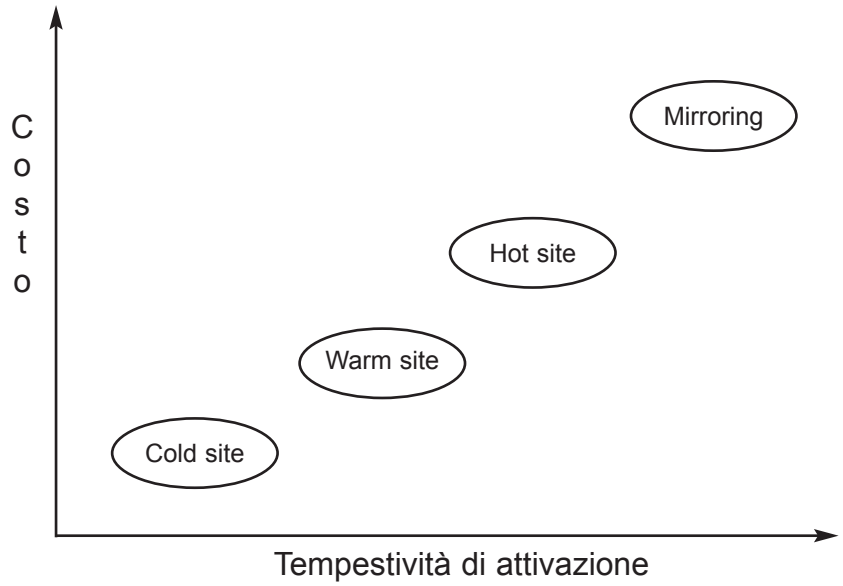


Figura 5-14 - Diagramma delle soluzioni alternative, per costo e tempestività di attivazione

5.2.2 Identity Management

A volte si presume che il principale obiettivo di un sistema di gestione della sicurezza delle informazioni sia **solo** quello di escludere accessi **esterni** non autorizzati ai sistemi informativi. Di conseguenza gli sforzi si dirigono verso attività di protezione dei perimetri di rete e relativi apparati informatici.

Nella realtà i rischi si presentano, in ugual misura, all'**interno** delle organizzazioni oppure dall'esterno, ma attraverso l'ambito applicativo interno alle organizzazioni. Allo stesso tempo aumenta la richiesta di nuove applicazioni che consentano di estendere l'accesso ad una più vasta e varia moltitudine di utenti, spesso sconosciuti, quali business partner, fornitori, agenti, clienti e dipendenti.

Una soluzione per la gestione di rischi che incombono sulle informazioni si trova nei concetti di **Identity Management** (IdM), un termine definito per la prima volta in un white paper sviluppato con-

giuntamente da PricewaterhouseCoopers e Gartner Group[4], oggi largamente utilizzato. L'IdM è una convergenza di tecnologie e processi di business. Non c'è un singolo approccio poiché la strategia deve riflettere requisiti specifici all'interno del contesto tecnologico e di business di ogni specifica organizzazione. L'obiettivo generale è quello di **fornire validi accessi alle persone giuste nel momento giusto**.

Le categorie funzionali previste dall'IdM per la classificazione di tutti gli elementi tecnologici, organizzativi e di processo sono: **autenticazione**, **controllo degli accessi**, **gestione delle utenze e servizi di directory**.

L'**autenticazione** è un meccanismo che consente di effettuare transazioni, con diversi livelli di sicurezza, con la certezza dell' identità delle parti in causa.

Meccanismi di autenticazione sono ad esempio:

- user name e password
- personal identification number (PIN)
- certificati digitali
- token
- dispositivi biometrici
- smart card.

Dal punto di vista organizzativo e di processo è necessario **definire i ruoli** ed analizzare i rischi ai fini di identificare **chi** deve avere accesso a **che cosa**.

Il **controllo degli accessi** assicura che gli utenti abbiano accesso solamente a quelle applicazioni o risorse che sono abilitati a utilizzare. Questa infrastruttura è anche conosciuta con il nome di

---

4 "Identity Management: The business Context of Security." Whitepaper © 2001 PricewaterhouseCoopers LLP, Interviews & case studies © 2001 Gartner, Inc.

Privilege Management Infrastructure (PMI).

Le principali caratteristiche di questa infrastruttura sono:

- un'infrastruttura comune per l'autenticazione e l'autorizzazione all'uso di molteplici applicazioni
- utilizzo di piattaforme di Single Sign On per l'accesso alle applicazioni
- definizione dei ruoli (role based access control)
- monitoraggio degli accessi.

La **gestione delle utenze** è il termine utilizzato per definire tecnologie e processi che consentono di gestire un elevato numero di utenze. **User provisioning** è un altro termine usato per definire quest'ambito (vedi paragrafo 5.1.11).

Le principali funzioni delle tecnologie e dei processi di gestione delle utenze sono:

- automazione dei processi di workflow per creare partecipanti e dare loro accesso a tutte le applicazioni di cui necessitano per svolgere il loro lavoro (provisioning)
- rimozione automatica delle utenze cessate (deprovisioning)
- conferimento di un elevato grado di **autonomia controllata** agli utenti
- delega delle funzionalità di amministrazione degli accessi.

I **servizi di directory** consentono di gestire gli accessi alle directory. Una directory è un elemento software che immagazzina informazioni. L'accesso avviene di solito tramite il protocollo denominato **Lightweight Directory Access Protocol** (LDAP). L'evoluzione delle tecnologie estende il concetto alle Meta Directory ed alle Virtual Directory: queste ultime tendono ad evitare le duplicazioni mantenendo dei puntatori per reperire l'informazione, senza crearne una copia.

Le principali caratteristiche dei servizi di directory sono:

- archivio centralizzato, flessibile e sicuro per il profilo degli utenti

- scalabilità fino a molti milioni di utenti
- capacità di rilasciare rapide risposte a centinaia di domande al secondo
- integrazione basata sugli standard per le principali applicazioni.

I benefici nella corretta e completa implementazione di una soluzione di Identity Management includono:

- integrazione delle tecnologie
- costi di gestione più bassi
- aumento della produttività
- automazione dei processi
- maggiore efficienza complessiva
- conferimento di **autonomia controllata** a clienti, dipendenti, fornitori e partner
- maggiore protezione dei dati aziendali
- integrazione delle regole di conformità (privacy e altro)
- sicurezza **attiva e consapevole**
- definizione dei profili di accesso **razionale e organizzata**
- auditing costante.

5.2.3 Gestione operativa della sicurezza

Generalità

Da sempre si è riconosciuto ad ogni contromisura una efficacia limitata nel tempo, sia a causa di malfunzionamenti che possono verificarsi nei meccanismi di protezione, sia a causa della scoperta di nuove vulnerabilità e dell'insorgere di nuove minacce; solo ultimamente, tuttavia, questo concetto è entrato a pieno titolo nelle definizioni e negli obiettivi della sicurezza.

Ogni sistema di contromisure, pertanto, deve essere affiancato

dalla capacità di prendere conoscenza delle nuove vulnerabilità e delle nuove minacce. Inoltre, qualora malauguratamente, nonostante l'esistenza di una efficace infrastruttura di protezione, dovessero verificarsi incidenti, è indispensabile la capacità di rilevare tempestivamente gli stessi e di gestirli correttamente.

Questi due aspetti sono spesso denominati **Real Time Security Monitoring** ed **Incident Handling**. In questo contesto, la parola **monitoraggio** assume il significato di rilevazione degli incidenti, da non confondersi con il monitoraggio che viene effettuato su sistemi e reti ai fini di controllarne la corretta operatività.

Troviamo traccia di questo approccio su numerosi documenti di sicurezza nazionali ed internazionali degli ultimi anni, ma è solo ultimamente, con la crescita del numero degli attacchi e degli incidenti di sicurezza, che si è riconosciuta l'indispensabilità di queste funzioni.

Già nella Direttiva del Presidente del Consiglio dei Ministri del 16.1.2002, meglio conosciuta come Direttiva Stanca, venivano introdotti i concetti di **gestione degli incidenti e controllo e monitoraggio della sicurezza**.

Il Ministero per l'Innovazione Tecnologica ed il Ministero delle Comunicazioni hanno prodotto il già citato documento intitolato *"Proposte concernenti le strategie in materia di sicurezza informatica e delle telecomunicazioni per la Pubblica Amministrazione"*, pubblicato nel marzo 2004, in cui si trattano i concetti di monitoraggio e gestione degli incidenti promuovendo l'istituzione di funzioni di rilevamento delle attività di sicurezza tramite il monitoraggio attivo, di gestione degli incidenti informatici e di notifica delle minacce (early warning).

Inoltre il CNIPA sta perseguendo il piano di avviamento del **govcert.it**, organo di coordinamento e supporto agli **Incident Reponse Team** che andranno a formarsi all'interno della Pubblica Amministrazione.

Nel campo delle indicazioni internazionali, l'Information Security Forum ha fatto proprio l'approccio descritto costruendo attorno a questo una metodologia di gestione del rischio denominata FIRM, la quale, nelle sue prime pagine, definisce la sicurezza l'insieme di tre aree: la **prevenzione dagli incidenti**, la **rilevazione degli incidenti** e la **risposta**[5].

Ad oggi, il monitoraggio in tempo reale della sicurezza non è realizzabile attraverso la semplice acquisizione di strumenti tecnologici, nonostante il mercato proponga numerosi prodotti destinati a questo scopo. Occorre, in aggiunta, la capacità di avviare correttamente alcuni processi chiave del ciclo della sicurezza. Le componenti che determinano la qualità e l'efficacia di tali processi sono:

- **copertura temporale:** le nuove minacce si diffondono nell'arco di qualche minuto, indipendentemente dall'ora e dall'area geografica. Il monitoraggio deve avvenire 24 ore su 24, 365 giorni all'anno, in modo continuativo ed in tempo reale. A titolo indicativo, per un turno completo di 24 ore sono necessarie dalle 6 alle 10 persone
- **conoscenza:** l'analisi di eventi di sicurezza richiede un livello di competenza molto elevato che va mantenuto nel tempo. L'analisi di minacce che si manifestano per la prima volta nonché l'individuazione delle corrette procedure di gestione dell'incidente richiedono conoscenze molto specifiche sulle tecnologie impiegate presso l'organizzazione, nonché una forte esperienza nell'analisi di sicurezza
- **knowledge base:** l'accesso ad una knowledge base di sicurezza è fondamentale per consentire l'attività di analisi degli incidenti e la determinazione delle procedure di gestione dell'incidente
- **rilevazione e risposta agli incidenti:** poiché l'attività di rilevazione, come quella di risposta, si fondano sull'attività di persone, è fondamentale disporre di corretti processi di gestione e di piattaforme tecnologiche a supporto. È buona regola che i processi legati alla rilevazione e alla risposta agli incidenti siano conformi a standard internazionali riconosciuti, come il BS 7799
- **tecnologia:** esistono numerose piattaforme hardware/software per supportare le funzioni di monitoraggio e di risposta agli incidenti:

[5] *Vedi Allegato 2.2*

- sistemi di centralizzazione dei log
- sistemi di tracciatura degli incidenti
- sistemi di trouble ticketing
- sistemi per la realizzazione di portali di sicurezza
- sistemi centralizzati per il controllo e la gestione della sicurezza.

Il mercato offre diversi servizi per supportare l'adeguamento della conoscenza di nuove minacce e vulnerabilità come pure l'avviamento e la gestione di processi di rilevazione e risposta agli incidenti, di seguito descritti.

Managed Security Services

Sotto il nome di Managed Security Services (o MSS) ricadono due categorie di servizi molto differenti tra di loro:

- Security Management
- Real Time Security Monitoring.

Security Management

I servizi di gestione offerti da un Managed Security Service Provider (MSSP) hanno la finalità di fornire, sotto forma di servizio esterno, la gestione ordinaria e straordinaria degli apparati di sicurezza. In particolare, i dispositivi di sicurezza sono gestiti nei tre aspetti seguenti:

- gestione di guasti ed errori (fault management)
- gestione della configurazione (configuration management)
- gestione della performance (performance management).

Il **fault management** consiste nel gestire i dispositivi di sicurezza dei clienti in modo che questi funzionino sempre regolarmente. Questo risultato viene solitamente - ma non sempre - raggiunto attraverso un servizio esteso sull'arco 24x7. Alcuni servizi tipici della

gestione dei guasti includono:

- un checkup periodico dei dispositivi di sicurezza per far emergere possibili problemi
- la notifica ai clienti ogni volta che (per qualsiasi ragione) il dispositivo di sicurezza cessa di funzionare e un servizio di orientamento/guida circa le misure appropriate per rimediare al problema
- l'invio ai clienti di rapporti periodici che ricapitolano la situazione operativa dei dispositivi di sicurezza su un arco temporale stabilito.

Attraverso il **configuration management** il cliente delega a un MSSP la configurazione dei propri dispositivi di sicurezza. Il responsabile della gestione della configurazione normalmente si fa carico dei seguenti aspetti:

- modifiche e aggiornamenti (upgrade) delle applicazioni a supporto dei dispositivi di sicurezza, nonché dei sistemi operativi
- modifiche alle politiche (policy) e alle firme applicate ai dispositivi di sicurezza
- rapporti quotidiani, settimanali, o mensili che elencano tutti i nuovi aggiornamenti e le modifiche ai dispositivi di sicurezza dei clienti.

