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

AICA Associazione Italiana per l'Informatica ed il Calcolo Automatico

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

Riferimento Syllabus 2.0 (curriculum ufficiale AICA)
5.8.1 Concetti fondamentali

5.8.1.1: Conoscere il significato di: riservatezza (privacy), anonimato, diritto allo pseudonimo

▶ Sicurezza di rete – Aspetti sociali e legali

Codici e normative di sicurezza

Si conclude il corso per il conseguimento della certificazione EUCIP IT Administrator Sicurezza Informatica e in questa lezione parliamo di privacy e degli aspetti etici e sociali legati alla sicurezza informatica.
I contenuti sono composti da tre elementi: un articolo sulla rivista, un articolo molto più esteso in formato PDF, e un corso multimediale completo su DVD

di Giorgio Gobbi

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

La facilità di accesso e manipolazione delle informazioni resa possibile dagli sviluppi tecnologici e da Internet ha portato a legislazioni che riconoscono il diritto alla riservatezza, che si concretizza come la possibilità di controllare l'utilizzo delle proprie informazioni personali da parte di terzi.

Una prima esigenza è di evitare la divulgazione incontrollata d'informazioni che possono essere usate per recare danno all'individuo. Un'altra esigenza, non meno importante, è d'impedire l'incrocio tra banche dati diverse allo scopo di costruire un profilo soggettivo e dettagliato dell'individuo, utilizzabile a suo danno. Le normative vigenti, emanate in base alla direttiva CE n. 95/46, hanno lo scopo di regolamentare il trattamento dei dati personali. Misure come l'informativa all'interessato con la richiesta di consenso e l'adozione di misure di sicurezza per impedire la divulgazione dei dati servono a limitare l'uso delle informazioni personali ai casi previsti dalla legge e concordati col cittadino.

D'altra parte, l'utilizzo sempre più capillare delle tecnologie informatiche (basti pensare alle transazioni finanziarie e ai rapporti con la pubblica amministrazione) impedisce che le comunicazioni possano svolgersi nel completo anonimato, visti gli illeciti civili e penali che verrebbero commessi senza poter rintracciare i responsabili. Reati come truffe, terrorismo e pedofilia destano già allarme sociale e sono nel raggio d'attenzione di legislatori e forze dell'ordine; ben più diffusa tra la massa degli utenti Internet è la violazione del diritto d'autore, favorita da software di duplicazione e di scambio peer-to-peer e dalla pubblicazione illecita su Internet di materiale soggetto a copyright.

L'esigenza è quindi, da un lato, di assicurare l'anonimato degli interessati e la riservatezza delle informazioni scambiate nel rispetto dei diritti altrui e dei valori di una società democratica che si riconosce nella Convenzione Europea dei diritti dell'uomo del 1950 (basata sulla Dichiarazione Universale dei Diritti dell'Uomo del 1948), che nell'articolo 8 specifica il Diritto al rispetto della vita privata e familiare. D'altro canto, l'anonimato cessa di essere garantito quando si tratta d'individuare e perseguire i responsabili di azioni criminali.

A tale proposito, la "Raccomandazione n. R (99) 5 del Comitato dei Ministri agli stati membri relativa alla protezione della privacy su Internet e linee guida per la protezione delle persone rispetto alla raccolta e al trattamento di dati personali sulle autostrade dell'informazione", adottata dal Comitato dei Ministri del Consiglio d'Europa il 23/2/1999, ha fissato una serie di principi per equilibrare la privacy con l'impossibiltà di completo anonimato, che includono il diritto all'uso di pseudonimi. La raccomandazione suggerisce che sia prevista la possibilità d'uso di pseudonimi in modo che la reale identità personale degli utenti Internet sia nota solo ai service provider. In tal modo, l'utente può evitare di essere riconosciuto dagli altri utenti, ma resta legalmente re-

I contenuti delle 8 lezioni

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

Lezione 1: *Informazioni generali*
Lezione 2: **parte 1** *Crittografia - fondamenti e algoritmi*
Lezione 2: **parte 2** *Crittografia - applicazioni*
Lezione 3: *Autenticazione e controllo degli accessi*
Lezione 4: *Disponibilità dei dati*
Lezione 5: *Codice maligno*
Lezione 6: *Infrastruttura a chiave pubblica*
Lezione 7: **parte A** *Sicurezza di rete Ethernet e TCP/IP*
parte B *Sicurezza in mobilità e on line*
parte C *Impedire accessi non autorizzati*
parte D *Posta elettronica e firewall*
parte E *Difendersi dai nemici all'interno*
Lezione 8: *Aspetti sociali e legali della sicurezza IT*

sponsabile dei suoi comportamenti sulla rete, perché rintracciabile su richiesta dell'autorità giudiziaria.

Autenticazione e privacy

Abbiamo visto che la totale anonimità è irraggiungibile, dato che i provider e i gestori dei servizi di posta tengono traccia degli accessi da parte degli utenti, che devono essere registrati per utilizzare il servizio. Un certo livello di anonimità può essere raggiunto illegalmente, impossessandosi delle credenziali di accesso di un altro utente e usandole senza autorizzazione, ma si tratta di una soluzione limitata, rischiosa e di efficacia temporanea. Legalmente, un utente può utilizzare software e servizi (alcuni a pagamento, altri gratuiti) che garantiscono l'anonimità del browsing Internet e dei messaggi di posta inviati attraverso web mail. Tuttavia, anche in questi casi viene tenuta traccia dell'utilizzo del servizio, che può essere interrotto in qualsiasi momento in caso di abuso, inoltre le registrazioni sono a disposizione delle autorità competenti.

Se da un lato un utente è interessato a difendere la privacy e la riservatezza mentre naviga su Internet, in altre occasioni è di fondamentale importanza poter autenticare un soggetto per identificare con certezza l'autore di un certo comportamento o l'utente che accede a determinate risorse. Nel caso di azioni illecite o criminali, un'indagine può utilizzare tecniche di monitoraggio e i log dei provider Internet. Nel caso di accessi e transazioni legittime, l'autenticazione serve ad accertare l'identità di chi le esegue, impedendo l'accesso ai soggetti non autorizzati e, se abbastanza forte, vincolando l'utente a far fronte all'impegno contratto senza possibilità di ripudio (al di là di quelle stabilite per legge, come il diritto di recesso per gli acquisti online). L'autenticazione rappresenta una prova di identità, che identifica univocamente un individuo sulla base di uno o più dei seguenti fattori: un dato conosciuto (come una password o la risposta a una domanda), un oggetto posseduto (come un token USB o una Smart Card) o una caratteristica fisica (come un'impronta digitale o la mappa dell'iride).

