

**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**

**Sicurezza delle reti e sicurezza dell'informazione:
proposta di un approccio strategico europeo**

Sommario

1.	Introduzione.....	3
2.	Analisi della problematica legata alla sicurezza delle reti e dell'informazione.....	5
2.1.	Cosa si intende per sicurezza delle reti e dell'informazione	5
2.2.	Quadro generale delle minacce alla sicurezza.....	6
2.2.1.	Intercettazione delle comunicazioni.....	6
	Accesso non autorizzato a computer e reti informatiche	8
2.2.3.	Caduta della rete.....	9
2.2.4.	Esecuzione di "software maligni" (malicious software) che modificano o distruggono i dati.....	10
2.2.5.	Usurpazione di identità	11
2.2.6.	Incidenti ambientali ed eventi imprevisti.....	12
2.3.	Le nuove sfide	13
3.	Un approccio europeo.....	14
3.1.	Giustificazione di un intervento pubblico	14
3.2.	Sensibilizzazione.....	17
3.3.	Un sistema europeo di segnalazione e di informazione.....	18
3.4.	Sostegno tecnologico	19
3.5.	Sostegno alle attività di normalizzazione e certificazione in una logica di mercato	19
3.6.	Quadro giuridico.....	21
3.7.	La sicurezza nella pubblica amministrazione	23
3.8.	Cooperazione internazionale	23
4.	Prossime fasi	24

1. INTRODUZIONE

Le preoccupazioni in materia di sicurezza delle reti elettroniche e dei sistemi di informazione sono aumentate parallelamente al rapido incremento del numero di utenti e del valore delle transazioni effettuate sulle reti stesse. La sicurezza ha assunto un'importanza critica tale da farne un presupposto indispensabile per la crescita delle imprese di commercio elettronico e per il funzionamento dell'economia nel suo complesso. Il fatto che la sicurezza delle informazioni e delle comunicazioni figurino ormai in testa delle priorità politiche dell'Unione europea è dovuto a diversi fattori:

- I governi sono ormai consapevoli della forte dipendenza delle loro economie e dei loro cittadini da un efficace funzionamento delle reti di comunicazione e non pochi sono quelli che hanno cominciato il riesame delle disposizioni relative alla sicurezza.
- Grazie ad Internet si è venuto a creare un tessuto di connessioni globali che collega tra loro milioni di reti, grandi e piccole, centinaia di milioni di PC ed un numero crescente di altri apparecchi come i telefoni mobili. Tutto ciò ha determinato ad una significativa riduzione dei costi di accesso ad informazioni economiche preziose per i pirati informatici.
- Internet è il canale di transito di famosi virus informatici che in passato hanno causato ingenti danni dovuti alla distruzione dei dati e all'impossibilità di accedere alle reti. Tali problemi di sicurezza non riguardano un unico paese ma si propagano rapidamente tra gli Stati membri.
- Nel varare il piano d'azione eEurope 2002, i Consigli europei di Lisbona e di Feira hanno riconosciuto il ruolo di Internet quale importante motore della produttività dell'economia degli Stati membri dell'UE.

A fronte di questa situazione il Consiglio europeo di Stoccolma del 23 e 24 marzo 2001 ha deciso che *"il Consiglio svilupperà insieme alla Commissione una strategia globale per la sicurezza delle reti elettroniche, comprensiva di azioni concrete di attuazione. Tale strategia dovrebbe essere presentata in tempo per il Consiglio europeo di Göteborg."* La presente comunicazione costituisce la risposta della Commissione europea alla richiesta del Consiglio europeo.

Un ambiente in piena mutazione

La sicurezza è ormai una delle sfide più importanti con cui devono misurarsi i responsabili politici, i quali hanno ormai compreso le complesse implicazioni di una risposta adeguata al problema. Fino a pochi anni addietro la sicurezza delle reti era una questione che riguardava essenzialmente le imprese monopolistiche che fornivano servizi specializzati sulle reti pubbliche, in particolare sulla rete telefonica. La sicurezza dei sistemi informatici era un problema che riguardava solo le grandi organizzazioni e si limitava sul controllo degli accessi, per cui la definizione di una politica di sicurezza era un compito relativamente semplice. Successivamente, però, la situazione è notevolmente cambiata per effetto di una serie di fatti nuovi che hanno caratterizzato il mercato nella sua accezione più ampia, in particolare la liberalizzazione, la convergenza e la globalizzazione:

La proprietà e la gestione delle reti sono soprattutto private. I servizi di comunicazione sono aperti alla concorrenza e la sicurezza è un aspetto dell'offerta di mercato. Molti utenti non sono

tuttavia consapevoli dei rischi di sicurezza che corrono quando si collegano ad una rete e decidono pertanto senza piena cognizione di causa.

Le reti e i sistemi di informazione convergono. Le reti sono sempre più interconnesse tra loro, veicolano lo stesso tipo di servizi permanenti e personalizzati e condividono, in una certa misura, le stesse infrastrutture. I terminali (PC, telefoni mobili, ecc.) sono diventati elementi attivi dell'architettura di rete e possono essere collegati a reti diverse.

Le reti sono internazionali. Una quota sostanziale delle comunicazioni attuali è di tipo transfrontaliero o transita comunque da paesi terzi (talvolta senza che l'utente ne sia a conoscenza). Le soluzioni destinate a far fronte ai rischi di sicurezza devono necessariamente tener conto di questa situazione. La maggior parte delle reti è costituita da prodotti commerciali di imprese internazionali. I prodotti destinati alla sicurezza devono essere conformi alle norme internazionali.

Rilevanza sotto il profilo strategico

Gli sviluppi sopra ricordati limitano la possibilità delle autorità nazionali di intervenire sul livello di sicurezza delle comunicazioni elettroniche di cittadini ed imprese. Ciò non significa tuttavia che il settore pubblico non abbia più alcun ruolo da svolgere in questo campo.

Innanzitutto, **esistono a livello comunitario misure legislative specifiche che interessano la sicurezza delle reti e dell'informazione.** Prima fra tutte, il quadro normativo europeo sulle telecomunicazioni e sulla protezione dei dati obbliga operatori e fornitori di servizi a garantire un livello di sicurezza commisurato ai rischi.

In secondo luogo, crescono le preoccupazioni per la **sicurezza nazionale** in quanto i sistemi informativi e le reti di comunicazione sono ormai elementi costitutivi critici di altre infrastrutture (ad es. reti di fornitura idrica ed elettrica) e di altri mercati (ad es. il mercato finanziario internazionale).

Infine, vi sono ragioni che militano a favore di un intervento delle autorità nazionali per correggere **le imperfezioni del mercato.** I prezzi di mercato non sempre rispecchiano fedelmente i costi e i benefici derivanti dagli investimenti effettuati per migliorare la sicurezza delle reti e né gli operatori né gli utenti sopportano sempre le conseguenze del loro comportamento. Occorre tenere presente che oggi il controllo sulla rete non è una funzione centralizzata e le debolezze di un sistema possono essere sfruttate per attaccare un altro sistema. La complessità delle reti è tale che per gli utenti è arduo valutare i rischi potenziali.

La presente comunicazione intende pertanto individuare i settori nei quali sono necessari nuovi o più incisivi interventi del settore pubblico, a livello europeo o nazionale.

Nel **capitolo 2** vengono definiti i concetti di sicurezza delle reti e di sicurezza dell'informazione, vengono descritte le principali minacce alla sicurezza e valutate le soluzioni attualmente disponibili. Scopo del capitolo è fornire sufficienti elementi per la comprensione della problematica della sicurezza delle reti e dell'informazione che consenta di vagliare le soluzioni strategiche presentate nel capitolo successivo. L'intenzione non è quella di fornire un quadro tecnico completo dei problemi della sicurezza.