Il **performance management** comporta la raccolta e la presentazione di statistiche delle prestazioni registrate sui dispositivi di sicurezza del cliente. Il contenuto di tali rapporti include:

- statistiche sulla velocità ed efficienza riscontrate nella rete del cliente
- l'identificazione di **colli di bottiglia** interni alla rete che ne penalizzano il rendimento
- rapporti relativi alla performance complessiva, che consolidano tutti i dati di log generati dai dispositivi di sicurezza del cliente.

Real Time Security Monitoring

Il monitoraggio della sicurezza richiede un elevato grado di competenza nell'ambito della sicurezza e un'architettura sofisticata che aiuti ad analizzare i dati su molteplici dispositivi attraverso un'organizzazione globale.

Per i servizi di monitoraggio offerti dagli MSSP il termine **outsourcing** dev'essere inteso con cautela: i servizi offerti dall'esterno non vanno a sostituirsi al controllo interno ed in ogni caso la **cabina di regia** della sicurezza rimane all'interno dell'organizzazione. I servizi esterni vanno considerati come un utile supporto alla rilevazione degli incidenti.

I servizi di Real Time Security Monitoring sono costituiti dalle seguenti funzioni:

- raccolta e normalizzazione dei dati
- data mining
- correlazione automatizzata degli eventi correlati con la sicurezza
- risposta agli eventi
- reportistica degli eventi.

La **raccolta e normalizzazione dei dati** è un processo nel quale i dati legati ai dispositivi di sicurezza (log di firewall, alert IDS ecc.) sono raccolti e trasformati in un formato standard e indipendente dal tipo e dal produttore del dispositivo. Normalizzare i dati è essenziale per un monitoraggio efficace della sicurezza, poiché consente agli MSSP di utilizzare un insieme di interrogazioni standard per analizzare i dati dei dispositivi di sicurezza e isolare le tracce di attività pericolose.

Il processo di **data mining** prevede che un sistema automatizzato lanci costantemente interrogazioni verso i dispositivi di sicurezza per identificare i segni di attività pericolose, separando quindi il traffico di rete sospetto da quello legittimo. Questo è probabilmente l'elemento tecnologico centrale nel processo di monitoraggio: a questo proposito un cliente deve accertarsi che un MSSP sia in grado di sca-

lare le proprie capacità in termini di data mining all'aumentare dei dispositivi collegati all'architettura di back end. In altre parole, l'MSSP dev'essere in grado di sviluppare **query** sempre più sofisticate a mano a mano che nuovi dispositivi si aggiungono alla rete. Ma aumentare il numero delle interrogazioni non equivale necessariamente a migliorare il processo di data mining. In questo settore sono estremamente importanti la qualità delle interrogazioni e il loro continuo affinamento, così come la creazione tempestiva di nuove interrogazioni capaci di far emergere attività nocive in continua evoluzione. Solo grazie a processi di data mining molto sofisticati un MSSP può assicurare correlazioni efficaci tra dati e attacchi.

Un altro componente essenziale di un servizio di monitoraggio davvero efficace è la **correlazione automatizzata degli eventi connessi alla sicurezza**, cioè il raggruppamento automatico di specifiche tracce di attività nocive in base a criteri logici come fonte, tipo e destinazione dell'attacco. Il risultato di questo processo è la rapida ricostruzione degli attacchi, che consente agli analisti di visualizzare l'attacco nella sua interezza. Senza correlazione automatica, gli analisti della sicurezza sono costretti a ricucire insieme le sequenze dell'attacco facendo scorrere manualmente milioni di linee di dati registrati dai dispositivi di sicurezza. Persino sulle reti che sperimentano ridotti volumi di traffico questa operazione è chiaramente troppo dispendiosa in termini di tempo impegnato, oltre che complessa da gestire a qualsiasi livello di scalabilità.

La **risposta agli eventi** che hanno ricadute sulla sicurezza segue e dipende dall'esame dei dati - generati dal processo di correlazione - compiuto dagli analisti della sicurezza. In base alla natura dell'evento, la gamma di azioni può variare dalla semplice notifica al cliente fino alla comunicazione immediata dell'evento alle competenti autorità di polizia. La disponibilità di un servizio di analisi degli eventi della sicurezza compiuto da tecnici esperti sull'intero arco temporale (24x7) è un elemento decisivo per ogni servizio di sicurezza gestito.

La **reportistica degli eventi** è il processo adottato per notificare ai clienti gli eventi con impatto sulla sicurezza identificati sulla loro rete. In base alla natura dell'evento, i report possono essere trasmessi sotto forma di comunicazioni vocali immediate, oppure come

e-mail o notifiche in tempo reale pubblicate su un portale Web o, ancora, attraverso rapporti periodici.

Di norma, i servizi di monitoraggio vengono offerti per quelle piattaforme di sicurezza che forniscono informazioni significative sugli eventi (firewall, host e network intrusion detection system, ecc.).

Per offrire un efficace monitoraggio in tempo reale della sicurezza, un MSSP deve possedere tutte le caratteristiche sopra elencate. Protezione dalle vulnerabilità, riconoscimento e gestione in tempo reale dei rischi per la sicurezza in rete rappresentano risultati impossibili da raggiungere se uno solo di questi servizi viene a mancare.

È dunque la disponibilità di competenze professionali di alto livello unitamente ad un'architettura tecnica complessa capace di analizzare i dati su molteplici dispositivi a livello globale, che separa la gestione della sicurezza dal **semplice** monitoraggio. Un aspetto, questo, già evidenziato nell'articolo *"Top Guns"* apparso nella rivista **Information Security**: *"Il software per la sicurezza ha compiuto grandi passi in avanti nella capacità di consolidare, correlare e analizzare gli eventi e i log dei dati di molteplici dispositivi come firewall, IDS e router. Ma gli specialisti nelle postazioni di controllo dei SOC (Security Operations Center) degli MSSP affermano che quando si tratta di analizzare eventi con ricadute sulla sicurezza, l'intuizione, per quanto antico, resta lo strumento più affidabile"*[6].

Early warning

Gli incidenti di sicurezza che per numero e frequenza più hanno colpito le organizzazioni di tutto il mondo sono quelli derivanti da minacce esterne, quali **virus**, **worm** e altre forme di codice malevolo. Queste minacce, definite **globali** poiché colpiscono indiscriminatamente organizzazioni di tutto il mondo, non sono studiate per attaccare un'organizzazione specifica, anche se ultimamente sono divenute un veicolo per perpetrare attacchi mirati sfruttando le vulnerabilità tecniche esistenti ed approfittando del calo delle difese che le organizzazioni subiscono nel momento dell'emergenza.

---

[6] *R. Thieme, A. Briney - "Top Guns" in "Information Security", Agosto 2002.*

Tutti gli ultimi episodi famosi (Blaster, My Doom, Sasser, ecc.) hanno dimostrato come dal momento in cui è avvenuto il primo attacco al momento in cui è stata raggiunta la massima diffusione, il tempo trascorso è stato di poche ore.

Questo dato, unitamente al fatto che ad oggi non è possibile ragionare in ambienti completamente privi di vulnerabiltà, evidenzia la necessità di adottare strategie di tipo preventivo e proattivo.

I cosiddetti servizi di **early warning** o notifica preventiva possono aiutare le organizzazioni a conoscere in anticipo vulnerabilità e minacce emergenti e adottare le corrette contromisure per contrastare il fenomeno prima che questo colpisca l'organizzazione.

I servizi di early warning si dividono in due categorie:

- **notifica delle vulnerabilità:** attraverso questo servizio, l'organizzazione viene preavvertita ogni qual volta una nuova vulnerabilità viene scoperta. Poiché la mole di vulnerabilità scoperte ogni giorno è molto consistente, i servizi più avanzati permettono di ricevere esclusivamente la notifica di vulnerabilità relative alle tecnologie ed ai prodotti installati nell'organizzazione. Esistono anche servizi gratuiti, nella forma di mailing list, che però non garantiscono nessuna tempestività di segnalazione, né permettono di selezionare quali notifiche ricevere
- **notifica delle minacce:** la vulnerabilità, in se stessa, non è sufficiente per costituire un rischio per l'organizzazione. È l'esistenza di tecniche e metodi per lo sfruttamento della vulnerabilità a rendere possibile il suo impiego per attacchi e violazioni. I servizi di notifica delle minacce sono in grado di rilevare tempestivamente l'esistenza di attività in grado di sfruttare una vulnerabilità e di inviare una notifica alle organizzazioni aderenti. Al momento non esistono numerosi servizi di notifica delle minacce, poiché per la loro erogazione il fornitore deve disporre di una rete di analisi in tempo reale e di intelligence di dimensioni molto importanti, in grado di catturare immediatamente i primi segni di sfruttamento di una vulnerabilità.

  Unitamente alla segnalazione della nuova minaccia, i fornitori

di servizi di **early warning** forniscono una descrizione dettagliata del fenomeno, quali sistemi sono vulnerabili, il possibile impatto, i metodi di propagazione e le azioni suggerite per mitigare o annullare il rischio.

Incident handling

Tutte le infrastrutture di sicurezza, persino le migliori, non sono in grado di fornire una **garanzia assoluta di protezione** del sistema informativo. Sebbene negli ultimi anni gli strumenti per il miglioramento della sicurezza abbiano fatto enormi progressi, la loro efficacia è sempre limitata e comunque non assoluta. Conseguentemente è necessario poter disporre di opportune strutture per la gestione di tutti quegli eventi (incidenti, frodi, attacchi, malfunzionamenti, ecc.) che minacciano la continuità dei servizi e le informazioni.

Questa struttura organizzativa, normalmente denominata CERT (**Computer Emergency Response Team**), è responsabile della ricezione, analisi e gestione degli incidenti che riguardano la sicurezza informatica. Essa, inoltre, ha il compito di coordinare e seguire numerose attività fondamentali per garantire livelli di sicurezza adeguati per l'organizzazione

Attraverso l'attivazione del CERT, l'organizzazione sarà in grado di gestire in modo centrale tutti gli incidenti. In particolare, l'attivazione di un CERT consentirà all'organizzazione di:

- ottimizzare le risorse, i tempi, i costi e gli strumenti impiegati per la gestione degli incidenti attraverso la centralizzazione e il coordinamento delle attività
- salvaguardare il proprio patrimonio informativo, preservandone la riservatezza, l'integrità e la disponibilità, anche in conformità alle disposizioni per la tutela della privacy
- ridurre l'occorrenza e la probabilità di accadimento degli incidenti mediante attività di monitoraggio e prevenzione
- conoscere costantemente lo stato della sicurezza del proprio sistema informativo.

Poiché l'attivazione di un CERT è una attività molto complessa e prolungata è consigliabile rivolgersi a società specializzate in grado di fornire consulenza per

- definire il modello organizzativo
- disegnare l'architettura tecnologica del security operation center che ospiterà il CERT
- avviare il CERT e definire i processi e le procedure
- fornire risorse specializzate per la formazione del personale e per la gestione degli incidenti
- fornire servizi di supporto (real time security monitoring, early warning).

Help desk specialistico

I servizi di help desk specialistico sono molto utili in quanto forniscono, al momento del bisogno, il supporto e la competenza necessaria per la risoluzione di problemi/incidenti. Esistono numerosissimi servizi di help desk e supporto specialistico. Molto spesso, gli stessi produttori di tecnologie di sicurezza offrono servizi di supporto, ma nella maggior parte dei casi sono limitati alle loro piattaforme.

Riportiamo alcuni fattori da considerare al momento dell'acquisizione di un servizio di help desk di questo tipo:

- copertura oraria (orario lavorativo o h24)
- tipologia di supporto (base o specialistico)
- conoscenze richieste
- presenza di personale certificato sui prodotti impiegati dall'organizzazione
- modalità di gestione dei ticket rispetto al livello di gravità della chiamata
- procedure di sicurezza
- livelli di servizio
- presenza di portale (informativo o interattivo).

Verifica periodica della sicurezza

La verifica periodica del livello di sicurezza offerto dal sistema informativo è una buona prassi suggerita dalla quasi totalità delle indicazioni nazionali ed internazionali sulla sicurezza.

Al momento, non esistono standard consolidati e metodologie per la conduzione degli assessment: ogni fornitore ha sviluppato la propria metodologia, basata su strumenti di mercato, open source o sviluppati internamente.

Per queste ragioni, a parità di denominazione, le offerte presenti sul mercato possono differire notevolmente.

Riportiamo un elenco delle attività più comuni:

- **Vulnerability Assessment:** si tratta della verifica delle vulnerabilità presenti sui sistemi oggetto dell'analisi. Questa verifica viene effettuata attraverso strumenti, denominati **scanner**, che analizzano sistema per sistema alla ricerca di vulnerabilità conosciute. Il risultato di questa attività è un elenco delle vulnerabilità sistemistiche rilevate, suddivise per gravità
- **Penetration Test:** scopo del Penetration Test, anche denominato Ethical Hacking, è analizzare le vulnerabilità presenti sui sistemi e tentare di sfruttarle per verificare la violabilità del sistema. L'attività è svolta da un gruppo di esperti di sicurezza spesso denominato **Tiger Team**, il quale utilizza tecniche di hacking per rilevare ogni punto debole del sistema.