Riservatezza e autenticazione sembrano due obiettivi antagonisti, ma ciò è vero solo in termini relativi e in determinate circostanze. Ad esempio, la richiesta di autenticazione per eseguire una transazione commerciale protegge i contraenti e normalmente comporta una perdita accettabile della riservatezza, se ogni parte in causa applica le leggi sul trattamento delle informazioni personali o sensibili.

Nel panorama italiano di leggi e decreti, un esempio che tratta sia di autenticazione sia di privacy è il decreto legislativo 196/2003 (Nuovo codice in materia di protezione dei dati personali). Gli articoli da 31 a 34 prescrivono sia la riservatezza a protezione dei dati personali sia le misure autenticazione e autorizzazione come condizione per accedere alle informazioni. L'allegato B precisa le "misure minime di sicurezza" che devono essere adottate dai soggetti che trattano dati personali per non incorrere in responsabilità penali. In particolare, sulla base delle indicazioni comunitarie, il legislatore italiano ha stabilito la necessità di proteggere i computer utilizzati nel trattamento di dati personali attraverso un sistema di credenziali di autenticazione basato su codice di identificazione e password o altro dispositivo di autenticazione, come token, Smart Card o caratteristica biometria eventualmente associata a un codice o password. Tra le norme specificate, c'è la lunghezza minima di otto caratteri per le password, il suo contenuto non associabile all'utente, la sua modifica al primo utilizzo e almeno ogni sei mesi (pena la perdita delle credenziali) e regole di utilizzo delle credenziali.

La scelta di imporre forme di autenticazione per accedere alle risorse si riflette nella protezione dei tre attributi fondamentali della sicurezza:

1. riservatezza delle informazioni, riducendo il rischio di accesso alle informazioni (visione o furto) da parte di soggetti non autorizzati;
2. integrità dei dati, riducendo il rischio di modifiche, aggiunte e cancellazioni per interventi non autorizzati:
3. disponibilità dei dati, riducendo il rischio che agli utenti legittimi sia impedito di accedere alle risorse nei tempi e modi appropriati.

Ci sono circostanze in cui l'autenticazione può avere risvolti delicati: procurarsi la possibilità di sapere quando un soggetto ha avuto accesso a una risorsa e quali operazioni ha eseguito può costituire una violazione della legge sulla privacy, se l'interessato non è stato adeguatamente informato; inoltre, in Italia, azioni di monitoraggio che possano configurarsi come controllo a distanza (lecite in altri paesi) sono vietate dallo statuto dei lavoratori.

In un'azienda, la registrazione delle attività degli utenti durante la giornata comporta la registrazione nei file di log di un ingente quantità di informazioni, soprattutto se gli accessi sono soggetti ad autenticazione. L'analisi di tali informazioni, se condotta con l'intenzione di scoprire come un lavoratore impiega il tempo e le risorse, rischia di contravvenire alla legge sulla privacy e allo statuto dei lavoratori.

L'autenticazione, d'altra parte, ha una funzione essenziale nelle organizzazioni e trova applicazioni che per loro natura hanno l'esigenza di verificare con certezza l'identità di chi esegue le operazioni. Il settore bancario, ad esempio, prevede forme di autenticazione particolarmente sofisticate per garantire che solo un certo soggetto sia autorizzato a eseguire una certa transazione. A tale scopo la legislazione comunitaria, seguita poi da quella nazionale, ha introdotto vari tipi di firma elettronica, solo alcuni dei quali hanno efficacia giuridica. Le quattro tipologie di firma previste sono:

1. Firma elettronica semplice: è l'insieme dei dati in forma elettronica allegati o connessi tramite associazione logica ad altri dati elettronici, utilizzati come metodo di autenticazione informatica. E' paragonabile a una firma cartacea non riconosciuta, quindi non ha valore legale.
2. Firma elettronica avanzata: è ottenuta attraverso una procedura informatica che garantisce la connessione univoca al firmatario e la sua univoca identificazione, creata con mezzi su cui il firmatario mantiene un controllo esclusivo e collegata ai dati cui si riferisce in modo da rilevare se essi sono stati successivamente modificati.
3. Firma elettronica qualificata: una firma elettronica avanzata, in sé tecnologicamente neutra, assume valore legale (pari a una firma autografa) solo quando è utilizzata insieme a un "certificato qualificato" ed è creata attraverso un "sistema di creazione di firma sicura". Per produrre una firma di tale livello bisogna soddisfare una trentina di requisiti.
4. Firma digitale: è una specie particolare di firma elettronica qualificata, basata sulla crittografia a chiave asimmetrica (detta anche crittografia a chiave pubblica). Il decreto legislativo 82/2005 è impostato come se si potessero avere più tipi di firma elettronica qualificata, cioè più sistemi che consentono l'identificazione univoca del titolare, uno dei quali è la firma digitale a chiavi asimmetriche. Di fatto, però, la firma digitale è l'unico tipo di firma elettronica avanzata oggi noto e utilizzato, per cui i due concetti tendono a coincidere.

L'articolo 21 del DL 82/2005 stabilisce, con un rimando al Codice Civile, che la firma digitale (o altra firma elettronica qualificata) è probatoria salvo querela per falso, equiparando il documento informatico sottoscritto con firma digitale alla scrittura privata con firma autografa. La titola-

5.8.2 Tecnologie a tutela della privacy

5.8.2.1: Conoscere l'equilibrio fra esigenze di autenticazione e diritto alla privacy

rità della firma digitale è garantita dagli enti certificatori accreditati presso il CNIPA (Centro Nazionale per l'Informatica nelle Pubbliche Amministrazioni, ex AIPA), che tengono registri delle chiavi pubbliche presso i quali si può verificare la titolarità del firmatario di un documento elettronico (verificando la validità del certificato digitale del titolare e dei certificati delle Certification Authority interessate). I certificatori hanno requisiti di capitale sociale non inferiore a quello richiesto per svolgere attività bancaria, quindi non sono individui (come i notai), bensì grandi enti o società. Una chiave privata viene fornita a pagamento e ha una scadenza, il che potrebbe essere opinabile, visto che la firma (autografa o digitale) è un mezzo legale per l'esercizio dei diritti naturali della persona.