Nel **capitolo 3** si propone un approccio europeo inteso a migliorare la sicurezza delle reti e dell'informazione cercando di individuare le aree in cui l'intervento pubblico può integrare le soluzioni fornite dal mercato con interventi a livello politico. In ossequio alla richiesta del Consiglio europeo di Stoccolma vengono elencate misure strategiche concrete. L'approccio strategico proposto va visto come parte integrante dell'attuale normativa in materia di servizi di comunicazione elettronica e di protezione dei dati e - più di recente - criminalità informatica.

2. ANALISI DELLA PROBLEMATICHE LEGATA ALLA SICUREZZA DELLE RETI E DELL'INFORMAZIONE

2.1. Cosa si intende per sicurezza delle reti e dell'informazione

Le reti sono sistemi che consentono di conservare, elaborare e veicolare i dati. Si compongono di elementi trasmissivi (cablaggio, collegamenti senza filo, satelliti, *router*, *gateway*, commutatori, ecc.) e di servizi di supporto (sistema dei nomi di dominio - DNS con relativo *root server*, servizio di identificazione della linea chiamante, servizi di autenticazione, ecc.). Le reti sono collegate a svariati applicativi (sistemi di consegna di posta elettronica, *browser*, ecc.) e apparati terminali (apparecchio telefonico, computer *host*, PC, telefono mobile, palmare, elettrodomestici, macchinari industriali, ecc.).

I requisiti generici di sicurezza delle reti e dei sistemi di informazione presentano le seguenti caratteristiche interdipendenti:

- i) **Disponibilità:** è la conferma che i dati sono accessibili e i servizi funzionano anche in caso di interruzioni dovute alla cessazione dell'alimentazione elettrica, a catastrofi naturali, eventi imprevisti o ad attacchi di pirateria informatica. Si tratta di un requisito fondamentale nei casi in cui l'indisponibilità di una rete di comunicazione può causare interruzioni in altre reti importantissime quali quelle dei trasporti aerei o dell'alimentazione elettrica.
- ii) **Autenticazione:** è la conferma dell'identità dichiarata da un organismo o un utente. 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 le banche Internet). 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.
- iii) **Integrità:** è la conferma che i dati trasmessi, ricevuti o conservati sono completi e inalterati. Il requisito dell'integrità dei dati è particolarmente importante per le procedure di autenticazione nella conclusione dei contratti o quando è indispensabile garantire l'accuratezza dei dati (dati medici, progettazione industriale, ecc.).
- iv) **Riservatezza:** è la protezione dei dati trasmessi o conservati per evitarne l'intercettazione e la lettura da parte di persone non autorizzate. La riservatezza è particolarmente necessaria per la trasmissione di dati sensibili ed è uno dei requisiti che garantiscono il rispetto della vita privata degli utenti delle reti di comunicazione.

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 costosi che un attacco doloso.

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

2.2. Quadro generale delle minacce alla sicurezza

Le imprese che operano in rete per vendere prodotti o organizzare la consegna di forniture possono essere paralizzate da un attacco di tipo "denial of service" (diniego di servizio). Informazioni personali e finanziarie possono essere intercettate ed utilizzate per scopi non consentiti. La stessa sicurezza nazionale può trovarsi minacciata. Questi sono solo esempi dei rischi che si possono correre a causa di un inadeguato livello di sicurezza. Occorre distinguere tra attacchi dolosi (capitoli da 2.2.1 a 2.2.5) ed eventi imprevisti (capitolo 2.2.6). Lo scopo di questi capitoli è descrivere i diversi tipi di rischio al fine di creare le basi per un approccio strategico inteso a migliorare la sicurezza (cfr. capitolo 3).

2.2.1. 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 i *router*, le *gateway*, i commutatori e i *server* di rete.

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. Ogni paese dispone di una specifica normativa che consente alle forze dell'ordine di chiedere al giudice un decreto (nel caso di due Stati membri, un'ordinanza del ministro) che autorizza l'intercettazione.

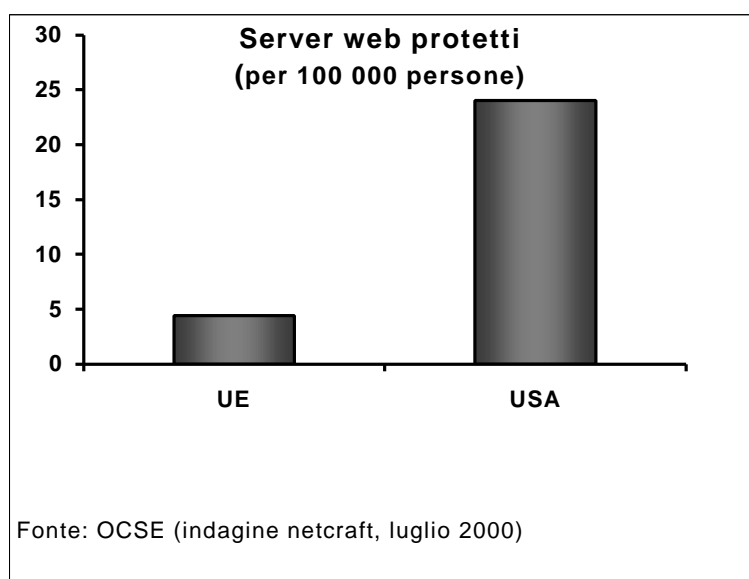
Danni potenziali - Un'intercettazione illecita può configurarsi come una violazione del diritto alla vita privata di una persona oppure come uso indebito dei dati intercettati, come una *password* o gli estremi di una carta di credito, per fini di lucro o per sabotaggio. Si tratta di uno dei principali ostacoli alla diffusione del commercio elettronico in Europa.

Soluzioni possibili – Le difese contro le intercettazioni possono essere attuate dagli **operatori** (protezione della rete), come previsto, tra l'altro, dalla direttiva 97/66/CE¹, 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. 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. L'obbligo di autorizzare le intercettazioni legali fa sì che nella maggior parte degli Stati membri l'efficacia dei dispositivi di cifratura sia inferiore a quanto permetterebbero le tecnologie disponibili. Per lo stesso motivo, la cifratura può essere attivata o disattivata dalle stazioni di base senza che l'utente ne sia a conoscenza.

¹ Direttiva sul trattamento dei dati personali e sulla tutela della vita privata nel settore delle telecomunicazioni (GU L 24 del 30.1.1998).

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 praticamente tutti i tipi di comunicazioni². Vi sono prodotti specifici destinati a criptare le conversazioni telefoniche o le trasmissioni via fax. Anche la posta elettronica può essere criptata mediante software dedicati, moduli di cifratura integrati nel programma di trattamento testi oppure software cliente di posta elettronica. Il problema è che se l'utente cripta 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 "Secure Socket Layer" (SSL), un sistema che cripta le comunicazioni tra il server del web e 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 comunitario più liberale in

materia di controllo sulle esportazioni di prodotti e tecnologie a duplice uso³. Le statistiche rivelano che il numero di *server web* protetti in Europa è largamente inferiore a quello degli Stati Uniti (cfr. grafico).