  I Penetration Test posso essere eseguiti in modalità:
  - **blind:** al Tiger Team non vengono fornite informazioni sul sistema da analizzare, sarà compito del team individuare tutte le informazioni necessarie per effettuare l'analisi
  - **overt:** al Tiger Team vengono fornite quante più informazioni possibili sul sistema da analizzare, al fine di permettere loro una analisi più dettagliata possibile.

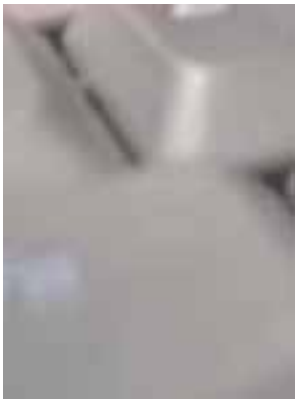
Penetration Test possono essere effettuati da remoto, ma solo sui server visibili attraverso le connessioni Internet. Per l'analisi dei sistemi interni, l'attività deve essere condotta all'interno dell'organizzazione.

- **Policy Assessment:** è l'attività di verifica delle policy dell'organizzazione e della loro corretta implementazione sui sistemi e sulle applicazioni. Di norma, questa attività viene condotta attraverso l'uso di strumenti specifici per la lettura e l'analisi delle policy configurate sui sistemi e sulle applicazioni. Le policy riscontrate sui sistemi vengono confrontate con le policy aziendali e con indicazioni e standard internazionali, nonché con **best practice**
- **Security Assessment:** è l'attività di verifica del piano di sicurezza di una organizzazione. Può essere fatta seguendo diversi riferimenti, tra cui il BS7799 e le best practice prodotte da organismi internazionali come l'Information Security Forum. Scopo del security assessment è rilevare le aree più a rischio e di fornire le indicazioni per impostare azioni correttive adeguate
- **Application Assessment:** è l'attività di verifica del livello di sicurezza offerto da alcune applicazioni, in particolare dalle applicazioni Web. Questa attività è estremamente utile per tutte quelle organizzazioni che dispongono di applicazioni Web critiche (transazionali) e che vogliono verificare il loro livello di sicurezza. Queste attività sono condotte con tecniche molto simili a quelle dei penetration test e devono essere svolte da personale altamente specializzato e con una provata esperienza in materia.

Dal momento che non esiste una modalità standard di erogare questa tipologia di servizi di verifica, per la valutazione delle diverse offerte presenti sul mercato, è opportuno verificare i seguenti aspetti:

- risultati finali: quali saranno i risultati finali dell'attività e come verranno presentati (documenti, incontro di discussione, ecc.)
- competenze: la qualità di questi servizi è fortemente legata alla competenza e all'esperienza dei consulenti che effettueranno l'analisi
- metodologia: dal momento che la maggior parte delle aziende che propongono servizi di assessment ha sviluppato una propria metodologia, è importante comprenderne i principi

- best practice: quando si valutano processi e modalità di gestione, la misurazione deve essere effettuata sulla base di indicazioni, linee guida, policy interne o best practice da individuare preventivamente
- sicurezza: i servizi di analisi della sicurezza richiedono che il fornitore abbia accesso ad informazioni riservate dell'organizzazione. È opportuno verificare con il fornitore quali procedure e quali strumenti di sicurezza verranno adottati per garantire la protezione delle informazioni di cui verrà in possesso
- strumenti: parte delle attività di verifica sono condotte con l'utilizzo di strumenti. Verificare con il fornitore quali strumenti verranno adottati, ed il loro livello di invasività e di impatto sull'infrastruttura dell'organizzazione. Verificare, inoltre, la possibilità di installare questi strumenti in modo definitivo all'interno dell'infrastruttura per agevolare eventuali verifiche future.



6 - Il governo della sicurezza nella PA e nelle aziende private

6.1 IL GOVERNO DELLA SICUREZZA COME FATTORE DI GARANZIA SOCIALE NELL'UTILIZZO DELLE RETI

Da alcuni anni il termine **governo** (in inglese **governance**) è stato introdotto per definire, relativamente ad un determinato processo che, al limite, può essere inteso come l'intero processo aziendale, quell'insieme di attività finalizzate ad assicurarne la corretta gestione, non solo ai fini dell'efficacia aziendale e del rispetto delle leggi, ma anche della garanzia degli azionisti e, più in generale, degli stakeholder[1]. Il termine implica, accanto a caratteristiche di creatività e raziocinio, anche una marcata componente etica.

Si potrebbe ipotizzare che l'esigenza di codificare la governance risponda a due necessità:

- la necessità di basarsi su un framework formale e condiviso per affrontare la complessità oramai insita nei processi odierni di business
- la necessità di utilizzare un modello concettuale rigoroso per rendere trasparenti anche agli stakeholder, non direttamente coinvolti nella gestione aziendale, i criteri di implementazione dei processi di governance.

[1] *vedi nota 1 del capitolo 5.*

Ovviamente, in una filiera di astrazione decrescente, la governance della sicurezza discende da quella dei sistemi ICT, che, a sua volta, fa parte del più ampio tema della **corporate governance**.

Tra le prime iniziative che hanno introdotto e sviluppato questi concetti occorre citare il progetto COSO[2] che ha supportato e prodotto, recentemente, con la collaborazione di Pricewaterhouse-Coopers, un documento intitolato *"Enterprise Risk Management - Integrated Framework"*. In questo documento vengono definite e illustrate, con un'enfasi sull'aspetto dell'analisi del rischio ma non solo, le componenti intese a costituire, nel loro insieme, l'edificio della corporate governance. Il medesimo comitato COSO aveva prodotto, agli inizi dello scorso decennio, un primo documento, con le medesime finalità, intitolato *"Internal Control - Integrated Framework"*.

Nel corso degli ultimi anni si sono verificati negli USA e in Europa (anche, com'è noto, nel nostro Paese) casi eclatanti di cattiva e fraudolenta gestione amministrativa dell'impresa, tali da giustificare, accanto ad iniziative **private** quali quella citata, iniziative specifiche del legislatore. Tra queste citiamo negli USA il *"Sarbanes-Oxley Act"* del 2002 ed, in Italia, la *"legge Draghi"* (D. lgs. 58/1998) e la più recente norma sulla riforma del diritto societario in vigore dal 1 gennaio 2004.

In specifici settori contribuiscono a enfatizzare gli obiettivi di corporate governance il codice di autodisciplina redatto dal Comitato delle società quotate dalla Borsa Italiana (conosciuto come *"Codice Preda"*, rivisto nel 2002) e, in ambito bancario, con valenza europea, il protocollo *"Basilea II"*.

Può essere interessante e costruttivo, in questa sede, analizzare quelli che possono considerarsi le componenti concrete e tangibili che concorrono a formare il concetto di governance della sicurezza, anche in un'ottica di fattibilità.

Proviamo ad elencarli di seguito, secondo uno schema che consente di ottenere una visione complessiva del governo della sicu-

---

[2] *COSO - The Committee of Sponsoring Organisations of the Treadway Commission - è un comitato costituitosi nel 1985 e tuttora vigente per iniziativa delle cinque maggiori organizzazioni professionali finanziarie USA, finalizzato a supportare la produzione di documenti e metodologie intese ad assicurare eticità, correttezza e trasparenza alla gestione ammnistrativa aziendale.*

rezza[3]:

- direzione strategica della sicurezza
  - promozione della sicurezza all'interno dell'organizzazione - la direzione aziendale deve essere direttamente impegnata nel supportare l'implementazione di un sistema di gestione della sicurezza e tale impegno deve essere chiaro e visibile all'interno e all'esterno dell'organizzazione
  - strategia per la sicurezza - una visione strategica di insieme per guidare le singole attività di realizzazione, mantenimento e miglioramento del sistema di gestione della sicurezza
  - ROI/indicatori di performance - un sistema di indicatori per la direzione aziendale che consenta di misurare il successo delle attività intraprese e del sistema posto in essere.
- piano per la sicurezza
  - definizione del piano di gestione delle singole attività nell'ambito di un programma di iniziative sinergiche
  - individuazione della disponibilità di risorse e competenze.
- linee guida per la sicurezza
  - le direttive, da quelle della direzione a quelle operative, le linee guida, le procedure per l'implementazione della sicurezza.
- gestione della sicurezza
  - gestione delle utenze e delle infrastrutture - processi e procedure per la gestione operativa e l'amministrazione della sicurezza
  - monitoraggio della sicurezza - monitoraggio e gestione degli incidenti volti ad assicurare il mantenimento della sicurezza
  - riservatezza - protezione della riservatezza delle informazioni.

---

[3] *Si tratta del "capability model" © di KPMG per il governo della sicurezza.*

- coordinamento con le funzioni di business
  - partecipazione degli utenti finali - coinvolgimento degli utenti finali nelle valutazioni che implicano la considerazione degli aspetti di business
  - consapevolezza degli utenti - il livello di consapevolezza degli utenti finali su responsabilità in essere e garanzie offerte dai diversi sistemi.
- sicurezza del patrimonio informativo
  - sicurezza applicativa
  - sicurezza dei data base e degli archivi
  - sicurezza dei server, delle workstation, dei desktop, ecc.
  - sicurezza della rete interna/esterna
  - antivirus
  - sviluppo dei sistemi.
- protezione della tecnologia e continuità
  - sicurezza fisica e protezione ambientale
  - disaster recovery - procedure e piani per la disponibilità e il ripristino dei sistemi.

Il buon governo della sicurezza dipende dalla presenza di tutte le componenti citate: un punto di debolezza in una di esse può comportare la mancanza di efficacia delle altre componenti (ad esempio, la mancanza di una guida strategica può comportare che linee guida e/o procedure di gestione siano incoerenti tra loro e, quindi una non corretta configurazione dei sistemi). Esiste, cioè, una sorta di interrelazione gerarchica, di causa ed effetto, tra ciascun livello del modello proposto e il livello successivo.

Preme inoltre sottolineare che le componenti citate sono solo parzialmente di natura tecnologica: il buon governo della sicurezza è un problema di natura gestionale, risolvibile attraverso una visione sinergica di persone, processi e tecnologie.

6.2 L'ATTUAZIONE DEL GOVERNO DELLA SICUREZZA NELLE ORGANIZZAZIONI

Il grado di formalizzazione ed estensione di ciascuna delle componenti descritte può chiaramente variare da realtà a realtà. Ed è

possibile applicare a ciascuna di essere il cosiddetto **maturity model**[4], cioè un modello concettuale, largamente utilizzato nell'ambito della valutazione dei sistemi di governance in senso ampio. Tale modello permette di valutare il grado di maturità di un determinato processo, assegnando allo stesso un punteggio da 0 a 5, secondo la scala che segue:

- attività totalmente assente - 0
- attività condotta in modo occasionale e non replicabile - 1
- attività svolta regolarmente e con modalità costanti - 2
- attività documentata in una procedura diffusa all'interno dell'organizzazione e svolta conformemente a tale procedura- 3
- attività documentata in una procedura con definizione di indicatori che consentono di monitorarne l'efficacia e di misurarne le performance - 4
- attività eseguita e monitorata automaticamente, secondo i più elevati standard disponibili sul mercato - 5

L'utilizzo di tale modello, così come l'applicazione pratica dei concetti del governo della sicurezza, deve però essere effettuato sulla base di un criterio, che si potrebbe definire di buon senso, di commisurazione tra il grado di maturità desiderabile e il livello di rischio o di complessità che la specifica organizzazione si trova a fronteggiare. In altre parole per organizzazioni semplici e non esposte a rischi elevati potrebbe essere ragionevole perseguire un livello di maturità non elevato (ad esempio, nella scala sopra esposta, un livello due o addirittura uno, per alcuni processi), mentre organizzazioni complesse ed esposte a rischi elevati dovrebbero posizionarsi ad un livello di maturità tra il quarto e il quinto della scala indicata.

Un'altra utile guida per l'attuazione del governo della sicurezza può essere ravvisata nel già più volte citato BS 7799. Tale standard ha l'obiettivo di indirizzare l'esigenza di proteggere le informazioni (elaborate con strumenti elettronici, ma anche conservate su supporti non elettronici, come quelle scritte su documenti cartacei) all'interno di una

---

[4] *Quanto delineato in questo paragrafo è trattato in modo ampio nella pubblicazione dell'IT Governance Institute , "CobiT® Management guidelines"*

determinata organizzazione, comprese le sue interrelazioni con l'esterno.

Tale esigenza può essere raggiunta attraverso l'implementazione di quello che viene definito **sistema di gestione della sicurezza delle informazioni** (ISMS - Information Security Management System). L'ISMS è composto da:

- politica di sicurezza, che fornisce le direttive aziendali per la sicurezza delle informazioni
- organizzazione, che assicura la corretta gestione della sicurezza delle informazioni all'interno dell'organizzazione
- classificazione e controllo del patrimonio, che assicura l'identificazione dei beni aziendali (dove per beni si intendono anche le informazioni) e la definizione e applicazione di misure di protezione adeguate al loro valore
- sicurezza del personale, per ridurre il rischio di errori, furti, frodi, ecc.
- sicurezza fisica e ambientale, per prevenire accessi non autorizzati, danni e incidenti
- gestione operativa e delle comunicazioni, che assicura una gestione operativa corretta e sicura delle elaborazioni e delle macchine
- controllo degli accessi alle informazioni
- sviluppo e manutenzione delle applicazioni, che assicura che la sicurezza sia incorporata nei sistemi informativi
- gestione della continuità operativa, che assicura una tempestiva reazione ad interruzioni operative e la protezione delle attività critiche da disastri e incidenti rilevanti
- conformità con la legge, che assicura di ottemperare a leggi e a regolamenti pertinenti.