5.8.2.2: Conoscere le tecnologie per l'incremento della privacy (PET)

Tecnologie a tutela della privacy

Nel corso degli anni, le aziende si sono trovate costrette, anche a termini di legge, ad adottare sistemi di sicurezza basati su tecnologie sempre più sofisticate, rese necessarie dall'evoluzione e diffusione dei mezzi di attacco e dal crescente danno causato da tali attacchi a organizzazioni sempre più dipendenti dai sistemi e dalle reti informatiche per il proprio funzionamento.

Il trattamento di dati personali è regolamentato da numerose leggi, tra cui la Direttiva 95/46/CE del Parlamento Europeo e del Consiglio dell'Unione Europea (relativa alla tutela delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati) e DL 196/2003 (codice in materia di protezione dei dati personali).

La direttiva europea stabilisce che:

1. Gli Stati membri garantiscono, conformemente alle disposizioni della direttiva, la tutela dei diritti e delle libertà fondamentali delle persone fisiche e particolarmente del diritto alla vita privata, con riguardo al trattamento dei dati personali.
2. Gli Stati membri non possono restringere o vietare la libera circolazione dei dati personali tra Stati membri, per motivi connessi alla tutela garantita a norma del paragrafo 1.

Il codice italiano della privacy, molto più dettagliato, rimarca il diritto di chiunque alla protezione dei dati personali che lo riguardano e disciplina le modalità di trattamento dei dati, specificando anche i requisiti di sicurezza dei dati e dei sistemi informatici. Include anche una sezione sulle sanzioni, che per i casi più gravi possono arrivare a 90.000 euro di sanzione amministrativa, reclusione fino a tre anni (nei casi di responsabilità penale) e pagamento dei danni.

Entrambe le leggi stabiliscono che la custodia e il trattamento dei dati personali sono legati ai progressi tecnici, alla natura dei dati e alle caratteristiche del trattamento, in modo che adeguate misure preventive di sicurezza riducano al minimo i rischi in termini di riservatezza, integrità e disponibilità.

Gli articoli di legge includono due concetti che meritano attenzione nell'ambito della sicurezza informatica: l'idoneità e l'evoluzione delle misure di sicurezza.

L'idoneità è un criterio che non descrive una particolare soluzione se non attraverso i risultati ottenuti. In caso di contestazione, chi è responsabile delle scelte e dell'attuazione delle politiche di sicurezza dovrà dimostrare di avere adottato le misure necessarie per evitare la perdita di sicurezza che si è verificata e che quest'ultima è attribuibile a eventi fortuiti o di causa maggiore.

L'evoluzione delle misure di sicurezza è inevitabile per stare al passo (idealmente per anticipare) delle modalità e degli strumenti di attacco. L'aggiornamento delle politiche di sicurezza e delle contromisure tecnologiche è indispensabile per mantenere nel tempo l'idoneità delle soluzioni messe in campo ed evitare quindi azioni di responsabilità civile intraprese dai soggetti che si dichiarano danneggiati.

L'esigenza di ottenere gli obiettivi di sicurezza in termini e costi ben definiti ha favorito l'outsourcing della sicurezza attraverso contratti che impegnano il fornitore a gestire le problematiche di sicurezza in nome e per conto del committente. Tali contratti garantiscono il rispetto di specifici SLA (Service Level Agreement) o di standard internazionali come il BS 7799/ISO 17799 (vedi la lezione 1) che, se adottati, producono il livello di idoneità del livello di sicurezza richiesto dai legislatori.

L'Allegato B del Codice della privacy italiano (Disciplinare tecnico in materia di misure minime di sicurezza) definisce le misure minime di sicurezza che devono essere adottate dalle organizzazioni che trattano dati personali attraverso strumenti elettronici o in altro modo. Si deve tuttavia osservare che l'osservanza delle misure minime di legge elencate nell'Allegato B (riportate nel riquadro) evita il rischio di sanzioni di tipo penale, ma solo l'adozione di misure di livello superiore - idonee al conseguimento degli obiettivi - può tenere l'azienda al riparo da azioni di responsabilità civile. L'Allegato B prescrive l'uso di credenziali di autenticazione per accedere al sistema, specifica norme per la scelta e l'amministrazione delle password, prevede sistemi di autorizzazione per limitare gli accessi alle informazioni minime necessarie e include altre misure di sicurezza (aggiornamenti software, backup periodici, sistemi anti-intrusione, programmi anti-malware). Ulteriori misure sono richieste per il trattamento e la custodia di dati sensibili o giudiziari Il tutto deve essere descritto nel documento programmatico; sia il documento sia le misure di sicurezza (tecniche e amministrative) devono essere aggiornati con cadenza annuale.

Nell'allegato B (Vedi più avanti) il legislatore, conscio che la sicurezza non è un prodotto che si acquista, ma un costante processo che coinvolge diverse figure aziendali, ha stabilito che il titolare e il responsabile del trattamento dei dati personali devono redigere, almeno una volta l'anno, un documento programmatico sulla sicurezza dei dati particolarmente dettagliato. I contenuti richiesti comprendono i dati trattati, il personale responsabile, l'analisi dei rischi, le contromisure fisiche, procedurali e tecniche da adottare, le misure di disaster recovery adottate, le azioni programmate di formazione del personale, i criteri per garantire i criteri minimi di sicurezza del trattamento dati in caso di outsourcing, i criteri da adottare per la cifratura o altra forma di protezione di dati sensibili.

È interessante notare che la legge recepisce l'importanza dell'analisi del rischio (vedi lezione 1), che include il censimento dei beni da proteggere, la valutazione delle minacce e dei danni potenziali e la definizione delle contromisure. Anche le attività di formazione e gli interventi organizzativi lasciano trasparire la necessità di coinvolgere nelle problematiche di sicurezza tutti i soggetti che condividono la responsabilità della custodia e del trattamento dei dati.

Anche in caso di outsourcing, il titolare conserva la responsabilità finale del trattamento dei dati e per contratto dovrà ricevere dal fornitore un documento che attesti la conformità con le disposizioni dell'allegato B. La mancata adozione delle misure minime di sicurezza è sanzionata penalmente dal Codice della privacy; l'articolo 169 prevede l'arresto sino a due anni o l'ammenda da 10.000 a 50.000 euro per chi è soggetto al codice e omette di adottare le misure minime prescritte.

L'insieme delle sanzioni, suddivise tra violazioni amministrative e illeciti penali, è descritto negli articoli 161-172 del codice.