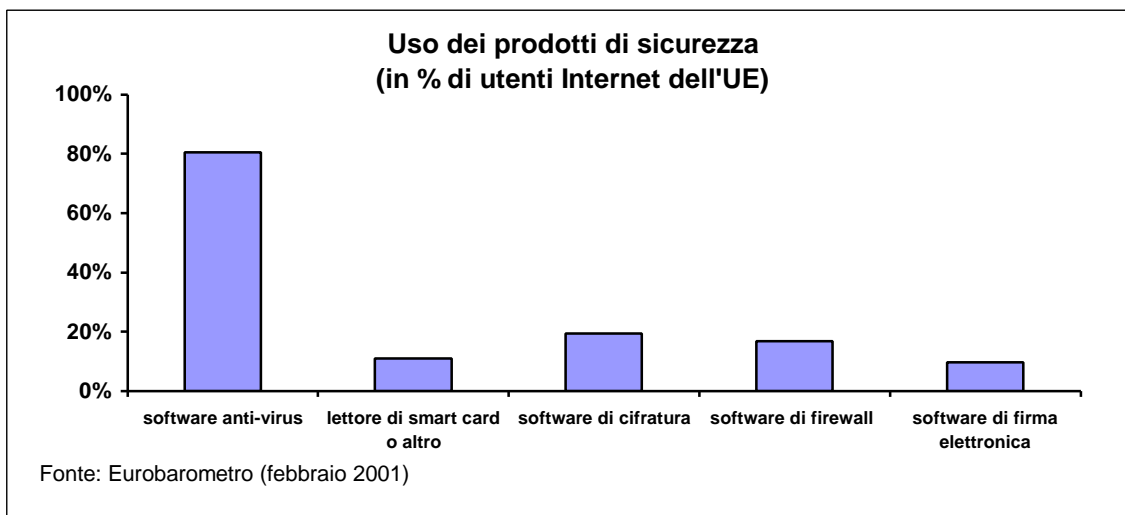
Operatori, utenti e produttori sono confrontati al problema della concorrenza e della non interoperabilità tra le norme esistenti. Ad esempio, in materia di protezione della posta elettronica due norme si contendono la supremazia sul mercato⁴. L'importanza dell'Europa in questo campo è limitata. Ne risulta una profusione di prodotti non europei che applicano queste norme e il cui utilizzo da parte degli utenti europei è subordinato alla politica in materia di controllo delle esportazioni americana. Desto preoccupazione, inoltre, il livello di sicurezza garantito da molti di questi prodotti (cfr. Echelon⁵) e alcuni Stati membri stanno valutando la possibilità di aumentare

² Cfr. comunicazione della Commissione "Garantire la sicurezza e l'affidabilità nelle comunicazioni elettroniche", dell'8 ottobre 1997, COM(1997) 503 def.

³ Regolamento (CE) n. 1334/2000 del Consiglio che istituisce un regime comunitario di controllo delle esportazioni di prodotti e tecnologie a duplice uso.

⁴ S-MIME (secure multiple Internet mail extensions) e OpenPGP (Pretty Good Privacy) sono entrambe norme elaborate dall'IETF (Internet Engineering Task Force).

⁵ Si dice che il sistema ECHELON viene utilizzato per intercettare le normali e-mail, fax, telex e comunicazioni telefoniche trasmesse sulle reti di telecomunicazioni di tutto il mondo. Si vedano al riguardo le attività del comitato temporaneo del Parlamento europeo su Echelon (http://www.europarl.eu.int/committees/echelon_home.htm).



il livello di riservatezza dei prodotti avvalendosi di software di tipo *open source*. Queste attività, tuttavia, si trovano ancora in una fase pilota⁶, 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*.

2.2.2. Accesso non autorizzato a computer e reti informatiche

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 interne, 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.

Danni potenziali - 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 (spesso detta '*hacking*', seccante) 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, in particolare finanziari, numero di conto e dati 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*.

Soluzioni possibili – I metodi più comunemente utilizzati per difendersi dall'accesso non autorizzato consistono nell'installare una *password* 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 cards*). L'efficacia di questi sistemi dipende dal modo in cui le loro caratteristiche si contrappongono ai rischi inerenti ad 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

⁶ Il governo tedesco finanzia attualmente un progetto basato sulla norma OpenPGP, chiamato GNUPG (<http://www.gnupg.org>).

utenti e i fornitori non saranno pienamente consapevoli della vulnerabilità delle loro reti le soluzioni potenziali rimarranno inesplorate. Il grafico qui sotto 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).

2.2.3. Caduta della rete

Gran parte delle reti sono ormai informatizzate e pilotate 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 computer che gestiscono il traffico. In futuro, tuttavia, le reti telefoniche potrebbero essere più vulnerabili a questi attacchi perché contengono 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 di quest'anno sono state evidenziate lacune nel software utilizzato dalla maggior parte dei *server* di nomi di dominio.⁷
- **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 Flooding (saturazione) e Denial of service (diniego di servizio):** questo tipo di attacchi paralizza la rete sovraccaricandola di messaggi artificiali che impediscono o riducono le possibilità di accesso legittimo da parte degli utenti. È un fenomeno simile a quello degli apparecchi fax bloccati da messaggi lunghi e ripetuti. Il *flooding* consiste nel tentativo di sovraccaricare i *server web* o la capacità di trattamento dei fornitori di servizi Internet con messaggi generati automaticamente.

Danni potenziali - 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 immateriale in termini di immagine. Le imprese si avvalgono

⁷ Fonte: CERT/CC (<http://www.cert.org/advisories/CA-2001-02.html>).

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.

Soluzioni possibili - 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 clienti 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.

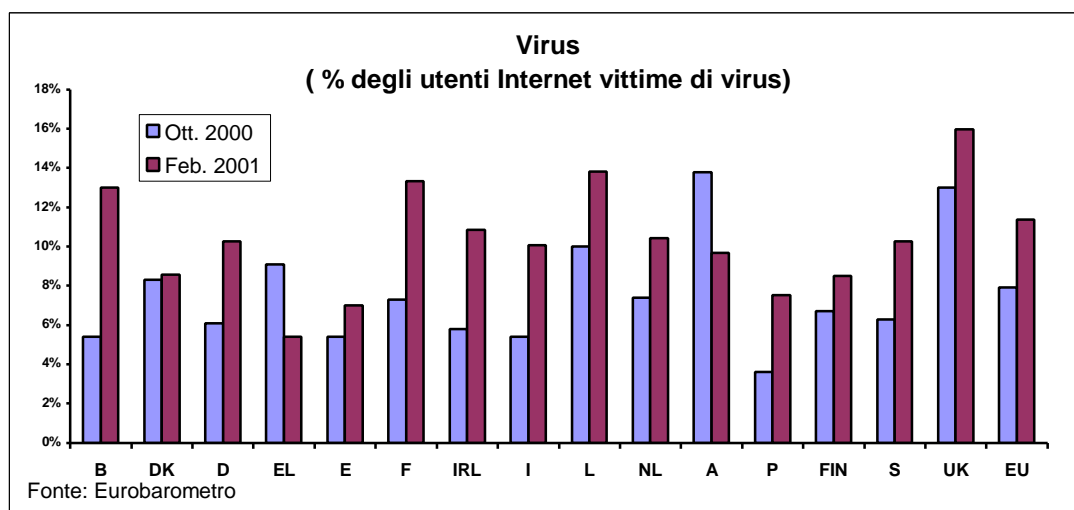
Il volume di dati trasmessi impedisce di filtrare con precisione il traffico perché una tale verifica paralizzerebbe la rete. Per lo stesso motivo, la rete effettua solo funzioni di filtraggio e di controllo dell'accesso poco sofisticate. Le funzioni di sicurezza più specifiche (autenticazione, integrità, cifratura) sono implementate alle estremità della rete, vale a dire sui terminali e i *server* che fungono da punti terminali.

2.2.4. Esecuzione di "software maligni" (*malicious software*) che modificano o distruggono i dati

I computer funzionano con i software. I software, però, possono essere utilizzati 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 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.