6.3 LA SICUREZZA DELLE RETI, UN BENE NAZIONALE ED EUROPEO DA PROMUOVERE

La sicurezza informatica ha assunto sempre più un connotato di **sicurezza della conoscenza** delle aziende e degli individui. Sicurezza che è indispensabile garantire in un'economia della conoscenza, in linea con le raccomandazioni della Commissione Europea e

con gli impegni assunti dall'UE nella conferenza di Lisbona. Un concetto questo della **sicurezza della conoscenza**, che pone l'attenzione sulle persone (giuridiche o fisiche) e sulla modalità con cui queste proteggono le informazioni che hanno più care per competere o per conservare intatto il diritto alla riservatezza.

Lavorando a questo documento, gli autori hanno effettuato un fruttuoso confronto di esperienze e di osservazioni riguardanti lo scenario nazionale ed europeo, valutando le best practice in uso e riesaminando come oggi le aziende possono affrontare il tema della protezione delle reti e delle informazioni.

L'impressione generale è che qualcosa sia stato fatto nel corso degli ultimi anni, una maggiore sensibilità al tema si stia consolidando ma che, complessivamente, molto resti da fare.

In questo contesto la nascita di ENISA appare come una grande opportunità, anche per il nostro Paese, per definire e attuare politiche condivise all'interno dell'Unione Europea e sviluppare la sensibilità e la consapevolezza della sicurezza nella Società.

Tuttavia, per evitare che ENISA sia vissuta come un apparato distante dai problemi e dalla vita di tutti i giorni, alla nascita dell'agenzia è necessario che si accompagni un impegno di tutti gli attori coinvolti. Per questo fine è certamente utile proseguire il lavoro intrapreso in questo documento, raccogliendo le indicazioni che verranno da ENISA per promuoverle in ambito nazionale e, viceversa, portare in quella sede la specificità delle esigenze nazionali.

Le istituzioni, i professionisti della sicurezza, gli utenti, le aziende, possono avere grande utilità nel trovare un luogo comune di confronto nel quale condividere esperienze ed esigenze e proporre e condurre iniziative di informazione, formazione, raccomandazione. Il bisogno di sicurezza si fa sempre più ampio aprendo spazi a nuove realtà che si dimostrino in grado di rispondere ad una domanda crescente. Tuttavia questo bisogno deve poter trovare risposte efficienti, professionalità ed esperienze in grado di poter garantire che un investimento in sicurezza non diventi un farmaco placebo i cui effetti sono solo una maggiore tranquillità interiore di chi investe a fronte di una immutata esposizione al rischio.

Nelle indagini statistiche il problema della sicurezza, sempre al primo posto nell'attenzione dei cittadini, è vissuto come una esigenza condivisa nelle nostra Società. La sicurezza pubblica, stradale, finanziaria sono i temi di cui sentiamo maggiormente parlare e di cui tutti noi sentiamo maggiormente la necessità. Il tema della **sicurezza della conoscenza** sta prepotentemente conquistando terreno nell'attenzione pubblica, non come sarebbe necessario che fosse, ma di più di quanto avveniva qualche anno fa. A questo hanno contribuito anche le recenti normative come ad esempio il Testo unico sulla privacy e il protocollo Basilea II nell'ambito del credito bancario.

L'augurio di chi, assieme al Ministero delle Comunicazioni e al Ministero per l'Innovazione, ha realizzato questo documento è che esso possa costituire un primo risultato concreto di un impegno, da proseguire nel tempo, volto a costruire una **cultura della sicurezza**, tramite un raccordo attivo e dialettico con le istituzioni e con l'attuazione di una **cinghia di trasmissione** con la società civile, il mondo delle imprese, i cittadini. Un impegno da intendersi nel senso espresso da de Toqueville di **interesse ben inteso**, l'interesse dei singoli cittadini che, adeguatamente perseguito, coincide con l'interesse comune della società.

Componente importante di questo impegno è la disponibilità verso il Paese per dare interpretazioni condivise delle raccomandazioni ENISA e dei numerosi organismi/associazioni internazionali che si occupano di sicurezza; per condurre politiche comuni di diffusione della cultura sulla sicurezza, adottare approcci e metodologie che siano adatti alle specifiche esigenze del sistema produttivo italiano e che tengano conto delle specificità del nostro sistema giuridico e della nostra cultura, ponendo le risultanze di questa attività anche a disposizione del legislatore.

Tutto ciò coinvolgendo le istituzioni, i professionisti, gli utenti, le imprese in associazione tra loro proseguendo un progetto iniziato grazie alla sensibilità delle istituzioni e da proseguire affinché possa trasformarsi in uno strumento concreto al servizio della **sicurezza della conoscenza**

ALLEGATO 1
Riferimenti normativi, regolamentari e di *best practice*

A - Documenti dell'OCSE e delle Nazioni Unite

Linee Guida *"Sicurezza dei sistemi e delle reti d'informazione: verso una cultura della sicurezza"*. - Luglio 2002
www.innovazione.gov.it

Linee Guida *" Protecting Consumers from Fraudulent and Deceptive Commercial Practices Across Borders"* - giugno 2003.
www.innovazione.gov.it

Risoluzione delle Nazioni Unite A/RES/58/199 del 23.12.2003 "Creation of a global culture of cyber-security and the protection of critical information infrastructures"
www.apectel29.gov.hk/download/estg-13.pdf

B - Direttive e altri documenti UE

Direttiva 1999/93/CE del Parlamento europeo e del Consiglio del 13 dicembre 1999 relativa ad un quadro comunitario per le firme elettroniche.
www.innovazione.gov.it

"Resolution on network and information security" (11 dicembre 2001).
www.innovazione.gov.it

Comunicazione della Commissione al Parlamento Europeo, al consiglio, al Comitato economico e sociale e al Comitato delle Regioni Sicurezza delle reti e sicurezza dell'informazione: proposte di un approccio strategico europeo - (giugno 2001).
www.innovazione.gov.it

Direttiva 2002/19/CE - *"Accesso alle reti di comunicazione elettronica e alle risorse correlate, e interconnessione delle medesime"* (Direttiva accesso).

Direttiva 2002/20/CE - *"Autorizzazioni per le reti e i servizi di comunicazione elettronica"* (Direttiva autorizzazioni).

Direttiva 2002/21/CE - *"Quadro normativo comune per le reti ed i servizi di comunicazione elettronica"* (Direttiva Quadro).

Direttiva 2002/22/CE - *"Servizio universale e diritti degli utenti in materia di reti e di servizi di comunicazione elettronica"* (Direttiva sul servizio universale).

Direttiva 2002/58/CE - *"Trattamento dei dati personali e alla tutela della vita privata nel settore delle comunicazioni elettroniche del 12 luglio 2002"* (Direttiva privacy).
www.innovazione.gov.it

C - Leggi dello Stato italiano e normativa correlata

Legge 23 dicembre 1993 n. 547 *"Modificazioni e integrazioni alle norme del codice penale e del codice di procedura penale in tema di criminalità informatica"*.

Legge 15 marzo 1997, n. 59 - *"Delega al Governo per il conferimento di funzioni e compiti alle regioni ed enti locali, per la riforma della Pubblica Amministrazione e per la semplificazione amministrativa"*
L'art. 15 della legge istituisce la RUPA.

www.parlamento.it/parlam/leggi

D. lgs. 13 maggio 1998, n. 171, modificato dal **D. Lgs. 28 dicembre 2001 n. 467** (G.U. 3 giugno 1998, n. 127). *"Disposizioni di tutela della vita privata nel settore delle telecomunicazioni, in attuazione della direttiva 97/66/CE del Parlamento europeo e del Consiglio, ed in tema di attività giornalistica".*

(Testo modificato dal **D. Lgs. 28 dicembre 2001 n. 467**)
www.interlex.it

DPCM 8 febbraio 1999, G.U. n. 87 del 15 aprile 1999, *"Regole tecniche per la formazione, la trasmissione, la conservazione, la duplicazione, la riproduzione e la validazione, anche temporale, dei documenti informatici, ai sensi dell'art. 3 comma 1, del D.P.R. 10 novembre 1997, n. 513".*
www.innovazione.gov.it

"Testo unico delle disposizioni legislative e regolamentari in materia di documentazione amministrativa", D.P.R. n. 445/2000, 28 dicembre 2000 Capo II, Sezione I, Articolo 6 - 7, Sezione II, Articolo 8 - 10, Sezione III, Articolo 14 - 17, Sezione IV, Articolo 20, Sezione V, Articolo 22 - 29, Capo III, Articolo 38, Sezione III, Articolo 43, comma 6.
www.innovazione.gov.it

"Regole tecniche per il documento informatico nella PA" - 23 novembre 2000, Deliberazione n. 51/2000 del 23 novembre 2000. Definisce le regole tecniche per formazione e conservazione di documenti informatici delle pubbliche amministrazioni ai sensi dell'art. 18, comma 3, del D.P.R. 10 novembre 1997, n. 513. Tali regole sono adeguate periodicamente dall'Autorità per l'informatica nella pubblica amministrazione alle esigenze istituzionali, organizzative, scientifiche e tecnologiche.
www.innovazione.gov.it

DPCM 11 aprile 2002 - *"Schema nazionale per la valutazione e la certificazione della sicurezza delle tecnologie dell'informazione, ai fini della tutela delle informazioni classificate, concernenti la sicurezza interna ed esterna dello Stato".*
www.innovazione.gov.it

D. lgs. n. 10 del 15 febbraio 2002 - *"Recepimento della direttiva 1999/93/CE sulla firma elettronica"*.
www.innovazione.gov.it

D.P.R. 7 Aprile 2003 - *"Regolamento recante disposizioni di coordinamento in materia di firme elettroniche a norma dell'articolo 13 del decreto legislativo 23 gennaio 2002, n. 10"*. - 7 aprile 2003.

Apporta modifiche al "Testo unico delle disposizioni legislative e regolamentari in materia di documentazione amministrativa", D.P.R. 445/2000 (Testo A).
www.innovazione.gov.it

D. lgs. 9 aprile 2003, n. 68 - *"Attuazione della direttiva 2001/29/CE sull'armonizzazione di taluni aspetti del diritto d'autore e dei diritti connessi nella società dell'informazione"*.

Le nuove norme prevedono, tra l'altro, l'estensione delle sanzioni per illeciti prima non previsti, quali l'elusione delle misure tecnologiche per la protezione dei dati e la loro diffusione on-line.
www.innovazione.gov.it

"Regole per un corretto invio delle e-mail pubblicitarie" - 29 maggio 2003.

Provvedimento generale del Garante per la Protezione dei Dati personali del 29 maggio 2003.
www.innovazione.gov.it

D. lgs. 30 giugno 2003, n. 196 - *"Codice in materia di protezione dei dati personali"*.

Pubblicato su G.U. del 29 luglio 2003, Serie Generale n. 174, Supplemento ordinario n. 123/L.
www.innovazione.gov.it

DPCM 30 ottobre 2003 - *"Definizione di uno Schema nazionale per la valutazione e certificazione della sicurezza di sistemi e prodotti nel set-*

tore della tecnologia dell'informazione".
www.innovazione.gov.it

DPCM 13 gennaio 2004 - *"Regole tecniche per la formazione, la trasmissione, la conservazione, la duplicazione, la riproduzione e la validazione, anche temporale, dei documenti informatici"*.
www.innovazione.gov.it

Decreto interministeriale 17 febbraio 2005 *"Linee guida provvisorie per l'applicazione dello schema nazionale per la valutazione e certificazione di sicurezza nel settore Ict"*.
www.innovazione.gov.it

D. lgs. 28 febbraio 2005 n.42 *"Istituzione del sistema pubblico di connettivita' e della rete internazionale della pubblica amministrazione, a norma dell'articolo 10, della legge 29 luglio 2003, n. 229"*
www.innovazione.gov.it

D - Documenti ministeriali e AIPA/CNIPA

Circolare AIPA/CR/27 16 febbraio 2001.

"Utilizzo della firma digitale nelle Pubbliche Amministrazioni".

Alla luce delle disposizioni normative sul tema, la circolare AIPA/CR/27 offre una sintesi ed una guida alle indicazioni operative e agli ambiti di utilizzo della firma digitale nelle Pubbliche Amministrazioni.

Ai sensi dell'Art. 17 del decreto del Presidente della Repubblica 10 novembre 1997, n. 513.
www.innovazione.gov.it

"Linee guida in materia di digitalizzazione della PA per l'anno 2002".