Cookies e loro gestione

5.8.2.3 Conoscere i cookie e le relative modalità di gestione

I cookies (biscottini), detti anche HTTP cookies, sono pacchetti d'informazioni inviati da un web server a un browser e restituiti dal browser ogni volta che accede allo stesso server nella stessa sessione e talvolta anche in sessioni successive. I cookies sono registrati come piccoli file di testo sul computer dell'utente e sono utilizzati per autenticazione, per tenere traccia della sessione e per conservare informazioni specifiche dell'utente.

Quando fu progettato il protocollo HTTP (HyperText Transfer Protocol), responsabile del trasferimento di informazioni sul web, l'accento fu messo sulla semplicità e sulle prestazioni; di conseguenza, ogni pagina è richiesta e fornita individualmente, senza mantenere uno stato di sessione che leghi tra loro una serie di richieste e risposte. Tale comportamento era adeguato per consultare informazioni pagina per pagina e saltare liberamente da un link all'altro senza lasciare traccia delle operazioni precedenti. Quando però nacquero le prime applicazioni di e-commerce, fu evidente la necessità di tenere traccia della transazione in corso, che in generale richiedeva l'apertura di più pagine.

La soluzione escogitata da Netscape fu l'invenzione dei cookies, supportati dal loro browser dal 1994 e integrati in Internet Explorer nel 1995.

La prima applicazione dei cookies è stata la realizzazione di un carrello virtuale per i siti di e-commerce, dove gli acquirenti mettono (e tolgono) gli articoli da acquistare mentre esplorarano le pagine del sito. Il carrello degli acquisti è tuttora uno degli utilizzi principali dei cookies, ma ce n'è altri, come l'autenticazione degli utenti (login con nome utente e password, anche in connessione sicura), la personalizzazione della navigazione (riconoscendo le impostazioni dell'utente, per esempio il numero di risposte per pagina in un motore di ricerca) e il tracking della navigazione nei siti (registrando un cookie ogni volta che l'utente visita una pagina per la prima volta).

Il trasferimento delle informazioni del cookie avviene quando il web server risponde alla richiesta della pagina web da parte del client. Se il server utilizza i cookies, la risposta include, nell'intestazione HTTP, una o più richieste di creazione di cookies, attraverso il comando Set-Cookie. Il browser salva le informazioni dei cookies su hard disk in un'apposita directory. Per esempio, Windows XP conserva i cookies in \Documents and Settings\<nome utente>\Cookies. Ogni cookie è un file di testo non più lungo di 4 KB e un browser ne può conservare almeno 300 e accetta almeno 20 cookies per dominio. Un cookie è cancellato alla chiusura del browser o alla data di scadenza, se specificata.

Ogni volta che un browser si connette a un sito web, verifica se tra i propri cookies ce n'è qualcuno associato al dominio del sito e, in tal caso, li allega alla richiesta HTTP. Il web server utilizza i cookies ricevuti per riconoscere l'utente; per esempio, nel caso di una sessione di acquisto on-line o altra transazione economica (come online banking o stipula di un contratto di assicurazione auto) i cookies tengono il legame tra le pagine della sessione finché tutti i dati sono stati raccolti e la transazione viene confermata (o viene annullata durante il tragitto).

Quello che segue è un esempio di scambio di messaggi HTTP tra l'utente (tramite browser IE) e il web server di un sito di e-commerce. Il traffico è stato catturato mediante l'utility HTTPLook (www.httpsniffer.com).

Il primo messaggio (in blu) è quello inviato dal client (il browser) al server quando l'utente inserisce l'URL del sito per aprirne la home page. Dato che è la prima volta che l'utente visita il sito, non ha sul computer cookies associati al relativo dominio.

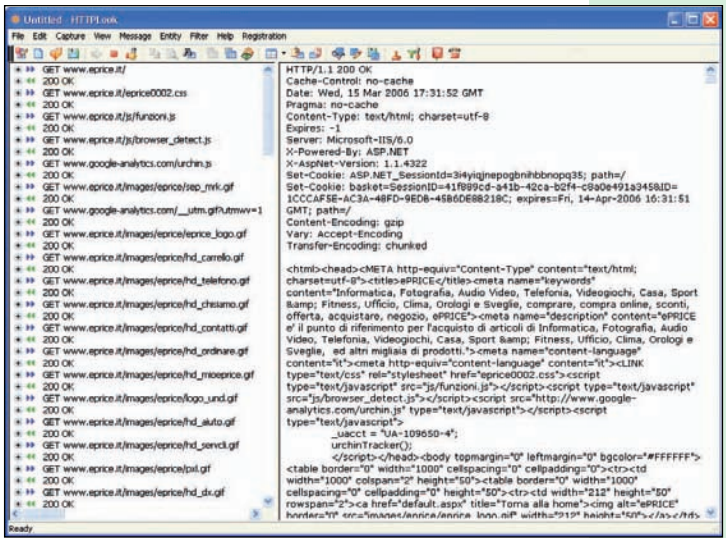
Il server risponde inviando al browser un messaggio HTTP (in rosso) contenente, tra l'altro, due richieste di creazione di cookies (Set-Cookie); l'intestazione HTTP è seguita dalla pagina HTML richiesta dal browser.

Il terzo messaggio (in blu) è la successiva richiesta dal browser al web server; il browser trova nella relativa directory i due cookies relativi al dominio del web server e li allega alla richiesta, in modo che il server riconosca la sessione in corso e prosegua nel dialogo.

L'apertura della home page di questo sito comprende un centinaio di messaggi GET (richieste) HTTP inviati dal browser e le relative risposte del web server. La maggior parte delle richieste è associata alla sessione in corso e quindi include i relativi cookies.