Danni potenziali - 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, 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.



Soluzioni possibili - 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 del software di difesa antivirus.

2.2.5. 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.

Danni potenziali - 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 denuncia 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.

Soluzioni possibili - L'introduzione di un'autenticazione legata all'introduzione 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 alcuna garanzia di non essere stati contraffatti. Un terzo, spesso chiamato "autorità di certificazione" o, nella direttiva sulla firma elettronica⁸, "prestatore di servizi di certificazione", può presentare tali garanzie. Il problema legato alla diffusione di questa soluzione è simile a quello incontrato in materia di cifratura, ossia la necessità di un'interoperabilità 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.

2.2.6. 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).

Danni potenziali: 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.

Soluzioni possibili: 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 sua rete di appartenenza non sia disponibile (come i passeggeri vengono trasferiti verso un'altra compagnia aerea in caso di annullamento del loro volo). 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

⁸ Direttiva 1999/93/CE del Parlamento europeo e del Consiglio, del 13 dicembre 1999, relativa ad un quadro comunitario per le firme elettroniche (GU L 13 del 19.1.2000, pag. 12).

catastrofe naturale (cfr. direttiva 97/33/CE sull'interconnessione⁹ e direttiva 98/10/CE sulla telefonia vocale¹⁰). 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.

2.3. Le nuove sfide

La sicurezza delle reti e dell'informazione è chiamata 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.

- i. Le reti e i sistemi di informazione 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 in 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, per cui 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 manodopera per ripristinare la rete) ma anche diversi costi immateriali, in particolare in termini di immagine, difficili da quantificare.

- ii. **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*) che recano, 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

⁹ GU L 199 del 26.7.1997.

¹⁰ GU L 101 dell'1.4.1998.

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 tenderanno 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.
- 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 networks*, 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.

3. UN APPROCCIO EUROPEO

3.1. Giustificazione di un intervento pubblico

La protezione delle reti di comunicazione ha acquistato le caratteristiche di una questione prioritaria per i responsabili politici per motivi riconducibili alla protezione dei dati, al funzionamento dell'economia, alla sicurezza nazionale e alla volontà di promuovere il commercio elettronico. Ciò spiega la presenza di una serie di salvaguardie nelle direttive dell'UE sulla protezione dei dati e nel quadro normativo per le telecomunicazioni (come già accennato al punto 3.6). Tali misure devono tuttavia essere applicate in un ambiente in costante mutazione caratterizzato da nuove tecnologie, mercati concorrenti, convergenza delle reti e globalizzazione. Affrontare tali sfide è ancor più difficile perché il mercato avrà tendenza a ridurre gli investimenti in sicurezza per i motivi esposti qui di seguito.

La sicurezza delle reti e dell'informazione è una merce comprata e venduta sul mercato ed è ormai parte integrante delle clausole contrattuali siglate tra le parti. Il mercato dei prodotti di sicurezza ha conosciuto una forte crescita negli ultimi anni: secondo certi studi il mercato mondiale dei software per la sicurezza di Internet aveva un valore di circa 4,4 miliardi di USD alla fine del 1999¹¹, valore che aumenterà del 23% all'anno sino a raggiungere 8,3 miliardi di USD nel 2004. In Europa, le previsioni indicano che il mercato dei prodotti di sicurezza per le comunicazioni elettroniche passerà da 465 milioni di USD nel 2000 a 5,3 miliardi di USD

¹¹ IDC: Internet security market forecast and analysis, 2000-2004 Report #W23056 - ottobre 2000.

nel 2006¹², mentre il mercato della sicurezza delle tecnologie dell'informazione passerà da un valore di 490 milioni di USD nel 1999 a 2,74 miliardi di USD nel 2006¹³.

Generalmente, l'ipotesi implicita è che basterà il meccanismo dei prezzi per garantire l'equilibrio tra costi di protezione delle reti ed esigenze specifiche di sicurezza. Alcuni utenti esigeranno un livello più elevato di sicurezza mentre per altri sarà sufficiente un livello inferiore, anche se le autorità pubbliche potrebbero imporre un livello minimo. La scelta degli utenti si rifletterà nel prezzo che saranno disposti a sborsare per proteggersi. Tuttavia, come indica l'analisi del capitolo 2, per numerosi rischi le soluzioni non esistono ancora o vengono difficilmente messe in commercio a causa di talune imperfezioni del mercato:

- i) **Costi e benefici sociali.** Gli investimenti per migliorare la sicurezza delle reti generano costi e benefici sociali che i prezzi di mercato non rispecchiano adeguatamente. **Dal punto di vista dei costi**, i soggetti del mercato non rispondono per i danni derivanti dal loro comportamento in relazione alla sicurezza. Gli utenti e i fornitori che adottano un basso livello di sicurezza non incorrono in una responsabilità civile. La situazione è simile a quella di un conducente distratto che non è ritenuto responsabile del costo del traffico venutosi a creare a causa dell'incidente che ha provocato. Anche su Internet molti attacchi hanno avuto per bersaglio le apparecchiature scarsamente protette di utenti relativamente negligenti. **Ma i prezzi di mercato non rispecchiano neppure i benefici della sicurezza.** Quando gli operatori, i fornitori o i prestatori di servizi accrescono il livello di sicurezza dei loro prodotti molti dei benefici dei loro investimenti giovano non solo ai loro clienti ma a tutti coloro che, direttamente o indirettamente, fanno uso delle comunicazioni elettroniche, in altre parole all'economia nel suo complesso.
- ii) **Asimmetria dell'informazione.** Le reti diventano sempre più complesse e raggiungono un mercato più ampio che comprende molti utenti con una scarsa conoscenza delle tecnologie e dei loro rischi potenziali. Ciò significa che gli utenti non saranno pienamente consapevoli dei rischi in materia di sicurezza e che molti operatori, produttori di software e fornitori di servizi avranno difficoltà a stabilire l'entità e l'estensione della vulnerabilità. Molti nuovi servizi, applicativi e software presentano caratteristiche affascinanti che sono spesso fonte di maggiore vulnerabilità dei sistemi (ad es. il successo del *World Wide Web* è parzialmente dovuto alla gamma di applicativi multimediali che possono essere facilmente scaricati, ma questi software 'plug-in' sono spesso porte di accesso per gli attacchi di pirateria). Se i benefici sono visibili, i rischi sono invece invisibili ed i fornitori sono più motivati ad offrire nuove caratteristiche piuttosto che maggiore sicurezza.
- iii) **Problemi legati ad un intervento pubblico.** Gli operatori adottano sempre più spesso lo standard Internet o comunque collegano le proprie reti a Internet. Internet, tuttavia, non è una rete concepita obbedendo a criteri di sicurezza ma, al contrario, per garantire l'accesso e facilitare lo scambio di informazioni. Questa è stata del resto la chiave del suo successo. Internet è diventata una rete globale di reti, caratterizzata da un'ineguagliabile ricchezza e diversità. Gli investimenti in sicurezza spesso fruttificano solo se un certo numero di persone adottano lo stesso approccio. La ricerca di soluzioni per la sicurezza necessita pertanto di una **cooperazione**, ma la cooperazione è efficace solo se una massa critica di soggetti vi partecipa. È questa una condizione difficile da realizzare perché vi sono grossi vantaggi per chi opera per proprio conto. L'interoperabilità tra prodotti e servizi darà vita ad una

¹² Frost & Sullivan: The European Internet communication security markets, report 3717 - novembre 2000.