Direttiva del Ministro per l'Innovazione e le Tecnologie del 21 dicembre 2001.
www.innovazione.gov.it

Direttiva del 16 gennaio 2002 del Presidente del Consiglio dei Ministri - Dipartimento per l'Innovazione e le Tecnologie "Sicurezza Informatica e delle Telecomunicazioni nelle Pubbliche Amministrazioni Statali".
www.innovazione.gov.it

Allegato 1 - Valutazione del livello di sicurezza.

Autovalutazione - Il questionario ha lo scopo di guidare l'Amministrazione nel processo di auto-valutazione del proprio livello di sicurezza, rispetto alla base minima raccomandata.

Allegato 2 - Base minima di sicurezza.

Indicazioni per assistere i Ministeri nell'individuazione delle misure di protezione che debbono essere realizzate e gestite con assoluta priorità, al fine di supportare le Amministrazioni sia nell'applicazione degli adempimenti normativi di riferimento (es. D. lgs. 675 e 318) sia nel contrastare eventuali potenziali minacce .

"Proposte in materia di sicurezza informatica e delle telecomunicazioni per la pubblica amministrazione" (marzo 2004).

Volume redatto dalla Comitato Tecnico Nazionale sulla sicurezza informatica e delle telecomunicazioni nelle pubbliche amministrazioni.
www.innovazione.gov.it

"Linee guida per l'utilizzo della firma digitale".

Documento redatto dal CNIPA (maggio 2004) per supportare gli utenti e le aziende circa l'utilizzo della firma digitale.
www.innovazione.gov.it

ALLEGATO 2
Esempi di metodologie ed approcci di analisi dei rischi

Nel presente allegato sono state riassunte alcune delle principali metodologie di analisi dei rischi in ambito teleinformatico. Questo allo scopo di fornire una panoramica sull'applicazione pratica dei diversi principi enunciati al capitolo 4.

Le metodologie e i relativi applicativi software di cui al presente allegato sono riportati a mero titolo esemplificativo e costituiscono solo una parte delle metodologie e dei prodotti in uso. La loro inclusione nella presente appendice non esaurisce il ventaglio delle possibili soluzioni e non costituisce un indirizzo o una raccomandazione all'uso.

I contributi sono stati forniti dalle persone e aziende indicate nelle schede che seguono.

Allegato 2.1 - Defender Manager

Informazione fornita da Giuseppe Carducci Artenisio di Securteam srl - Elsag (gruppo Finmeccanica)

Che cosa è

Defender Manager® è un applicativo, realizzato da Securteam (gruppo Finmeccanica), che attua un modello di analisi e gestione del rischio per supportare le decisioni in materia di sicurezza, costituendo un sistema informativo per la gestione della sicurezza dell'informazione e assistendo nelle fasi di:

- descrizione del perimetro d'intervento e dello scenario d'interesse
- classificazione delle informazioni
- individuazione delle minacce e analisi del rischio
- scelta delle misure di protezione commisurate ai risultati dell'analisi del rischio
- verifica del mantenimento nel tempo della capacità di soddisfare la politica di sicurezza aziendale
- pianificazione delle misure di protezione che si intendono attuare
- documentazione delle misure di protezione attuate.

Defender Manager® si inserisce nel processo ciclico di gestione della sicurezza mantenendo e documentando gli interventi realizzati, aggiornando i livelli di rischio esistenti e in generale dando visibilità alla direzione e alle parti interessate dei progressi ottenuti in termini di protezione.

A chi è rivolto

Defender Manager® è adatto all'impiego in entità aziendali medio/grandi comprese le realtà complesse come gruppi industriali di grandi dimensioni composti da più società. Esso consente, infatti, di operare in diversi perimetri/scenari, magari appartenenti ad una o a più società, ma anche di gestire molteplici interventi di messa in sicurezza secondo strategie differenziate e in linea con i criteri scelti da ciascuna società.

Il processo di gestione della sicurezza coinvolge, a vario titolo e con compiti e responsabilità distinti, molte figure all'interno dell'organizzazione (responsabile sicurezza, auditor, proprietari dei dati, proprietari dei processi, gestori delle applicazione e delle infrastrutture, ecc.) e pertanto si caratterizza per la sua trasversalità rispetto a processi e funzioni aziendali.

Al fine di facilitare il coinvolgimento di tutti gli attori nel processo di gestione della sicurezza Defender Manager® è stato realizzato in architettura WEB: un dettagliato sistema di controllo delle autorizzazioni permette a ogni figura di accedere alle funzionalità di propria pertinenza disponendo semplicemente di un browser.

Principi base

I principi cardine alla base di Defender Manager® possono essere sintetizzati come di seguito:

- il dato costituisce l'elemento centrale del processo di analisi del rischio
- riservatezza, integrità e disponibilità sono i parametri di sicurezza in relazione ai quali viene valutato il rischio
- il rischio è inteso come la combinazione della probabilità di un evento dannoso e della gravità delle sue conseguenze
- le misure definite per il raggiungimento degli obiettivi di sicurezza sono commisurate, a fronte dei tre parametri di sicurezza, ai relativi livelli di rischio.

Struttura della base informativa

La base informativa di Defender Manager® è articolata in tre aree che contengono i modelli dei perimetri di intervento, la Politica di trattamento del rischio e la documentazione di sicurezza.

Base dati "modello perimetro di intervento"

Per ogni perimetro viene definito in Defender Manager® il modello ai fini dell'analisi della sicurezza.

Base dati "Politica di trattamento del rischio"

Defender Manager® si avvale di una base dati contenente le minacce alla sicurezza dell'informazione e i relativi attacchi, e le misure di sicurezza ritenute idonee a contrastare le suddette minacce ed attacchi.

Il database, nella sua versione base eventualmente personalizzabile, viene fornito popolato con una Politica di trattamento del rischio in linea con quanto previsto dallo standard ISO/IEC IS 17799 per condurre un'analisi del rischio per la certificazione BS 7799 del Sistema di Gestione della Sicurezza delle Informazioni (SGSI).

Base dati "documentazione di sicurezza"

In Defender Manager® è prevista un'area documentale pubblica destinata a contenere informazioni di carattere generale di supporto al processo di gestione della sicurezza (normativa di legge e aziendale, standard e normative tecniche di riferimento, linee guida, procedure, istruzioni operative, ecc.).

Il processo di analisi e trattamento del rischio

Per ogni componente viene stimato il livello di rischio rispetto alle minacce pertinenti. Tale stima viene eseguita in funzione del livello di esposizione alle minacce (frequenza degli attacchi, portati anche

senza successo, per perpetrare la minaccia) e del valore del bene trattato (classe di criticità dell'informazione rispetto alla riservatezza, integrità e disponibilità).

Sulla base del livello di rischio vengono selezionate, dalla Politica di trattamento del rischio, le contromisure con la graduazione ritenuta adeguata per mitigare il rischio.

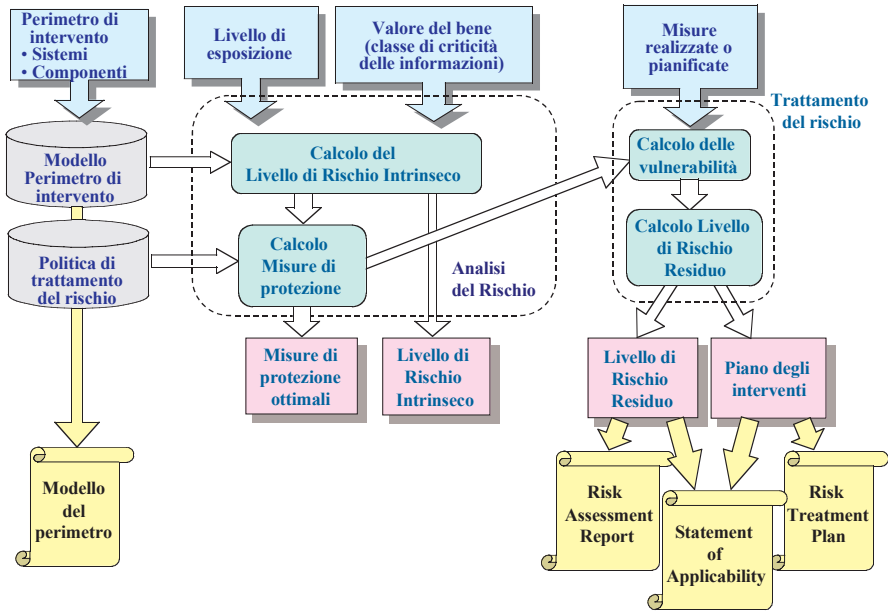
Tale processo, eseguito per tutte le componenti, porta a definire il profilo ottimale di protezione ovvero l'insieme di misure di protezione che mitigano il rischio in maniera ritenuta adeguata.

Confrontando le misure di protezione realizzate con quelle definite nel profilo di protezione ottimale (gap analysis) viene determinato il rischio residuo che rappresenta una misura dello scostamento dal profilo di protezione ottimale. Analizzando tali scostamenti si produce un piano che indica, evidenziandone le priorità, quali interventi è necessario compiere per ridurre gli scostamenti e avvicinarsi al profilo di protezione ottimale.

L'utilizzo di Defender Manager® nell'ambito di un processo strutturato di gestione della sicurezza permette, fra l'altro, di:

- evidenziare la rispondenza delle protezioni attuate o pianificate agli obiettivi di sicurezza stabiliti
- valutare l'adeguatezza delle protezioni realizzate o pianificate ai rischi individuati
- valutare le misure attuate o pianificate alla luce delle migliori prassi di sicurezza
- indicare quali misure implementare e/o potenziare e secondo quali priorità (Piani di intervento)
- assicurare la necessaria trasparenza documentando i razionali sottesi alle scelte effettuate
- assicurare nel tempo una costante verifica dell'efficacia del processo
- facilitare l'elaborazione di numerosi report sia di carattere direzionale, sia di carattere operativo e fornire automaticamente la

documentazione prevista dal BS 7799 - 2:2002 fra cui il Risk Assessment Report, il Risk Treatment Plan e lo Statement of Applicability.



Allegato 2.2 - Le metodologie dell'Information Security Forum e l'analisi dei rischi specifica alle reti informatiche

Informazione fornita da Sebastiano D'Amore di PricewaterhouseCoopers Advisory

L'Information Security Forum (ISF) è una organizzazione internazionale, indipendente e non-profit, operante esclusivamente in ambito **Information Security**. È sostenuta da oltre 250 tra le maggiori aziende ed enti mondiali e svolge le seguenti principali attività:

- pubblica e mantiene aggiornato lo "Standard of Good Practice" (SoGP, versione 4.0 2003), che nasce dalle esperienze condivise dei propri membri e dai principali standard internazionali (p.e. BS 7799)
- organizza regolarmente un'Information Security Survey che fornisce benchmarking ai propri membri e mantiene aggiornata una visione d'insieme sullo stato dell'arte
- sviluppa progetti, studi, linee guida e pubblicazioni su argomenti quali: Corporate Governance, Information Risk Management, Security Management & Operations, Internet & Network Security, Communication Security, Technical Architectures, Crittografia, ecc.

In materia di analisi dei rischi l'ISF dispone di tre metodologie con le seguenti principali caratteristiche:

- SPRINT: Metodo Statico ad alto livello
- SARA: Metodo Statico a livello più approfondito
- FIRM: Sistema completo di gestione dei rischi in modo dinamico con sistema di misurazione del rischio basato su **scorecard**.

SPRINT

É stato sviluppato nell'intento di rispondere ad una esigenza sempre più crescente di semplificazione dell'attività di analisi dei rischi, consentendo anche ai **business manager** di divenire parte attiva del processo. La metodologia, difatti, è orientata al business ed è utilizzabile anche da persone con limitata esperienza specifica. La metodologia si applica in tempi brevi e produce rapporti sintetici che evidenziano rischi chiave e piani d'azioni per ricondurli a livelli accettabili.

Più in dettaglio SPRINT si sviluppa lungo le seguenti tre macro fasi:

1 - Business Impact Assessment (BIA) & Overall classification (valutazione del livello di rischio di business associato all' information system): consente di calcolare le conseguenze sul business derivanti dalla perdita di riservatezza, integrità e disponibilità delle informazioni correlate ai processi, utilizzando una scala di valori qualitativi di **business impact rating**.

In base ai risultati conseguiti dalla compilazione degli appositi questionari (form di BIA, uno per la riservatezza, uno per l'integrita e uno per la disponibilità), si classificano i sistemi e le applicazioni oggetto di analisi su una scala di valori rappresentanti il diverso livello di criticità (**regolari**, **importanti ma non critici**, **critici**).

Nel caso di sistema **regolare**, ossia non critico (livello di rischio basso), il processo di SPRINT termina; in tale caso si ritiene sufficiente controllare solamente l'effettiva presenza dei controlli di base necessari a mantenere l'ottimale livello di protezione del sistema.

Si procede con le restanti fasi della metodologia SPRINT, nel caso di sistema ritenuto **importante ma non critico** (livello di rischio medio).

Si continua con l'approccio previsto da SARA, metodologia

complementare a SPRINT (descritta successivamente) nel caso di sistema **critico** (livello di rischio alto), in quanto tal caso necessita un approccio più analitico condotto da personale specializzato.