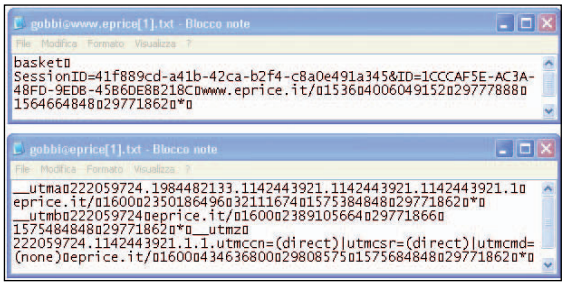
```
GET / HTTP/1.1
Accept: image/gif, image/x-xbitmap, image/jpeg,
  image/pjpeg, application/x-shockwave-flash,
  application/vnd.ms-powerpoint, application/vnd.ms-excel,
  application/msword, */*
Accept-Language: it
Accept-Encoding: gzip, deflate
User-Agent: Mozilla/4.0 (compatible; MSIE 6.0; Windows
  NT 5.1; SV1; .NET CLR 1.0.3705)
Host: www.eprice.it
Connection: Keep-Alive

HTTP/1.1 200 OK
Cache-Control: no-cache
Date: Wed, 15 Mar 2006 17:31:52 GMT
Pragma: no-cache
Content-Type: text/html; charset=utf-8
Expires: -1
Server: Microsoft-IIS/6.0
X-Powered-By: ASP.NET
X-AspNet-Version: 1.1.4322
Set-Cookie: ASP.NET_SessionId=
  3i4yiqjnepogbnihbbnopq35; path=/
Set-Cookie: basket=SessionID=41f889cd-a41b-42ca-
  b2f4-c8a0e491a345&ID=1CCCAF5E-AC3A-48FD-9EDB-
  45B6DE8B218C; expires=Fri, 14-Apr-2006 16:31:
  51 GMT; path=/
Content-Encoding: gzip
Vary: Accept-Encoding
Transfer-Encoding: chunked
<html>
.....
</html>
```



***HTTPLook** è un esempio di utility che cattura il traffico HTTP*

```
GET /eprice0002.css HTTP/1.1
Accept: */*
Referer: http://www.eprice.it/
Accept-Language: it
Accept-Encoding: gzip, deflate
User-Agent: Mozilla/4.0 (compatible; MSIE 6.0;
   Windows NT 5.1; SV1; .NET CLR 1.0.3705)
Host: www.eprice.it
Connection: Keep-Alive
Cookie: ASP.NET_SessionId=3i4yiqjnepogbnihbbnopq35;
   basket=SessionID=41f889cd-a41b-42ca-b2f4-
   c8a0e491a345&ID=1CCCAF5E-AC3A-48FD-9EDB-
   45B6DE8B218C
```



Due cookies *creati nella directory Cookies di Windows*

Impostazioni *della privacy connessa ai cookies in Internet Explorer*

Impostazione *della privacy in ZoneAlarm Security Suite*

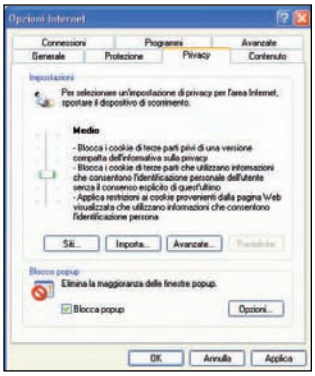
Gestione *dei cookies in Mozilla Firefox (Fedora Core Linux)*

L'introduzione dei cookies non fu di dominio pubblico finché il Financial Times non pubblicò un articolo nel febbraio 1996 attirando l'attenzione dei media per le potenziali implicazioni in tema di privacy. Da lì in poi anche i legislatori hanno più volte deliberato in proposito. Le specifiche per i cookies sono state pubblicate nelle RFC 2109 e 2965. A seguito delle notizie dei media, che hanno riportato i casi di uso illegale dei cookies per raccogliere informazioni personali, molti si sono fatti la falsa idea che i cookies siano una specie di virus o di spyware. E' importante tenere presente che i cookies sono file di testo, non programmi, quindi non possono agire sul sistema. Inoltre, nei moderni sistemi operativi dotati di account personali (resi obbligatori dal codice della privacy), un browser può accedere solo ai cookies dell'utente che li possiede. Inoltre, un web server può ricevere solo le informazioni relative ai cookies del proprio dominio (quelli che ha creato), non può attingere alle informazioni registrate nei cookies relativi ad altri domini.

Un rischio associato all'uso dei cookies deriva dal fatto che una pagina web può contenere immagini e altri componenti memorizzati su altri server in altri domini. I cookies creati durante l'accesso a tali componenti si chiamano third-party cookies (cookies di terze parti). Le aziende di marketing e pubblicità utilizzano questo genere di cookies per tenere traccia della navigazione di un utente da un sito all'altro, in modo da inviargli pubblicità mirata basata sui propri interessi e abitudini. La possibilità di costruire un profilo degli utenti è stata considerata da certi gruppi una minaccia alla privacy, specialmente se il tracking delle informazioni avviene su più domini attraverso cookies di terze parti. La Direttiva 2002/58/EC del Parlamento europeo e del Consiglio dell'Unione europea del 12 luglio 2002 sul trattamento dei dati personali e la protezione della privacy nel settore delle comunicazioni elettroniche include regole sull'uso dei cookies. In particolare, l'articolo 5, paragrafo 3 stabilisce che memorizzare dati (come i cookies) nel computer di un utente è permesso solo se: 1) l'utente è informato sull'utilizzo di tali dati e 2) l'utente ha la possibilità di rifiutare la memorizzazione. L'articolo dichiara anche i casi in cui la memorizzazione dei cookies è necessaria per motivi tecnici e sono esonerati dalla regola. Tale norma non ha avuto applicazione uniforme nell'Unione Europea.

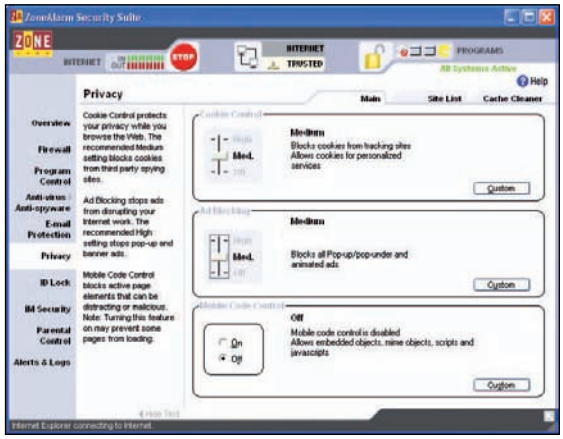
L'utente ha la possibilità di modificare le impostazioni di default del browser in modo da abbassare o innalzare il livello di privacy associato ai cookies. In Windows XP il comportamento di default è il blocco dei cookies di terze parti che possono costituire un rischio per la privacy dell'utente. In Internet Explorer > Strumenti > Opzioni Internet > Privacy, il cursore del livello di privacy è per default su Medio, ma può essere regolato in una di sei posizioni, da Accetta tutti i cookies a Blocca tutti i cookies.

La sezione Generale della finestra Opzioni Internet include un bottone per cancellare tutti i cookies dell'utente corrente in Internet Explorer.