¹³ Frost & Sullivan: The European Internet system security markets, report 3847 - luglio 2000.

concorrenza tra i prodotti per la sicurezza. ma, i costi di coordinamento sono elevati in quanto potrebbero essere necessarie soluzioni globali, mentre taluni operatori sono tentati di imporre sul mercato soluzioni proprietarie. Poiché numerosi prodotti e servizi si basano ancora su soluzioni proprietarie non vi è alcun vantaggio nel ricorrere a norme sicure che rappresentano un maggiore livello di protezione solo se vengono adottate da tutti.

A causa di queste imperfezioni del mercato il quadro normativo per le telecomunicazioni e la protezione dei dati impone già ad operatori e fornitori di servizi l'obbligo di garantire ad un determinato livello di sicurezza nelle comunicazioni e nei sistemi di informazione. I motivi di una politica europea nel campo della sicurezza delle reti e dell'informazione potrebbero essere descritti nei seguenti termini. Innanzi tutto, le pertinenti normative dell'UE devono essere applicate in modo efficace, il che implica **una visione comune della sottostante problematica della sicurezza e delle misure specifiche da adottare**. Il quadro normativo è destinato ad evolvere in futuro, come del resto già evidenziato dalla proposta di nuovo quadro normativo per le comunicazioni elettroniche o dalle imminenti proposte collegate alla discussione sulla criminalità informatica. In secondo luogo, alcune imperfezioni del mercato inducono a concludere che le forze del mercato non riescono a generare investimenti sufficienti nelle tecnologie e nella cultura della sicurezza. **L'intervento pubblico può migliorare il funzionamento del mercato e nel contempo permettere una più efficace applicazione del quadro normativo**. Infine, dato che i servizi di comunicazione e di informazione sono essenzialmente transfrontalieri, è necessario un approccio strategico europeo **per garantire che il mercato interno di tali servizi possa avvalersi dei vantaggi delle soluzioni comuni ed operare efficacemente sulla scena mondiale**.

Le misure strategiche proposte in materia di sicurezza delle reti e dell'informazione vanno viste non solo nel contesto della vigente normativa sulle telecomunicazioni e la protezione dei dati ma anche in quello delle più recenti iniziative in materia di criminalità informatica. La Commissione ha recentemente pubblicato una comunicazione sulla criminalità informatica¹⁴ che, tra le altre iniziative, prevede l'istituzione di un forum UE sul "cybercrimine" per migliorare la comprensione reciproca e la cooperazione a livello comunitario tra tutte le parti interessate. Un'iniziativa in materia di sicurezza delle reti e dell'informazione costituirà l'anello mancante di questo quadro di riferimento. Il grafico qui sotto indica le tre aree strategiche ed illustra, con alcuni esempi, le loro interrelazioni.



¹⁴ Creare una società dell'informazione sicura migliorando la sicurezza delle infrastrutture dell'informazione e mediante la lotta alla criminalità informatica, COM(2000) 890. <http://europa.eu.int/ISPO/eif/internetPoliciesSite/Crime/crime1.html>

3.2. Sensibilizzazione

Troppi utenti, sia pubblici che privati, sono tuttora ignari dei rischi legati all'uso delle reti di comunicazione e delle soluzioni già escogitate per farvi fronte. Il problema della sicurezza è complesso e gli stessi esperti hanno talvolta difficoltà a valutare i rischi. La mancanza di informazioni è una delle anomalie del mercato alle quali la politica in materia di sicurezza deve porre rimedio. Vi è il pericolo che certi utenti, allarmati da numerosi rapporti sulle minacce alla sicurezza, rinuncino del tutto al commercio elettronico. Altri invece sono meno informati o sottovalutano il rischio e potrebbero agire imprudentemente. Alcune imprese potrebbero volontariamente minimizzare il rischio per timore di perdere clienti.

Paradossalmente, su Internet sono disponibili molte informazioni sulla sicurezza delle reti e dell'informazione e le riviste di informatica dedicano molto spazio all'argomento. Il problema per l'utente è ottenere informazioni adeguate e comprensibili, che siano aggiornate e rispondano alle sue esigenze. L'industria automobilistica è un eccellente esempio del modo in cui complesse norme di sicurezza possano trasformarsi in un importante argomento di marketing. Infine, il diritto comunitario obbliga i fornitori di un servizio di telecomunicazioni accessibile al pubblico ad informare gli abbonati in merito ai rischi di violazione della sicurezza della rete, alle possibili soluzioni e ai costi che ne derivano (cfr. articolo 4 della direttiva 97/66/CE).

Lo scopo delle iniziative di sensibilizzazione dei cittadini, delle amministrazioni e delle imprese è pertanto quello di mettere a loro disposizione informazioni accessibili, obiettive ed affidabili sulla sicurezza delle reti e dell'informazione. È necessaria una riflessione generale sulla sicurezza. Una volta sensibilizzato alla problematica, il pubblico potrà liberamente scegliere il livello di protezione a lui più confacente.

Azioni proposte

- Gli Stati membri devono varare una campagna di informazione e di educazione del pubblico e nel contempo aggiornare le iniziative in corso mediante una campagna su tutti i mass media diretta a tutti i soggetti interessati. Una campagna di informazione adeguata ed efficace è costosa. Per elaborare programmi informativi che presentino i rischi senza allarmare inutilmente il pubblico né incoraggiare i potenziali pirati occorre uno studio accurato.

La Commissione europea agevolerà lo scambio delle migliori pratiche adottate in questo campo e garantirà un certo livello di coordinamento comunitario delle campagne di informazione nazionali, in particolare per quanto riguarda il contenuto delle informazioni. Un elemento di questo approccio potrebbe essere un portale *web* a livello nazionale ed europeo. È inoltre opportuno prevedere un collegamento tra tali portali e siti *web* affidabili di partner internazionali.

- Gli Stati membri devono promuovere l'applicazione delle migliori pratiche in materia di sicurezza basate su dispositivi vigenti quali l'ISO/IEC 17799 (codice di buona pratica per la gestione della sicurezza dell'informazione - www.iso.ch). L'iniziativa dovrebbe avere per target principale le PMI. La Commissione sosterrà le iniziative degli Stati membri in questo senso.
- I sistemi scolastici degli Stati membri dovrebbero dedicare più spazio ai corsi incentrati sulla sicurezza. Occorre elaborare programmi di insegnamento a tutti i livelli, ad esempio una formazione in materia di rischi per la sicurezza delle reti aperte e vanno incoraggiate soluzioni efficaci, affinché diventino parte integrante del programma di informatica delle scuole.

Anche gli insegnanti devono ricevere una formazione in materia di sicurezza nei loro rispettivi programmi di formazione. La Commissione europea finanzia già lo sviluppo di nuovi moduli formativi curricolari nel quadro del proprio programma di ricerca.

3.3. Un sistema europeo di allarme ed informazione

Anche quando sono consapevoli dei rischi in materia di sicurezza gli utenti devono comunque essere informati delle nuove minacce. I pirati informatici troveranno inevitabilmente i punti deboli anche nel sistema di protezione più perfezionato. L'industria sviluppa continuamente nuovi applicativi e nuovi servizi, di migliore qualità, che rendono più attraente il mondo di Internet, ma che aprono involontariamente nuove breccie nelle barriere di sicurezza e quindi nuovi rischi.

Anche i tecnici di rete e i tecnici della sicurezza più esperti sono spesso presi alla sprovvista dal carattere innovativo di alcuni attacchi. È pertanto necessario predisporre un sistema di allarme tempestivo che possa rapidamente avvertire tutti gli utenti e disporre nel contempo di una fonte di consulenza rapida ed affidabile sul modo di arginare gli attacchi. Anche il mondo dell'economia necessita di un meccanismo riservato di segnalazione sugli attacchi subiti che non rischi di compromettere la fiducia del pubblico. A ciò deve aggiungersi una visione più lungimirante della sicurezza, che analizzi i dati concreti raccolti e valuti i rischi adottando una prospettiva più ampia.