2 - Threats, Vulnerabilities and Control Assessment: prevede, utilizzando il relativo questionario, di:

- valutare e correlare minacce e vulnerabilità, in relazione ai parametri della sicurezza (riservatezza, integrità e disponibilità), sulla base di una scala di **vulnerability rating**
- calcolare il livello di esposizione ai rischi
- identificare i controlli (requisiti di sicurezza) necessari per contrastare i rischi calcolati.

3 - Action Plan: consente di definire un piano d'interventi per l'implementazione dei controlli individuati nella fase precedente.

SARA

É una metodologia associata a SPRINT ed orientata a sistemi **altamente critici**. In sostanza utilizza i risultati conseguiti in SPRINT, nella fase di **Business Impact Assessment**, per poi consentire di effettuare un Risk Assessment sui sistemi critici identificando più nei dettagli l'esatta natura dei rischi e calcolandone più accuratamente il livello in base alla quale si determinano le contromisure (security controls).

FIRM (Fundamental of Information Risk Management)

È una metodologia completa di analisi e gestione dei rischi che

consente di monitorare e gestire l'efficacia del Sistema di Gestione della sicurezza all'interno di organizzazioni complesse, in maniera continuativa e dinamica. Più nei dettagli:

- fornisce una metodologia per il calcolo e il monitoraggio continuo dei rischi che consente a tutte le figure aziendali, coinvolte nel processo di gestione della sicurezza, di ottenere una chiara visione dello scenario dei rischi aziendali
- è composta da una serie di azioni da mettere in atto per portare il rischio all'interno di un livello accettabile al management
- utilizza metriche di calcolo del rischio, sia di tipo qualitativo che quantitativo, basate sul concetto di **scorecard**, che offrono una visione d'insieme e a diversi livelli di dettaglio
- fornisce un metodo per registrare gli incidenti mantenendo dinamica la misurazione del rischio, insieme ad altre misure di aggiornamento dinamiche ed indotte
- si concilia con le normali attività operative (implementazione di nuovi sistemi, manutenzione dei sistemi esistenti, operatività).

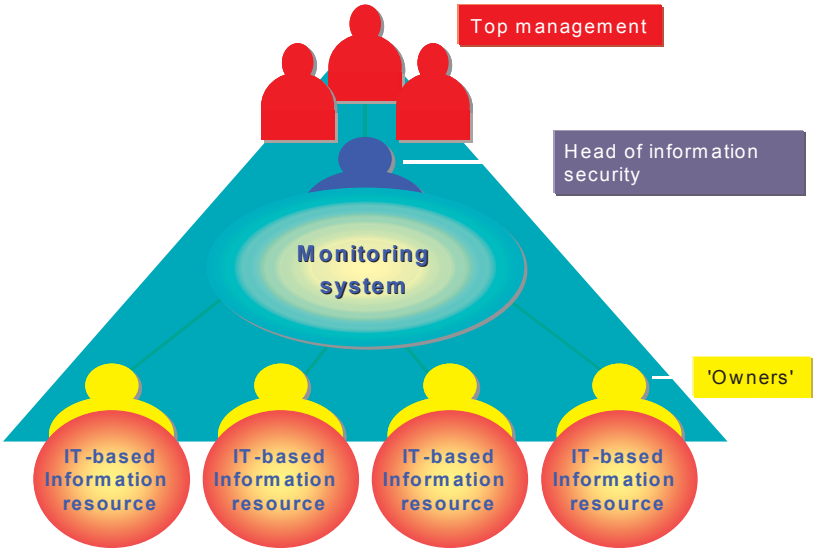
Il concetto di base della metodologia è dato dall'**Information Resource** (la risorsa informativa) che evidenzia la correlazione tra dati, informazioni, applicazioni e sistemi informativi (Architetture, piattaforme ed apparati).

Primaria attività di FIRM è il censimento e la classificazione delle **risorse informative** che costituiscono poi il contesto di protezione. Da qui si procede con approccio sistematico a:

- definire ambito e scopo del monitoraggio: in particolare l'obiettivo è quello di tenere pienamente informato il top management sull'evolversi del livello di rischio informatico, interno all'organizzazione, e incoraggiare gli **owner** ad abbassare il rischio a un livello ritenuto accettabile dal top-management
- definire coerentemente ruoli e responsabilità e linee di comu-

nicazione in seno all'azienda; ogni linea aziendale (dall'owner al Top Management, passando dai coordinatori e custodi del processo di monitoraggio) ricopre determinati ruoli e si assume precise responsabilità, utilizzando standard e protocolli di comunicazione predeterminati

- predisporre i **sound fact-gathering tool** per l'analisi e la gestione dei rischi (balance scorecard per la valutazione dei rischi, questionario di assessment degli incidenti, ecc.)
- realizzare e gestire un processo dinamico (costruttivo e continuativo) di misurazione e monitoraggio
- predisporre report e presentazioni concise per il Top-Management.



La metodologia FIRM è inoltre supportata da tool specifici (es. Citicus One), che consentono di gestire tutte le fasi del processo attraverso appositi cruscotti informatizzati.

In definitiva, l'elemento di spicco della metodologia è rappresentato dal suo sistema di misurazione **preciso** e a **ciclo continuo** che supporta il top-management e gli owner a:

- estendere l'approccio all'intera organizzazione, indipendentemente dalla sua struttura e scala gerarchica
- sostenere i principi chiave della Corporate Governance, rispondendo a esigenze di identificazione, monitoraggio e rilevazione di un rischio operativo fondamentale
- ridurre i costi, dirigendo meglio gli investimenti specifici ma anche misurandone l'efficacia (value reporting)
- incrementare il valore dell'azienda riducendo l'impatto negativo generato da incidenti e interruzioni di servizi primari.

NORA

Le metodologie dell'ISF fin qui sintetizzate, come anche altre, misurano i rischi posti all'organizzazione tramite modelli generici applicabili a qualsiasi contesto informatico.

Nel caso in cui il punto d'attenzione sia esclusivamente una rete di comunicazione informatica e si sia già optato per un elevato livello di difesa (tramite analisi dei rischi concettuale o perché la rete costituisce l'attività principale dell'organizzazione), è il caso di valutare metodologie specifiche.

PricewaterhouseCoopers, ad esempio, adotta una propria metodologia denominata NORA (Network Oriented Risk Assessment) che utilizza i seguenti elementi di base per il processo di analisi:

- Network Access Path (NAP): descrizione dei percorsi di accesso alla rete in termini di client, server e funzioni di rete (O&M, Billing, ecc.)
- Threat Scenario (scenari delle minacce): elaborati sulla base di scenari individuati all'interno dei sistemi informativi; NORA dispone di predefiniti "Threat Scenario", che devono poi essere mappati sulla specifica situazione della realtà aziendale oggetto di analisi, determinata dai NAP
- Dalla correlazione fra NAP e Threat Scenario si determina la matrice NSC (Nap/Scenario Combination)

- Impact Criteria: criteri di valutazione degli impatti (definiti su scala da 1 a 5)
- Probability Scale: valutazione della probabilità di attuazione delle minacce (su scala da 1 a 5)
- Gravity Matrix: combinazione di Impact Criteria e Probability Scale per dare valori di gravità.

La metodologia si sviluppa nelle seguenti tre fasi e relative attività:

Fase 1: Inizializzazione:

- rilevazione di tutti i link di rete
- rilevazione della struttura organizzativa (organizzazione a supporto della rete)
- rilevazione delle piattaforme tecnologiche
- raccolta di altre informazioni utili ai fini dell'avvio del processo di analisi (es. minacce e vulnerabilità di rete già conosciute, business driver)
- inventario della documentazione di rete.

Fase 2: Analisi:

- Risk Assessment:
  - mappatura delle Business communication sui Network Access Path (NAP)
  - definizione delle combinazioni possibili fra Threat Scenario e NAP, in base a matrice di NSC (Nap/Scenario Combination)
  - valutazione dei possibili impatti sugli scenari delle minacce, rispetto ai parametri RID, determinati in base agli Impact Criteria
  - analisi delle vulnerabilità, condotta tramite programmi

di audit, che consente di determinare la probabilità di accadimento di un determinato scenario di minacce (in base a probability scale), al fine di determinare la matrice di gravità (la Gravity Matrix, ricavata come combinazione di impatto e probabilità di accadimento)

- Futuri sviluppi:
  - valutazione di sviluppi futuri sulle tecnologie
  - valutazione degli impatti sulla sicurezza che tali sviluppi possono comportare.

Fase 3: Action Plan

Definizione di un piano d'azione sulla base di soluzioni generiche e della valutazione di quanto offre il mercato (i.e. stato dell'arte); è tipicamente strutturato su tre livelli così definiti:

- **Legacy system/Critical action**, per mitigare i rischi con gravità elevate
- **Legacy system/Complementary action**, per mitigare i rischi che si intende indirizzare a medio-lungo termine
- **The Way Forward**, per la pianificazione pro-attiva delle misure di sicurezza a fronte di sviluppi futuri di rete.

Allegato 2.3 - CRAMM

Informazione fornita da Giampaolo Scafuro di Sicurezza e Sistemi (distributore in Italia di CRAMM)

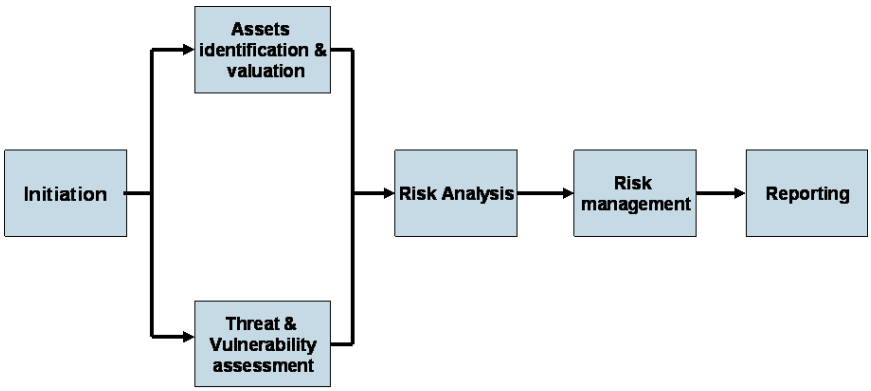
Che cosa è

CRAMM (CCTA Risk Analysis and Management Method) è la metodologia di supporto all'analisi e gestione dei rischi dei sistemi ICT, sviluppata dal CCTA (Central Computer Telecommunications Agency). La metodologia fornisce le linee guida da seguire per condurre l'analisi e si avvale di un software di supporto per l'inserimento, la memorizzazione e l'elaborazione delle informazioni. CRAMM si presenta sul mercato in diverse versioni, predefinite (UK Standard, NATO, NHS, Social Care, ecc.), che si adattano alle singole necessità. CRAMM V si compone di due distinte modalità di conduzione dell'analisi del Rischio: Expert e Express.

La modalità Express fornisce maggiore rapidità di conduzione ed è più adatta ad ambienti nei quali tempo e risorse possono essere limitati e non è necessario il livello di **precisione** del CRAMM Expert. Quanto descritto in questa scheda si riferisce principalmente alle potenzialità offerte dalla modalità Expert.

Principi base

CRAMM mette in atto un processo di analisi del rischio strutturato in fasi ciascuna supportata da questionari e linee guida.



All'interno del dominio di applicazione dell'analisi, vengono identificate le risorse più significative per il conseguimento della missione aziendale creando i modelli delle risorse.

L **'Asset Model** rappresenta la schematizzazione che la metodologia CRAMM ha previsto per organizzare le informazioni relative agli asset rilevati. Le possibili tipologie di asset trattabili sono:

- Data Asset (files, data-base, dati in trasmissione, documenti, ecc.)
- Physical Asset (rappresentano le componenti tecnologiche del perimetro di intervento)
- Software Asset (rappresentano le componenti applicative)
- Location Asset (individuano le stanze, gli edifici ed i siti fisici di cui il perimetro di intervento è composto)
- una particolare risorsa fisica è quella che nel CRAMM viene definita **End-User Service** (rappresenta la modalità di trasmissione ed elaborazione dei Data Asset rilevati).

Allo scopo di garantire Riservatezza, Integrità e Disponibilità ai Data Asset rilevati è necessario proteggere i Software Asset, Physical Asset e Location Asset che li supportano. A tal fine è necessario definire le dipendenze tra i diversi tipi di asset mediante la creazione degli Asset Model.

La valutazione degli asset avviene valutando, per ogni asset, la criticità in funzione di impatti e linee guida. Gli impatti valutano principalmente l'indisponibilità, la distruzione, la perdita di riservatezza e l'integrità delle informazioni. Le linee guida definiscono, invece, gli scenari su cui gli impatti trovano applicazione.

La fase di assessment delle minacce e delle vulnerabilità permette, attraverso un questionario apposito, di valutare il livello di probabilità di accadimento delle minacce ed il grado di vulnerabilità, in termini di esposizione alla minaccia, di ogni asset censito.

Tali informazioni permettono di determinare la misura di rischio che, secondo la metodologia CRAMM, è funzione di due aspetti distinti: la combinazione tra minaccia e vulnerabilità da una parte e l'impatto che il verificarsi dell'evento dannoso provocherebbe sulla risorsa in questione.