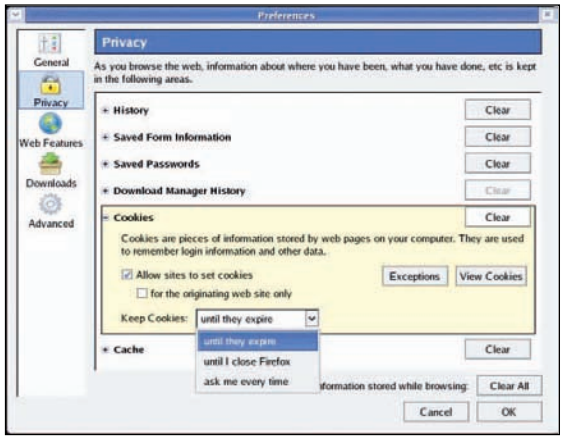


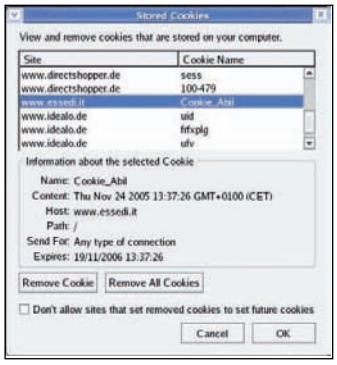
Anche le applicazioni di sicurezza individuale (come antivirus, firewall personali e anti-malware) installate sul computer possono includere un ulteriore controllo dei cookies a protezione della privacy.

L'utente che innalzi il livello di privacy è meno soggetto a cookies "invadenti" che tengono traccia dei siti visitati, ma il rovescio della medaglia è rappresentato da possibili inconvenienti nell'uso di siti di e-commerce; uno dei sintomi di eccessive restrizioni sui cookies è ad esempio l'impossibilità di depositare più articoli nel carrello degli acquisti. In altri casi, viene rifiutato l'accesso alla pagina con un messaggio che richiede l'attivazione dei cookies per poter procedere.



Anche in Linux i browser permettono di modificare le impostazioni di privacy connesse ai cookies. Ad esempio,





***Visualizzazione** dei cookies in Mozilla Firefox*

in Mozilla Firefox, aprendo Edit > Preferences > Privacy si può modificare la durata dei cookies, vedere l'elenco dei cookies memorizzati sul computer (con il contenuto in chiaro), cancellare determinati cookies (anche tutti) e rifiutare futuri cookies da particolari siti.

Aspetti etici (monitoraggio, sorveglianza)

5.8.2.4: Essere consapevoli delle implicazioni etiche (controlli nel lavoro, sorveglianza)

Gli ambienti di lavoro utilizzano in misura crescente tecnologie informatiche e di comunicazione che pongono notevoli problemi di natura etica e giuridica. Questi riguardano, da un lato, l'utilizzo corretto delle risorse da parte del personale e, per l'azienda, le attività di controllo e sorveglianza del personale.

Prima di entrare nel merito, è utile prendere atto di un comunicato stampa del Garante per la protezione dei dati personali, ampiamente riportato dalla stampa nazionale.

"Illecito spiare il contenuto della navigazione in Internet del dipendente"

Il Garante: "L'uso indebito del computer può essere contestato senza indagare sui siti visitati"

Il datore di lavoro non può monitorare la navigazione in Internet del dipendente. Il Garante privacy ha vietato a una società l'uso dei dati relativi alla navigazione in Internet di un lavoratore che, pur non essendo autorizzato, si era connesso alla rete da un computer aziendale. Il datore di lavoro, dopo aver sottoposto a esame i dati del computer, aveva accusato il dipendente di aver consultato siti a contenuto religioso, politico e pornografico, fornendone l'elenco dettagliato.

Per contestare l'indebito utilizzo di beni aziendali, afferma il Garante nel suo provvedimento (www.garanteprivacy.it/garante/doc.jsp?ID=1229854), sarebbe stato in questo caso sufficiente verificare gli avvenuti accessi a Internet e i tempi di connessione senza indagare sui contenuti dei siti. Insomma, altri tipi di controlli sarebbero stati proporzionati rispetto alla verifica del comportamento del dipendente.

"Non è ammesso spiare l'uso dei computer e la navigazione in rete da parte dei lavoratori", commenta Mauro Paissan, componente del Garante e relatore del provvedimento. "Sono in gioco la libertà e la segretezza delle comunicazioni e le garanzie previste dallo Statuto dei lavoratori. Occorre inoltre tener presente che il semplice rilevamento dei siti visitati può rivelare dati delicatissimi della persona: convinzioni religiose, opinioni politiche, appartenenza a partiti, sindacati o associazioni, stato di salute, indicazioni sulla vita sessuale".

Nel caso sottoposto al giudizio del Garante, dopo una prima istanza, senza risposta, rivolta alla società, il lavoratore aveva presentato ricorso al Garante contestando la legittimità dell'operato del datore di lavoro.

La società aveva allegato alla contestazione disciplinare notificata al lavoratore, in seguito licenziato, numerose pagine dei file temporanei e dei cookies originati sul suo computer dalla navigazione in rete, avvenuta durante sessioni di lavoro avviate con la password del dipendente. Da queste pagine, copiate direttamente dalla directory intestata al lavoratore, emergevano anche diverse informazioni particolarmente delicate che la società non poteva raccogliere senza aver prima informato il lavoratore. Sebbene infatti i dati personali siano stati raccolti nel corso di controlli informatici volti a verificare l'esistenza di un comportamento illecito, le informazioni di natura sensibile, in grado di rivelare ad esempio convinzioni religiose e opinioni sindacali o politiche, potevano essere trattate dal datore di lavoro senza consenso solo se indispensabili per far valere o difendere un diritto in sede giudiziaria. Indispensabilità che non è emersa dagli elementi acquisti nel procedimento.

Illecito anche il trattamento dei dati relativi allo stato di salute e alla vita sessuale. Secondo il Codice della privacy infatti tale tipo di trattamento può essere effettuato senza consenso solo se necessario per difendere in giudizio un diritto della personalità o un altro diritto fondamentale. La società in questo caso intendeva invece far valere diritti legati allo svolgimento del rapporto di lavoro.