Un lavoro di grande rilievo in questo campo viene svolto dagli organismi pubblici e privati di intervento in caso di emergenza informatica (CERT) o da organismi simili. Il Belgio, ad esempio, ha istituito un sistema di allarme virus che consente ai cittadini belgi di essere informati di una minaccia entro due ore. I CERT operano tuttavia in modo diverso a seconda degli Stati membri e la cooperazione è difficile; quelli già operativi non sempre dispongono dei mezzi tecnici adeguati e i loro compiti non sono definiti con precisione. Il coordinamento a livello internazionale avviene tramite il CERT/CC, un organismo parzialmente finanziato dal governo statunitense. I CERT europei sono tributari della politica di divulgazione delle informazioni del CERT/CC e di altri organismi.

A causa di tale complessità la cooperazione su scala europea è stata a tutt'oggi limitata. Una tale cooperazione è nondimeno essenziale per garantire una segnalazione precoce in tutta l'Unione mediante l'immediato scambio di informazioni ai primi segnali di attacco in un paese. È urgente, di conseguenza, che l'Unione europea rafforzi la cooperazione nel quadro del sistema CERT. Nell'ambito del piano d'azione «Europe» è stato deciso un primo intervento inteso a rafforzare la cooperazione pubblico/privato in materia di affidabilità dell'infrastruttura dell'informazione (tra cui lo sviluppo di sistemi di allarme preventivo) e a migliorare la cooperazione tra i vari CERT.

Azioni proposte

- È opportuno che gli Stati membri esaminino il funzionamento dei rispettivi sistemi CERT al fine di potenziarne risorse e competenze. A sostegno delle iniziative nazionali, la Commissione europea elaborerà una proposta concreta volta a rafforzare la cooperazione a livello europeo. La proposta comprenderà un progetto nell'ambito del programma TEN Telecom destinato a garantire un'efficace collegamento in rete e a definire opportune misure di accompagnamento nell'ambito del programma TSI per agevolare lo scambio di informazioni.
- Una volta istituita a livello di Unione europea, la rete CERT dovrà essere collegata ad organismi dello stesso tipo attivi in tutto il mondo, come ad esempio il sistema di segnalazione degli incidenti proposto dal G8.
- La Commissione propone di esaminare d'intesa con gli Stati membri il miglior modo di organizzare a livello europeo una raccolta di dati, un'analisi ed una programmazione di

risposte lungimiranti alle minacce attuali e future alla sicurezza. La struttura organizzativa di un eventuale organismo di questo tipo dovrà essere discussa dagli Stati membri.

3.4. Sostegno tecnologico

Al momento, il livello degli investimenti nella sicurezza della rete e dell'informazione non è ottimale, né dal punto di vista dell'adozione delle nuove tecnologie né della ricerca di nuove soluzioni. In un contesto in cui le nuove tecnologie emergenti comportano inevitabilmente nuovi rischi, è indispensabile che le attività di ricerca siano permanenti.

La sicurezza delle reti e dell'informazione è già parte del programma "Tecnologie della società dell'informazione" (TSI) del Quinto programma quadro per la ricerca dell'UE. Il bilancio è di 3,6 miliardi di euro per quattro anni e, nel biennio 2001-2002, 30 milioni circa di euro saranno destinati alle iniziative congiunte di ricerca nel settore delle tecnologie di sicurezza.

La ricerca tecnica nel campo della crittografia in Europa si trova in uno stadio avanzato. L'algoritmo belga 'Rijndael' ha vinto il concorso *Advanced Encryption Standard* indetto dall'organismo di normalizzazione statunitense (NIST). Il progetto TSI del NESSIE (*New European Schemes for Signature, Integrity and Encryption*) ha lanciato un grande concorso dedicato agli algoritmi di cifratura che risponde ai criteri dei nuovi applicativi multimediali, del commercio mobile e delle *smart card*.

Azioni proposte

- La Commissione propone di fare della sicurezza delle reti uno dei temi del Sesto programma quadro, attualmente discusso in sede di Consiglio e Parlamento europeo. Ai fini di un'ottimizzazione delle spese, occorre che tali attività si inseriscano in una strategia più ampia di miglioramento della sicurezza delle reti e dell'informazione. La ricerca finanziata nell'ambito del programma affronterà i problemi centrali posti dalle reti "tutto digitale" e dalla necessità di tutelare i diritti delle persone e delle collettività, incentrandosi sui meccanismi di sicurezza fondamentali e sulla loro interoperabilità, sui processi di protezione evolutivi, sulla crittografia avanzata, sullo sviluppo delle tecnologie di tutela della privacy, sulle tecnologie di gestione dei *digital assets* e sulle tecnologie di certificazione a sostegno delle funzioni economiche ed organizzative di sistemi dinamici e mobili.
- Gli Stati membri devono promuovere attivamente l'uso di potenti moduli di cifratura "integrabili"¹⁵. Le soluzioni di sicurezza basate sui moduli di cifratura integrabili devono fungere da alternativa alle soluzioni che prevedono una cifratura come parte integrante del sistema operativo.

3.5. Sostegno alle attività di normalizzazione e certificazione in una logica di mercato

Per risultare efficaci, le soluzioni volte ad aumentare il livello della sicurezza devono essere applicate di comune accordo dai soggetti che operano sul mercato e basarsi preferibilmente su norme internazionali aperte. Uno dei principali ostacoli all'adozione di molte soluzioni in materia di sicurezza, ad esempio le firme elettroniche, è la scarsa interoperabilità tra le varie tecnologie esistenti. Se due utenti desiderano comunicare in modo sicuro tra ambienti diversi è necessaria un'interoperabilità tra i loro apparati. Andrebbe pertanto incoraggiato l'uso di protocolli ed interfacce normalizzati, compresi i test di conformità e gli eventi di "interoperabilità". Da questo punto di vista norme aperte basate su software *open source* consentirebbero di correggere più rapidamente le anomalie e garantirebbero maggiore trasparenza.

Inoltre, una valutazione della sicurezza dell'informazione contribuirebbe ad accrescere la fiducia degli utenti. L'uso di criteri comuni ha facilitato il riconoscimento reciproco quale metodo di

¹⁵ "Integrabile" (*pluggable*) sta ad indicare che il software di cifratura può essere facilmente montato e fatto funzionare "sopra" il sistema operativo.

valutazione in molti paesi¹⁶. Alcuni di essi hanno concluso accordi con gli Stati Uniti e il Canada per il riconoscimento reciproco dei certificati di sicurezza relativi alle tecnologie dell'informazione.

La certificazione dei processi economici e dei sistemi di gestione della sicurezza delle informazioni è sostenuta dalla cooperazione europea per l'accreditamento (EA)¹⁷. L'accreditamento degli organismi di certificazione accresce la fiducia nelle loro competenze e nella loro imparzialità e facilita pertanto l'accettazione dei loro certificati nel mercato interno.

Oltre alla certificazione sono necessari anche test di interoperabilità. Valga come esempio di questo approccio l'iniziativa *European Electronic Signatures Standardisation Initiative* (EESSI) sulle firme elettroniche. Altri validi esempi sono l'iniziativa sulle *smart card* nel quadro di *eEurope* e l'iniziativa per l'attuazione dell'infrastruttura di chiave pubblica (PKI) avviata nell'ambito del programma IDA sullo scambio di dati tra le amministrazioni.