La valutazione è effettuata attraverso una scala di valori da 1 a 7 utilizzando una matrice di rischio. Le misure di protezione (contromisure) che vengono individuate rappresentano il profilo di protezione di ciascun asset e il punto di partenza per la fase di gestione del rischio.

CRAMM seleziona le opportune misure di sicurezza confrontando i rischi associati a ciascuna minaccia individuata, con il livello di sicurezza che la contromisura è in grado di soddisfare. In questa fase sono valutate le differenze tra le misure di sicurezza proposte da CRAMM e quelle esistenti allo scopo di identificare eventuali aree deboli o aree in cui esistono misure di sicurezza ridondanti.

Le misure di sicurezza fornite (hardware, software, comunicazioni, procedurali, fisiche, organizzative) sono raggruppate, in funzione degli obiettivi di sicurezza che esse soddisfano. Per ciascuna delle fasi precedentemente descritte CRAMM fornisce report che riassumono i risultati conseguiti.

CRAMM: BS 7799

I controlli del CRAMM sono conformi con quanto richiesto dallo standard ISO 17799. Il prodotto può essere utilizzato per supportare le aziende nella valutazione della conformità con lo standard BS 7799 parte 2 del 2002 e, a tale scopo, mette a disposizione una sezione specifica che consente, tra l'altro, di effettuare una gap analysis secondo i principi **plan**, **do**, **check**, **act** e di produrre tutta la documentazione necessaria.

A chi è rivolto

CRAMM è adatto a tutte le realtà aziendali medio/grandi comprese entità complesse come gruppi industriali di grandi dimensioni. Si

adatta in modo più puntuale agli ambienti IT indirizzandone gli aspetti tecnici (hardware, software, protocolli di comunicazione, ecc.) nonché la sicurezza fisica (site, building, room). Per tali aspetti include anche riferimenti puntuali alla sicurezza organizzativa e procedurale.

L'utilizzo di CRAMM nell'ambito di un processo di gestione della sicurezza permette di:

- supportare l'utente nell'intero processo strutturato di gestione della sicurezza grazie a template, maschere applicative e schemi di review a supporto
- valutare lo stato di protezione dell'intero perimetro di analisi mediante la verifica dell'adeguatezza delle protezioni realizzate o pianificate rispetto ai rischi individuati
- valutare le misure attuate o pianificate alla luce delle migliori prassi di sicurezza
- disporre di un profilo di protezione, mirato ad ogni singolo asset, con l'indicazione della priorità per identificare facilmente quali sono gli interventi più urgenti e quali possono essere posticipati
- permettere una costante verifica dell'efficacia del processo mediante le attività di review messe a disposizione dal prodotto
- supportare l'utente nell'attività di documentazione del processo di gestione della sicurezza grazie alla presenze di numerosi report sia di carattere direzionale sia di carattere operativo.

Allegato 2.4 - RISKWATCH

Informazione fornita da Renzo Dell'Agnello di Elea S.p.A (distributore in Italia di RiskWatch)

RiskWatch è un **risk management system** sviluppato dalla RiskWatch Inc. e utilizzato dalle grandi aziende e pubbliche amministrazioni a livello mondiale. RiskWatch è stato sviluppato in varie versioni in lingue diverse dall'inglese: di queste la più rilevante per l'Italia è la versione **VPI,** sviluppata, fin dall'inizio della commercializzazione in Italia, dall'ELEA.

Caratteristiche specifiche della versione VPI sono la lingua (italiano) e la conformità alla legislazione italiana (ad es. il D. lgs. 196/03 relativo alla privacy), oltre che la conformità agli standard di riferimento, in particolare all'ISO 17799/BS 7799. La versione VPI ha inoltre caratteristiche aggiuntive rispetto alla versione internazionale.

Dalla valutazione delle esigenze di aziende e pubbliche amministrazioni in ambito sicurezza si è rilevata la necessità di disporre di impostazioni metodologiche di analisi del rischio differenti in funzione del tipo di analisi e di organizzazione, oltre che del budget a disposizione per tali attività. Per questa ragione RiskWatch VPI supporta impostazioni metodologiche quantitative (SQRM e TLQ), qualitative (TLQ QUAL) e semiquantitative (TLQ/SQRM).

La SQRM è la metodologia standard di RiskWatch disponibile anche nella versione internazionale inglese.

La TLQ QUAL invece è una metodologia qualitativa che consente notevoli riduzioni di tempi e di costi permettendo nel contempo una valutazione completa del livello di sicurezza e una identificazione dei rischi considerati possibili nell'ambito dell'analisi. Genera degli indici particolarmente rilevanti per la valutazione del livello di rischio come ad esempio l'**Impact Relative Index**.

La metodologia TLQ QUAL non è che la versione qualitativa della metodologia TLQ e si differenzia da essa solo perché non prevede l'ultima fase di tale metodologia in cui si richiedono dati quantitativi; inoltre non avendo alcuni risultati quantitativi ha un differente sistema di reporting. La TLQ per le sue caratteristiche consente di effettua-

re l'analisi costi/benefici come la SQRM.

La metodologia semiquantitativa TLQ/SQRM assomma tutti i vantaggi della ricerca metodologica in ambito analisi del rischio alle possibilità di elaborazione e flessibilità di RiskWatch VPI.

Tale impostazione metodologica consente di ottenere una valutazione del livello di rischio con un minimo di ancoraggio ai valori reali degli asset (accetta in input valori sia quantitativi sia qualitativi, con uno specifico processo di normalizzazione), fornendo nel contempo l'**Impact Relative Index** e la **Backward Tracebility**, caratteristiche proprie della metodologia TLQ e TLQ QUAL.

Alcuni concetti e termini utilizzati nella descrizione precedente sulle metodologie supportate da RiskWatch VPI necessitano di approfondimento per coloro che non hanno avuto modo di conoscere tali impostazioni metodologiche precedentemente descritte.

Per **Backward Tracebility** si intende la possibilità, una volta valutato il valore di rischio, di conoscere la percentuale di tale rischio dovuta alle **aree di vulnerabilità** rilevanti per una data minaccia e da tale informazione poter risalire alle vulnerabilità elementari che hanno causato il rischio in oggetto.

Per **Impact Relative Index** (IRI) s'intende un indice di misura del rischio **relativo**, espresso con la metrica 0 - 100 che rappresenta il rapporto tra il rischio effettivo ed il rischio massimo (0 rischio nullo, protezione ottimale e 100 rischio massimo, nessuna protezione) per una determinata minaccia. Esso esprime anche la mancanza di protezione che si ha per tale minaccia.

L'idea che sta alla base della metodologia semiquantitativa TLQ/SQRM è, oltre la possibilità di gestire dati quantitativi e qualitativi, anche quella che identifica due tipi di valutazioni sostanzialmente **indipendenti** di cui è costituito il processo di analisi del rischio.

La prima valutazione è quella relativa al **valore esposto al rischio** cioè il valore di rischio che si avrebbe se non vi fosse nessuna protezione in essere, corrispondente al valore di rischio massimo.

La seconda valutazione è quella relativa al **livello di protezione**, la cui determinazione può essere identificata tramite un confronto

con un modello di protezione, come si dice **allo stato dell'arte**, cioè ottimale per le conoscenze tecniche attuali, corrispondente al livello di protezione definito.

Dalle valutazioni precedenti si ottiene il livello di rischio effettivo (RLE- Risk Level Estimated) espresso con una metrica da 0 a 10. Da tale valore, una volta definita una soglia di accettabilità, è possibile decidere se intervenire e, utilizzando la possibilità di **backward traceability**, dove intervenire.

Le stesse risposte ai questionari con le informazioni sull'ambito sotto analisi sono utilizzabili su tutte le impostazioni metodologiche, essendo tutte tra loro compatibili. È dunque possibile utilizzare un'impostazione più semplice e passare ad una più completa in maniera modulare e scalabile recuperando gli investimenti fatti.

RiskWatch VPI unisce la flessibilità in ambito metodologico ad un supporto completo a livello operativo, con possibilità di acquisire informazioni a livello di intranet e di rete geografica, di ottenerle tramite questionari stampati personalizzati o tramite appositi applicativi che interagiscono direttamente con le persone che forniscono le informazioni.

RiskWatch VPI ha funzionalità di import/export dei dati ed una estesa possibilità di reporting con grafici e tabelle degli indici significativi dell'analisi. Vi è inoltre una completa funzione di auditing del processo di analisi e dei dati rilevati, oltre che statistiche sulla rilevazione.

Allegato 2.5 - Information Security Assessment (ISA), Enterprise Security Architecture (ESA) e analisi dei rischi

Informazione fornita da Simona Napoli e Andrea Mariotti di KPMG

L'analisi dei rischi è finalizzata all'individuazione del valore delle informazioni gestite all'interno dei processi aziendali e del livello di rischio cui sono sottoposte, e, conseguentemente, alla definizione delle più opportune contromisure di sicurezza da adottare per la protezione delle informazioni; l'analisi dei rischi consente altresì di definire politiche e standard di sicurezza che siano contestualizzati alla realtà aziendale.

In tale accezione essa costituisce quindi un passo fondamentale, sia per la valutazione dello stato attuale di sicurezza (Information Security Assessment), sia per la definizione dei requisiti del sistema di gestione della sicurezza che l'azienda intende realizzare (Enterprise Security Architecture).

La corretta applicazione dell'analisi dei rischi deve quindi consentire di:

- individuare i controlli di sicurezza da implementare attraverso l'applicazione degli standard internazionali di sicurezza maggiormente diffusi (BS 7799-2, ISO 17799, ecc.), alla cui redazione e sviluppo KPMG ha partecipato attivamente, in qualità di membro firmatario del comitato BSI-DISC BDD/2
- valorizzare esperienze e best practice consolidate a livello internazionale
- essere facilmente adattabile a contesti specifici attraverso la modifica dei modelli nel corso del tempo, seguendo l'evoluzione della tecnologia
- produrre documentazione organica e strutturata
- graduare le misure di sicurezza ottimizzando il rapporto costi-benefici e semplificando l'operatività degli utenti

- identificare le informazioni chiave da proteggere, sia ai fini del business sia ai fini del rispetto della normativa vigente; questa caratteristica è essenziale per garantire che le politiche di sicurezza siano applicate coerentemente con i requisiti di business e in armonia con la legislazione (ad es. Testo Unico sulla Privacy)
- costituire gruppi di lavoro interdisciplinari, al fine di rendere più agevole la condivisione degli obiettivi del progetto da parte delle diverse funzioni e di effettuare parallelamente la formazione dei partecipanti ai gruppi di lavoro e accrescerne la sensibilizzazione sulle problematiche connesse ai rischi, ai controlli e ai relativi requisiti di sicurezza informatica.

Infine l'utilizzo di strumenti che sfruttano funzionalità Intranet al fine di facilitare il reperimento e la gestione delle informazioni necessarie allo svolgimento dell'analisi, costituisce un ulteriore vantaggio, consentendo una migliore efficienza nei processi di revisione e gestione operativa.

Modello di riferimento

Al fine di rilevare le informazioni critiche ai fini di business e valutare il livello di rischio ad esse sotteso, è necessario in primo luogo ricondurle ai processi aziendali che le utilizzano ed individuare le relative modalità di gestione.

La mappatura delle informazioni viene condotta individuando i macrodati relativi ai processi aziendali, dove con macrodato si intende un insieme minimo di informazioni o un aggregato di dati, tali da costituire un raggruppamento omogeneo per l'applicazione delle misure di protezione.

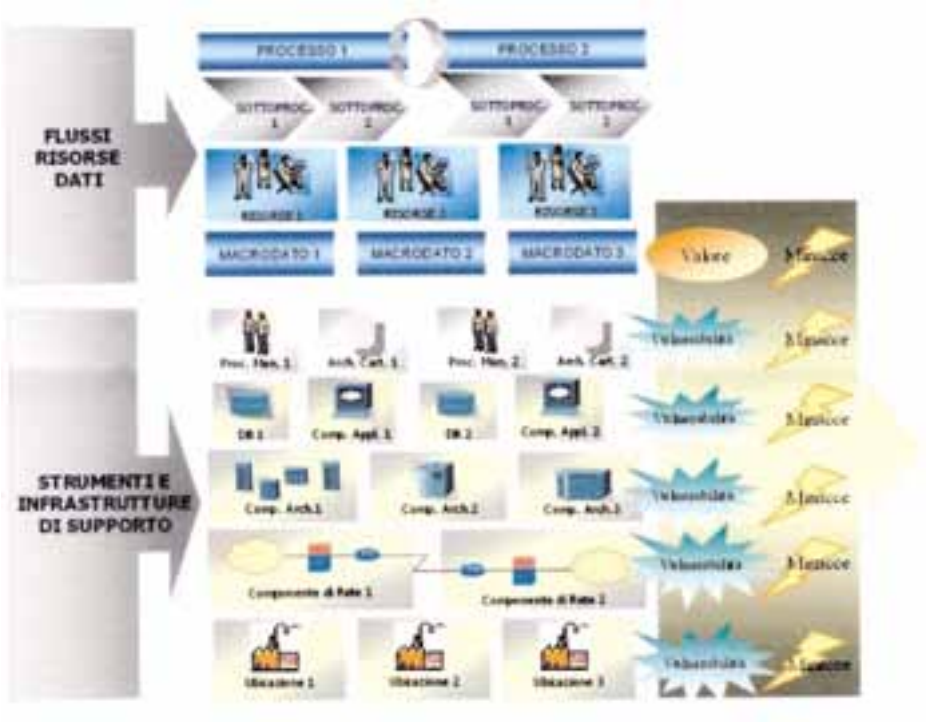
La criticità dei macrodati dipende dal valore che gli stessi hanno in termini di riservatezza, integrità e disponibilità all'interno del processo cui concorrono, indipendentemente dal tipo, dal formato e dai supporti di memorizzazione utilizzati.