Roma, 14 febbraio 2006

Un'altra indicazione viene dai sondaggi sull'uso di Internet negli ambienti di lavoro, indicato da più parti come la maggiore fonte di spreco di ore di lavoro. Qualche anno fa IDC appurò che il 30-40% delle ore di navigazione Internet nelle aziende americane non era per motivi di lavoro e che il 70% della banda aziendale era utilizzata a scopo non aziendale. Nel 2005 ha avuto vasta eco sui media (ad esempio www.sfgate.com/cgi-bin/article.cgi?f=/g/a/2005/07/11/wastingtime.TMP) un'indagine di America Online e Salary.com su 10.000 lavoratori americani, che ha rilevato che il lavoratore medio spreca ogni giorno due ore di lavoro, di cui la quota principale (44,7%) è data dalla navigazione Internet per scopi personali. Una ricerca di Benchmark Research commissionata nel 2005 da AMD (uno dei maggiori produttori di microprocessori), sull'utilizzo di Internet in Europa, ha appurato che gli utenti italiani sono al primo posto nell'uso del PC per scambiare file musicali in rete.

Questo piccolo campione di informazioni, facilmente ampliabile attingendo a Internet, indica che ci sono problematiche legate all'utilizzo dei computer e alle politiche di sicurezza aziendali. Infatti, l'uso delle risorse informatiche e di Internet non coinvolge solo aspetti organizzativi ed eventualmente disciplinari; sono soprattutto i comportamenti impropri o illeciti (uso del computer e della rete per scopi extra-lavoro) che causano le maggiori violazioni delle norme di sicurezza a cui l'azienda (a partire dai dirigenti) è vincolata (vedi codice della privacy). Quando un dipendente installa e utilizza un software di scambio file peer-to-peer (MP3 eccetera) non si limita a sprecare il proprio tempo e le risorse aziendali, ma può creare gravi falle di sicurezza nel sistema e nella rete, ad esempio per effetto di cavalli di Troia (mimetizzati da programmi utili o antispyware) di nuova generazione molto difficili da individuare ed eliminare. Inoltre le leggi sulla tutela del diritto d'autore, recentemente irrigidite, costituiscono un ulteriore rischio per l'azienda (in pratica i dirigenti) che non adotta misure per impedire il download e la diffusione di materiale (musica, film, software, eccetera) protetto da copyright.

Le problematiche derivanti dalle azioni del personale non sono puntualmente disciplinate né dal legislatore europeo né da quello italiano. Nell'ordinamento italiano, la principale norma di riferimento è l'art. 4 dello Statuto dei Lavoratori (Legge 300, 20 maggio 1970), sotto riportato.

Dalla Legge 20/5/1970, n. 300 (Statuto dei lavoratori)

ART. 4 - Impianti audiovisivi.

È vietato l'uso di impianti audiovisivi e di altre apparecchiature per finalità di controllo a distanza dell'attività dei lavoratori.

Gli impianti e le apparecchiature di controllo che siano richiesti da esigenze organizzative e produttive ovvero dalla sicurezza del lavoro, ma dai quali derivi anche la possibilità di controllo a distanza dell'attività dei lavoratori, possono essere installati soltanto previo accordo con le rappresentanze sindacali aziendali, oppure, in mancanza di queste, con la commissione interna. In difetto di accordo, su istanza del datore di lavoro, provvede l'Ispettorato del lavoro, dettando, ove occorra, le modalità per l'uso di tali impianti.

Per gli impianti e le apparecchiature esistenti, che rispondano alle caratteristiche di cui al secondo comma del presente articolo, in mancanza di accordo con le rappresentanze sindacali aziendali o con la commissione interna, l'Ispettorato del lavoro provvede entro un anno dall'entrata in vigore della presente legge, dettando all'occorrenza le prescrizioni per l'adeguamento e le modalità di uso degli impianti suddetti.

Contro i provvedimenti dell'Ispettorato del lavoro, di cui ai precedenti secondo e terzo comma, il datore di lavoro, le rappresentanze sindacali aziendali o, in mancanza di queste, la commissione interna, oppure i sindacati dei lavoratori di cui al successivo art. 19 possono ricorrere, entro 30 giorni dalla comunicazione del provvedimento, al Ministro per il lavoro e la previdenza sociale.

Al divieto per l'azienda di esercitare un controllo occulto dei lavoratori, si contrappongono tuttavia il dovere di diligenza e di fedeltà del lavoratore e il potere disciplinare del datore di lavoro. Ai sensi dell'art. 2104 del Codice Civile, "il prestatore di lavoro deve usare la diligenza richiesta dalla natura della prestazione dovuta e dall'interesse dell'impresa". Deve inoltre osservare le disposizioni per l'esecuzione e la disciplina del lavoro impartite dall'imprenditore e dai collaboratori di questo dai quali dipende gerarchicamente. Ai sensi dell'art. 2106 del CC, l'inosservanza delle disposizioni di cui all'art. 2104 può dare luogo all'applicazione di sanzioni disciplinari proporzionate alla gravità dell'infrazione.

L'articolo 7 dello Statuto dei Lavoratori (Sanzioni disciplinari) prevede che le sanzioni siano portate a conoscenza dei lavoratori e che debbano essere applicate in base a quanto stabilito dai contratti collettivi nazionali di lavoro.

A livello europeo, il Gruppo di lavoro in tema di protezione degli individui per quanto riguarda il trattamento dei dati personali presso la Commissione Europea il 29/5/2002 ha adottato un documento di lavoro (www.privacy.it/gruppridoc20020529.html) riguardante la vigilanza sulle comunicazioni elettroniche sul posto di lavoro, in particolare riguardo l'uso della posta elettronica e di Internet. Il suddetto gruppo di lavoro, costituito in applicazione della direttiva 95/46/CE del 24 ottobre 1995 del Parlamento Europeo e del Consiglio dell'Unione Europea, ha fissato una serie di principi assai rilevanti che devono essere applicati anche in Italia laddove si esercitino controlli sull'uso degli strumenti informatici e telematici che possano determinare il controllo sulle attività dei dipendenti.

Principio di necessità

Prima di attivare azioni di monitoraggio, si dovrebbe valutare se non si possano adottare altre forme di controllo meno invasive per il rispetto della dignità dei lavoratori. In ogni caso le attività di controllo devono essere eccezionali; possono essere intraprese solo se si sospetta che siano in atto attività criminose da parte del lavoratore, per esigenze legate alla sicurezza del sistema informatico aziendale o per garantire la continuità dell'attività dell'impresa.

Principio di finalità

La raccolta di dati riguardanti le azioni del lavoratore dovrebbe avvenire per uno scopo determinato, esplicito e legittimo, evitando di utilizzare tali dati in un secondo momento in modo incompatibile con le finalità dichiarate. Secondo il gruppo di lavoro, ciò significa, ad esempio, che se la raccolta e trattamento dei dati sono giustificati per ragioni riguardanti la sicurezza del sistema, quei dati non potranno in seguito essere elaborati per un altro scopo, come il controllo del comportamento del dipendente.