Non si assiste ad una scarsa volontà di standardizzazione, ma piuttosto alla presenza di un gran numero di standard e specifiche concorrenti che causano una frammentazione del mercato ed impediscono di definire soluzioni interoperabili. Le attività attualmente portate avanti in materia di normalizzazione e certificazione devono quindi essere meglio coordinate anche per tenere il passo con le nuove soluzioni di sicurezza proposte. L'armonizzazione delle specifiche condurrà ad una maggiore interoperabilità e, di conseguenza, ad una più rapida attuazione delle soluzioni da parte dei soggetti che operano sul mercato.

Azioni proposte

- Gli organismi di normalizzazione europei sono invitati ad accelerare i lavori sui prodotti e i servizi interoperabili e sicuri stabilendo un calendario ambizioso ed immutabile. Ove necessario dovranno adottare nuove forme di prodotti e di procedure al fine di accelerare le attività, intensificare la collaborazione con i rappresentanti dei consumatori e suscitare l'impegno dei soggetti operanti nel mercato.
- La Commissione continuerà a finanziare, in particolare mediante i programmi TSI e IDA, l'uso delle firme elettroniche, l'attuazione di soluzioni di infrastrutture a chiave pubblica (PKI) di facile uso per l'utente e la diffusione dei protocolli IPv6 e IPSec¹⁸ (come previsto dal piano d'azione *eEurope* 2002).
- Gli Stati membri sono invitati a promuovere l'uso delle procedure di certificazione e di accreditamento per le norme europee ed internazionali comunemente accettate in modo da facilitare il reciproco riconoscimento dei certificati. La Commissione valuterà, entro la fine del 2001, la necessità di un'iniziativa legislativa in materia di reciproco riconoscimento dei certificati.
- Gli operatori presenti sul mercato europeo sono incoraggiati a partecipare più attivamente alle attività degli organismi di normalizzazione europei (CEN, Cenelc, ETSI) ed internazionali (*Internet Engineering Task Force* (IETF), *World Wide Web Consortium* (W3C)).

¹⁶ Raccomandazione 95/144/CE del Consiglio sui criteri comuni per la valutazione della sicurezza delle tecnologie dell'informazione (attuati nella maggior parte degli Stati membri dell'UE).

¹⁷ La cooperazione europea per l'accreditamento riunisce gli organismi di accreditamento di 25 paesi appartenenti all'UE, all'EFTA e ai paesi candidati all'adesione.

¹⁸ L'IPv6 è un protocollo Internet che aumenta il numero di indirizzi IP possibili, ottimizza il *routing* dei messaggi ed accresce le possibilità di uso del protocollo IPSec. Quest'ultimo è un altro protocollo Internet destinato a garantire la riservatezza, ad evitare che i pacchetti siano "visti" se non dall'*host* destinatario e a provvedere all'autenticazione e all'integrità del messaggio per garantire che i dati nel pacchetto siano autentici e provengano dal corretto mittente.

- Gli Stati membri devono riesaminare tutte le pertinenti norme di sicurezza. Di concerto con la Commissione potrebbero essere organizzati concorsi per la realizzazione di soluzioni di cifratura e di sicurezza di livello europeo allo scopo di formulare la realizzazione di norme internazionali.

3.6. Quadro normativo

Tra i vari provvedimenti legislativi che interessano la sicurezza delle reti di comunicazione e dei sistemi d'informazione, il quadro normativo per le telecomunicazioni è il più completo. La convergenza delle reti fa sì che la problematica della sicurezza provochi un ravvicinamento delle normative e degli interventi regolatori tradizionalmente impiegati nei diversi settori. Si tratta delle **telecomunicazioni** (che comprendono tutte le reti di comunicazione), un settore regolamentato e deregolamentato allo stesso tempo, dell'**industria informatica**¹⁹, un settore in gran parte ancora non regolamentato, di **Internet**, che ha funzionato senza veri e propri interventi del settore pubblico, e del **commercio elettronico** sempre più oggetto di una regolamentazione specifica. Quando si parla di sicurezza, inoltre, non si può prescindere da considerazioni sulla responsabilità civile, la criminalità informatica, le firme elettroniche, la protezione dei dati e la regolamentazione delle esportazioni. Particolarmente importanti, al riguardo, sono le direttive sulla protezione dei dati, il quadro normativo sulle telecomunicazioni e diverse altre iniziative legislative citate nella comunicazione sulla criminalità informatica.

La tutela della vita privata è un obiettivo essenziale dell'Unione europea. Si tratta di un diritto fondamentale ai sensi dell'articolo 8 della Convenzione europea sui diritti dell'uomo²⁰. Anche gli articoli 7 e 8 della Carta dei diritti fondamentali dell'Unione europea²¹ prevedono che ogni individuo ha diritto al rispetto della propria vita privata e familiare, del proprio domicilio, delle sue comunicazioni e dei dati di carattere personale che lo riguardano.

Le direttive sulla protezione dei dati²² e in particolare l'articolo 5 della direttiva sulla protezione dei dati nel settore delle telecomunicazioni²³ obbligano gli Stati membri a garantire la riservatezza sulle reti di telecomunicazioni pubbliche e sui servizi di telecomunicazioni accessibili al pubblico. Inoltre, al fine di dare attuazione pratica al disposto dell'articolo 5, l'articolo 4 della medesima direttiva stabilisce che i fornitori di servizi e di reti offerti al pubblico sono tenuti ad adottare le necessarie misure tecniche ed organizzative per tutelare le sicurezze dei loro servizi. Sempre a norma di tale articolo, le suddette misure devono, tenuto conto delle attuali conoscenze in materia e dei costi di attuazione, garantire un livello di sicurezza adeguato al rischio incorso. Ciò significa che tutti gli operatori di rete sono soggetti all'obbligo di proteggere le comunicazioni da intercettazioni illegali. La natura paneuropea dei servizi e la più intensa concorrenza transfrontaliera renderanno necessaria una maggiore armonizzazione di tali disposizioni.

L'articolo 17 della direttiva generale sulla protezione dei dati (95/46/CE) obbliga i responsabili dei trattamenti ad adottare misure per garantire un livello di sicurezza appropriato rispetto ai

¹⁹ Le prescrizioni di sicurezza riguardano i componenti elettrici di un computer ma non i dati da esso trattati.

²⁰ http://europa.eu.int/comm/internal_market/en/media/dataprot/inter/con10881.htm#HD_NM_15

²¹ GU C 364 del 18.12.2000, www.ue.eu.int/df/docs/en/CarTEEN.pdf.

²² Direttive 95/46/CE (GU L 281 del 23.11.1995) e 97/66/CE (GU L 24 del 30.1.1998) <http://europa.eu.int/ISPO/infosoc/telecompolicy/en/9766en.pdf>

²³ “Gli Stati membri garantiscono mediante normative nazionali la riservatezza delle comunicazioni effettuate mediante la rete pubblica di telecomunicazione e i servizi di telecomunicazione offerti al pubblico. In particolare essi vietano l'ascolto, l'intercettazione, la memorizzazione o altri generi di intercettazione o di sorveglianza delle comunicazioni ad opera di persone diverse dagli utenti, senza il consenso di questi ultimi, eccetto quando sia autorizzato legalmente, a norma dell'articolo 14, paragrafo 1”.

rischi presentati dal trattamento e alla natura dei dati da proteggere, in particolare se il trattamento implica la trasmissione in rete dei dati. Il responsabile del trattamento deve attuare misure tecniche ed organizzative appropriate al fine di garantire la protezione dei dati personali dalla distruzione accidentale o illecita, dalla perdita accidentale o dall'alterazione, dalla diffusione o dall'accesso non autorizzati, segnatamente quando il trattamento comporta trasmissioni di dati all'interno di una rete, o da qualsiasi altra forma illecita di trattamento di dati personali. Tali disposizioni incidono sulle prescrizioni di sicurezza delle reti e dei sistemi di informazione utilizzati da persone fisiche ed organismi, in particolare i fornitori di servizi di commercio elettronico. La natura paneuropea dei servizi e la più intensa concorrenza transfrontaliera rendono necessario specificare quali mezzi porre in essere per conformarsi alle suddette disposizioni.