Il livello di rischio viene definito in funzione del valore dei

macrodati, delle minacce cui sono sottoposti e delle vulnerabilità degli strumenti e delle infrastrutture di supporto (applicazioni, sistemi, reti, ubicazioni) che li gestiscono:

Rischio = f (Valore, Minacce, Vulnerabilità)

Pertanto il modello di riferimento utilizzato per l'analisi dei rischi può essere riassunto dalla seguente rappresentazione grafica:



Fasi dell'analisi dei rischi

Al fine di individuare i macrodati che costituiscono il patrimonio informativo aziendale, valutarne la criticità e la relativa esposizione al rischio e definire le contromisure di sicurezza da adottare, devono essere svolte le fasi descritte nel seguito.

Fase 1: Identificazione dei macro processi aziendali e mappatura dei sistemi informativi

Obiettivo principale della fase 1 è la rilevazione e la classificazione dei macro processi e dei sistemi informativi di supporto ai processi aziendali, identificando in maniera puntuale l'ambito di applicazione dell'analisi dei rischi.

L'identificazione dei macro processi permette di delineare la struttura dei flussi informativi che si generano durante le varie attività di cui i processi si compongono. Questa analisi rappresenta perciò la base di partenza su cui effettuare in seguito l'attività di classificazione delle informazioni, la stima delle minacce, l'analisi delle vulnerabilità e la determinazione dei livelli di rischio.

Fase 2: Classificazione del valore delle informazioni

La classificazione delle informazioni, con l'associazione del valore che le stesse hanno per l'organizzazione, è un processo fondamentale che costituisce la base per la valutazione dei rischi e consente parallelamente all'azienda di acquisire una miglior conoscenza del valore del proprio patrimonio informativo. La classificazione delle informazioni in termini di valore relativo (attività che può essere effettuata ai diversi livelli di aggregazione e che determina il valore assoluto dell'intero patrimonio informativo) esprime quindi la sensibilità e il livello di criticità che l'azienda attribuisce alle stesse.

Per rilevare il valore delle informazioni gestite si utilizza un'apposita matrice per ogni parametro di sicurezza (riservatezza, integrità, disponibilità) in cui deve essere riportato un giudizio sull'impatto provocato dall'eventuale verificarsi dell'evento descritto nelle rispettive colonne della matrice stessa. Successivamente viene calcolato il valore aggregato delle informazioni sommando i valori dei singoli parametri. Infine, in base al valore ottenuto, si associa l'informazione ad una categoria di criticità.

Fase 3: Stima delle minacce e analisi delle vulnerabilità

Stima delle minacce

La valutazione delle minacce è il processo che porta all'identificazione degli eventi che possono avere un impatto negativo sul valore del patrimonio informativo.

La valutazione delle minacce consiste nell'assegnare un valore che rappresenta la percezione del livello delle minacce per le informazioni aziendali. Questa valutazione viene fatta rispetto a diverse categorie di minacce, risultanti dalla fonte (ad es. interna/esterna) dalla natura (ad es. ostile/non ostile) e della complessità (ad es. strutturata/non strutturata).

Analisi delle vulnerabilità

Il processo di definizione della vulnerabilità dei sistemi informativi consiste nella valutazione e identificazione dei parametri da associare alle minacce precedentemente rilevate. Le vulnerabilità vengono definite come gap tra lo stato attuale delle informazioni e le aspettative di protezione ritenute adeguate e tali da impedire ad un agente esterno la compromissione delle informazioni. Le vulnerabilità analizzate dalla metodologia prevedono sia aspetti di natura tecnica, legati alla sicurezza logica o fisica degli strumenti e delle infrastrutture di supporto, sia aspetti di natura organizzativa, legati ad esempio alle procedure di lavoro o alle responsabilità del personale.

Le vulnerabilità delle applicazioni possono essere classificate secondo diverse categorie: controllo accessi, sviluppo e manutenzione, gestione degli outsourcer, auditing e log, backup, ecc.

Il livello di vulnerabilità di ogni applicazione dipende anche da quello della rete e dei sistemi necessari per l'operatività della stessa, le quali a loro volta possono essere classificate secondo ulteriori categorie (sicurezza dei sistemi operativi, antivirus, backup e disaster recovery, auditing e log, gestione degli outsourcer per quanto riguarda i sistemi; sicurezza infrastrutturale, accessi remoti, auditing e log per quanto riguarda la rete).

Inoltre, poiché le vulnerabilità dipendono anche dai luoghi fisici dove si svolgono le attività dei processi aziendali o dove sono collocati i supporti e le infrastrutture, vengono valutate anche le vulnerabilità delle ubicazioni raggruppate per categorie: perimetro di protezione, posizionamento e protezione delle apparecchiature, norme comportamentali, sistemi di controllo ambientale, controllo accessi fisici, aree di carico e scarico, protezione delle apparecchiature in entrata e in uscita, protezione dei cablaggi.

Ad ogni vulnerabilità è associato un peso che rappresenta il livello di rischio dovuto alla presenza di quella determinata vulnerabilità.

La suscettibilità è un indicatore che rappresenta l'esposizione al rischio delle informazioni ed è correlata alla presenza delle vulnerabilità e delle minacce. In particolare, il contributo di ogni singola vulnerabilità al valore della suscettibilità è determinato dal suo peso e dalla presenza di minacce che possono sfruttare tale vulnerabilità.

Fase 4: Definizione dei livelli di rischio ed identificazione delle misure di sicurezza da adottare

Il modello dei rischi utilizzato dalla metodologia prevede che il rischio sia determinato in funzione della combinazione del valore delle informazioni, della tipologia di minacce cui sono sottoposte e delle vulnerabilità.

Pertanto le informazioni raccolte nelle fasi precedenti consentono la determinazione del livello di rischio per ogni applicazione, definito nel seguente modo:

*Rischio = Valore * Suscettibilità*

In base al valore così ottenuto, si attribuisce una categoria di rischio (basso, medio, alto).

La valutazione del rischio ottenuta tramite l'utilizzo della metodologia costituisce il punto di partenza e la base su cui applicare le policy aziendali e predisporre piani di intervento a livello di singola area che siano omogenei ed allineati ai requisiti definiti a livello centrale.

Allegato 2.6 Symantec Security Risk Analysis Methodology (SSRAM)

Informazione fornita da Andrea Rigoni di Symantec

Che cosa è

Symantec Security Risk Analysis Methodology (SSRAM) è una metodologia sviluppata da Symantec che aiuta le organizzazioni a misurare il proprio livello di esposizione al rischio e a identificare un corretto piano di contromisure. SSRAM è inoltre un **framework** di riferimento che Symantec ha adottato nella realizzazione di servizi a supporto del Risk Management.

A chi è rivolto

SSRAM è rivolto a tutte le organizzazioni che hanno la necessità non solo di misurare il livello di rischio del proprio sistema informativo, ma anche di avviare i corretti processi di management e di controllo per governare il rischio in modo continuativo.

Principi base

SSRAM si basa sulla metodologia ISO/IEC 17799 per identificare il rischio totale per i servizi e gli asset identificati. Questo approccio fornisce informazioni statistiche che mostrano quali servizi e componenti siano esposti a maggiori rischi e che richiedono maggiore protezione. I rischi di base sono verificati partendo dal presupposto che non ci siano contromisure di sicurezza attive, fornendo quindi una visione oggettiva del rischio complessivo. I controlli di sicurezza previsti dalla ISO/IEC 17799:2000 sono raggruppati assieme per formare dei **filtri** (insiemi di contromisure) e vengono impiegati per calcolare la riduzione del rischio dovuta alla loro applicazione. Tutti i valori prodotti sono basati sulla visibilità che ha Symantec su nuove vulnerabilità, nuove minacce ed il loro impatto sui servizi ICT.

Strumenti e servizi

La metodologia SSRAM prevede sia una fase di misurazione del rischio, sia una fase di controllo costante.

Per supportare il cliente nell'utilizzo di questa metodologia, è disponibile SSRAM Toolkit, uno strumento software che aiuta il cliente in tutte le fasi di misurazione, di valutazione e di simulazione.

Le vulnerabilità e le minacce sono in continuo mutamento: ogni giorno vengono mediamente scoperte otto nuove vulnerabilità legate a tecnologie e prodotti commerciali. Inoltre, tutte le ultime minacce globali hanno colpito la maggior parte dei sistemi vulnerabili nell'arco di poche ore dalla loro comparsa. Per supportare la valutazione continua del profilo di vulnerabilità, minaccia ed impatto sui servizi, SSRAM prevede una classificazione ed una serie di metriche di valutazione delle vulnerabilità e delle minacce che possono essere utilizzate per alimentare un proprio database con servizi di Security Intelligence esterni.

Inoltre, è disponibile una metodologia, legata ad SSRAM, per l'avviamento di processi di controllo, monitoraggio e reazione agli incidenti, finalizzati alla riduzione o all'annullamento dell'impatto.

SICUREZZA DELLE RETI

dall'analisi del rischio
alle strategie di protezione

ALLEGATO 3
Elenco degli acronimi

Acronimi e abbreviazioni

Acronimo/Abbrev.	*Descrizione*
ADSL	*Asymmetric Digital Subscriber Line*
AIPA	*Autorità per l'Informatica nella Pubblica Amministrazione*
AP	*Access Point*
BSI	*British Standards Institute*
CA	*Certificazion Authority*
CC	*Common Criteria*
CENTR	*Council of European National Top Level Domain Registries*
CERT	*Computer Emergency Response Team*
CERT-AM	*CERT dell'Amministrazione Pubblica*
CNIPA	*Centro nazionale per l'informatica nella pubblica amministrazione*
CNR	*Consiglio Nazionale delle Ricerche*
CNSI	*Centro Nazionale per la Sicurezza Informatica*
CObIT	*Control Objectives for Information and related Tecnology*
COSO	*Committee of Sponsoring Organizations of the Treadway Commission*
CRAMM	*Risk Analysis and Management Methodology*
CRL	*Certificate Revocation List*
CSIRT	*Computer Security Incident Response Team*
DMZ	*Demilitarized Zone*
DNS	*Domain Name System*
EAP	*Extensible Authentication Protocol*
EFS	*Encrypting File System*
ENISA	*European Network and Information Security Agency*

Acronimo/Abbrev.	Descrizione
GMITS	Guidelines for the Management of IT Security
GSM	Global System for Mobile Communication
GPRS	General Packet Radio Service
HIDS	Host Intrusion Detection System
IANA	Internet Assigned Number Authority
ICANN	Internet Corporation for Assigned Names and Numbers
ICT	Information & Communication Technology
IdM	Identity Management
IDS	Intrusion Detection System
IETF	Internet Engineering Task Force
IPSec	IP Security
ISACA	Information System Audit and Control Association
ISDN	Integrated Services Digital Network
ISF	Information Security Forum
ISMS	Information Security Management System
ISO	International Standard Organisation
ISOC	Internet Society
LAN	Local Area Network
LDAP	Lightweight Directory Access Protocol
MPLS	Multi Protocol Label Switching
MSS	Managed Security Services
MSSP	Managed Security Service Provider
NAT	Network Address Traslation
NAT/PAT	Network Address Traslation/Port Address Traslation
NDA	non-disclosure agreement
NIDS	Network Intrusion Detection System
OCSE	Organizzazione per la Cooperazione e lo Sviluppo Economico
OTP	One time password
PA	Pubblica Amministrazione
PEAP	Protected Extensible Authentication Protocol
PIN	Personal Identification Number
PKI	Public Key Infrastructure
PMI	Privilege Management Infrastructure
PPAA	Pubbliche Amministrazioni
RADIUS	Remote Authentication Dial-In User Service
RAS	Remote Access Service

Acronimo/Abbrev.	Descrizione
RIPE NCC	Reseaux IP Européen Network Coordination Centre
ROI	Return on Investement
RTO	Recovery Time Objective
RUPA	Rete Unitaria della Pubblica Amministrazione
S/MIME	Secure Multipurpose Internet Mail Extensions
SIA	Sistema Informativo Aziendale
SOC	Security Operations Center
SPC	Sistema Pubblico di Connettività
SSL	Secure Sockets Layer
SSO	Single Sign On
TACACS	Terminal Access Controller Access Control System
TCP/IP	Transmission Control Protocol/ Internet Protocol
TLS	Transport Layer Security
UE	Unione Europea
UMTS	Universal Mobile Telecommunications System
URL	Uniform Resource Locator
VPN	Virtual Private Network
W3C	World Wid Web Consortium
WAN	Wide-Area Network
WEP	Wired Equivalent Privacy

Stampa: Pool Grafica Editrice S.r.l.
Via Crespina 42, 00146 Roma