Il **quadro normativo per i servizi di telecomunicazione dell'UE** contiene una serie di disposizioni relative alla "sicurezza delle operazioni in rete" (ossia, la disponibilità di una rete in caso di emergenza) e "all'integrità della rete" (ossia, garantire il corretto funzionamento di reti interconnesse)²⁴. Nel luglio 2000 la Commissione presentò una proposta per un nuovo quadro normativo per le comunicazioni elettroniche, che attualmente è soggetta alla procedura di codecisione ed è pertanto discussa in sede di Parlamento europeo e di Consiglio. La proposta della Commissione riafferma nella sostanza, seppur con alcune modifiche, le disposizioni precedenti relative alla sicurezza e all'integrità della rete.

L'attuale quadro normativo, pertanto, oltre a disciplinare le specifiche tematiche contemplate dai singoli atti legislativi, interessa anche taluni aspetti delle reti e dei sistemi di informazione trattati nella presente comunicazione.

La **comunicazione sulla criminalità informatica** ha innescato, nell'ambito dell'Unione, una discussione sul modo di reagire ad azioni criminali che fanno uso dei computer e delle reti elettroniche. La riflessione verrà portata avanti da tutte le parti interessate nell'ambito del Forum UE di imminente costituzione, come annunciato nella summenzionata comunicazione della Commissione. Il diritto penale degli Stati membri dovrà contemplare la fattispecie di reato consistente nell'accesso non autorizzato a reti informatiche e nella violazione della sicurezza dei dati personali. Non esiste al momento alcun tipo di ravvicinamento del diritto penale in questo campo tra i paesi dell'Unione e tale situazione, oltre ad essere causa di potenziali problemi nel caso di indagini su questo tipo di reati, non funge da valido fattore dissuasivo nei confronti dei pirati informatici o di coloro che intendono sferrare attacchi di tipo analogo. Un ravvicinamento delle legislazioni penali in materia di intrusione nelle reti informatiche agevolerà inoltre la cooperazione giudiziaria tra gli Stati membri.

Date le legittime preoccupazioni per la criminalità informatica è necessario riflettere sulle modalità e sui mezzi per dare effettiva esecuzione alle disposizioni di legge. Le preoccupazioni di ordine legale non devono tuttavia condurre all'elaborazione di soluzioni che compromettano la sicurezza dei sistemi di comunicazione e di informazione.

Azioni proposte.

- È necessaria una visione comune delle implicazioni giuridiche della sicurezza nelle comunicazioni elettroniche. La Commissione fornirà, a tal fine, un inventario delle misure nazionali adottate conformemente al pertinente diritto comunitario.

²⁴ Direttiva della Commissione sulla liberalizzazione 90/388/CE, direttiva sull'interconnessione 97/33/CE e direttiva sulla telefonia vocale 98/10/CE.

- Occorre che gli Stati membri e la Commissione continuino a sostenere la libera circolazione dei prodotti e dei servizi crittografici mediante una maggiore armonizzazione delle procedure amministrative di esportazione ed una più ampia liberalizzazione dei controlli all'esportazione.
- La Commissione proporrà un provvedimento legislativo basato sul titolo VI del trattato sull'Unione europea finalizzato a ravvicinare le legislazioni penali nazionali in materia di attacchi ai sistemi informatici, compresi gli attacchi di pirateria e gli attacchi di tipo *denial of service*.

3.7. La sicurezza nella pubblica amministrazione

Il piano d'azione eEurope 2002 mira ad incoraggiare una più intensa ed efficace interazione tra i cittadini e la pubblica amministrazione. Poiché gran parte dei dati scambiati tra i cittadini e le rispettive amministrazioni sono di natura personale o riservata (sanitarie, finanziarie, legali, ecc.), la sicurezza è un elemento essenziale ai fini del successo di questa iniziativa. Inoltre, grazie allo sviluppo dell'*e-government* (amministrazioni on line) le amministrazioni pubbliche fungono da **testimoni potenziali dell'efficacia delle soluzioni di sicurezza** e, al tempo stesso, da soggetti del mercato **in grado di influenzare gli sviluppi del settore mediante le loro decisioni di acquisto**.

Per le pubbliche amministrazioni si tratta non soltanto di acquistare tecnologie dell'informazione e della comunicazione che soddisfino i requisiti di sicurezza, ma anche di sviluppare al loro interno una cultura della sicurezza. Ciò può avvenire elaborando "politiche di sicurezza organizzativa" che rispondano alle esigenze dell'istituzione.

Azioni proposte.

- Gli Stati membri devono accogliere soluzioni efficaci ed interoperabili di sicurezza delle informazioni fra i requisiti fondamentali per l'amministrazione on line e programma gli appalti pubblici on line (*e-procurement*).
- Gli Stati membri devono introdurre la firma elettronica nei servizi pubblici offerti on line.
- Nel quadro dell'iniziativa *e-Commission*, la Commissione adotterà una serie di misure destinate a rafforzare le prescrizioni di sicurezza dei propri sistemi di informazione e di comunicazione.

3.8. Cooperazione internazionale

Le comunicazioni veicolate sulle reti attraversano le frontiere in una frazione di secondo, e alla stessa velocità viaggiano anche i problemi di sicurezza che ne derivano. La sicurezza di una rete è rappresentata dal suo anello più debole e l'Europa non può isolarsi dal resto della rete globale. La soluzione dei problemi legati alla sicurezza postula quindi necessariamente una cooperazione internazionale.

La Commissione europea partecipa già ai lavori di organismi internazionali quali il G8, l'OCSE e le Nazioni Unite. Il settore privato tratta del problema della sicurezza nel quadro di organismi quali il *Global Business Dialogue* (www.GBDe.org) o il *Global Internet Project* (www.GIP.org). Per la sicurezza a livello mondiale è indispensabile che questi organismi mantengano contatti permanenti.

Azioni proposte.

- La Commissione intensificherà con gli organismi e i partner internazionali il dialogo sulla sicurezza delle reti e in particolare sulla crescente dipendenza dalle reti elettroniche.

4. PROSSIME FASI

La presente comunicazione illustra le grandi linee strategiche per un'azione in questo settore. Si tratta ancora di un primo passo e che non va considerato un piano d'azione definitivo per la sicurezza delle reti in Europa. Vi figurano già alcune proposte di azione destinate a definire un quadro di riferimento per un approccio comune europeo. La fase successiva consisterà nella discussione a livello di Stati membri e di Parlamento europeo del quadro di riferimento e delle azioni proposte. Il Consiglio europeo di Göteborg del 15 e 16 giugno potrà fornire utili orientamenti sulle prossime fasi.

La Commissione intende aprire una discussione approfondita con l'industria, gli utenti e le autorità preposte alla protezione dei dati in merito alle modalità pratiche di attuazione delle azioni proposte. Le osservazioni possono essere inviate per posta elettronica all'indirizzo eeurope@cec.eu.int entro la fine del mese di agosto 2001. La presente comunicazione si configura quindi come un invito, rivolto alle parti interessate, ad esprimere i loro commenti al fine di definire un complesso organico di azioni concrete, eventualmente sotto forma di calendario, da realizzare entro la fine del 2001.