Principio di trasparenza

Il datore di lavoro deve dichiarare apertamente le sue attività e informare preventivamente i lavoratori riguardo i controlli messi in atto. In particolare, deve informare i lavoratori circa l'adozione di una policy aziendale per l'uso della posta elettronica e di Internet, nella quale siano descritte le modalità in cui i dipendenti possono utilizzare le infrastrutture di proprietà dell'impresa per comunicazioni personali o private. Inoltre dovranno essere descritti: i motivi e le finalità delle attività di vigilanza, i provvedimenti presi; la procedure adottate dal datore di lavoro per garantire il rispetto delle regole, indicando le modalità di contestazione delle infrazioni e della possibilità di difesa da parte dei lavoratori.

Secondo il gruppo di lavoro, il datore di lavoro dovrebbe informare immediatamente il lavoratore dell'infrazione, anche attraverso l'uso di avvisi sullo schermo del computer.

Inoltre, il gruppo di lavoro consiglia lo scambio di informazioni ed eventuali accordi con la rappresentanza sindacale prima dell'adozione definitiva delle policy all'interno dell'azienda.

Principio di legittimità

La raccolta e il trattamento dei dati riguardanti il lavoratore possono essere consentiti purché abbiano il fine di perseguire interessi legittimi da parte del datore di lavoro e non violino i diritti fondamentali dei lavoratori. Secondo il gruppo di lavoro, la necessità di tutelare l'azienda da seri pericoli, per esempio impedendo la trasmissione di informazioni confidenziali a un concorrente, può costituire tale interesse legittimo.

Principio di proporzionalità

I dati personali raccolti nell'ambito delle attività di controllo e vigilanza devono essere pertinenti e commisurati al raggiungimento dello scopo dichiarato. Ciò implica che la policy aziendale sia definita tenendo conto dell'analisi del rischio e delle contromisure pianificate.

Secondo il gruppo di lavoro, il principio di proporzionalità esclude il controllo a tappeto dell'uso della posta elettronica e di Internet da parte del personale, a meno che ciò si renda necessario per garantire la sicurezza del sistema. Il datore di lavoro dovrà inoltre valutare se non sia possibile ricorrere a modalità meno intrusive.

Il controllo della posta elettronica dovrebbe limitarsi ai dati riguardanti i flussi dei messaggi in ingresso e in uscita e al controllo degli allegati e non dovrebbe riguardare il contenuto dei messaggi. Qualora fosse indispensabile accedere ai contenuti, si dovrà tenere conto della sfera privata dei lavoratori e dei loro interlocutori. A tale proposito il gruppo di lavoro consiglia di inserire nei messaggi diretti all'esterno dell'azienda un avviso sull'esistenza dei sistemi di controllo.

Il controllo dell'uso di Internet dovrebbe consistere nell'adozione di filtri che blocchino l'accesso a determinati siti o categorie di siti web. Il servizio di web filtering può essere fornito dal firewall o può essere un servizio esterno, basato su categorie o su profili personalizzati. Anche in questo caso il gruppo di lavoro ritiene che un eventuale accordo con le rappresentanze sindacali possa portare all'a-

dozione di una policy che tenga conto in modo equilibrato degli interessi contrapposti.

Principio dell'accuratezza e conservazione dei dati

I dati personali archiviati dal datore di lavoro in relazione all'uso della posta elettronica aziendale e di Internet devono essere accurati e aggiornati e non essere conservati più a lungo del periodo necessario

Principio della sicurezza

Il datore di lavoro deve adottare le misure di sicurezza logiche e organizzative per garantire che i dati personali siano conservati in modo sicuro e protetto contro intrusioni dall'esterno. Inoltre il datore di lavoro ha il diritto di proteggere il suo sistema informatico dai virus informatici (intendendo l'intera gamma di malware) attraverso la scansione automatica dei messaggi di posta elettronica e del traffico Internet.

Si può osservare che il Codice della privacy (DL 196/2003) ha reso obbligatorie misure di sicurezza che potevano apparire facoltative, come la protezione fisica, procedurale/organizzativa e tecnica e, tra le misure tecniche, quelle idonee a impedire intrusioni (anche dall'interno), infezioni, perdite di dati e via dicendo.

Utilizzo della posta elettronica

Il gruppo di lavoro ritiene che per la posta elettronica e per quella tradizionale non ci debbano essere differenze di trattamento; di conseguenza, la posta elettronica deve fruire della stessa tutela dei diritti fondamentali di cui gode la posta cartacea. In particolare, il datore di lavoro deve evitare, per quanto possibile, intrusioni nella sfera privata del lavoratore.

Perciò il datore di lavoro deve informare in modo chiaro il lavoratore in relazione all'uso dell'indirizzo e-mail aziendale per scopi personali e sull'uso di web mail (e-mail attraverso il browser Internet anziché attraverso un programma di posta) e di indirizzi di posta privati per le loro comunicazioni personali.

Il gruppo di lavoro è a favore della soluzione web mail, che permette di separare i messaggi di lavoro da quelli privati. In tal caso, il datore di lavoro può limitarsi a controllare i flussi di corrispondenza e i tempi di utilizzo evitando ulteriori intromissioni nella sfera privata del lavoratore.

Il datore di lavoro dovrebbe informare il lavoratore della possibile necessità di accedere alla sua casella e-mail aziendale in caso di necessità (come l'assenza imprevista del dipendente), definendo le modalità di tale accesso.

Il datore di lavoro dovrà informare il lavoratore circa l'esistenza di procedure di backup dei messaggi di posta elettronica, la durata della conservazione e la loro cancellazione (da notare che l'azienda potrebbe essere tenuta a conservare i messaggi e-mail - anche interni - come parte della documentazione ufficiale dei propri affari, ad esempio per dimostrare le posizioni degli interessati, la sequenza degli eventi e la legalità del proprio operato).

Il datore di lavoro dovrà informare il lavoratore sui rischi connessi all'utilizzo della posta elettronica in relazione alla sicurezza del sistema informativo aziendale (i danni causati dal malware trasportato via e-mail possono riguardare il computer locale, la rete, i server, i sistemi operativi, le applicazioni, eccetera).

Il datore di lavoro dovrà infine evidenziare il ruolo delle rappresentanze sindacali nell'applicazione della policy aziendale.

Utilizzo di Internet

Spetta al datore di lavoro decidere se e in che misura ai lavoratori è consentito l'uso di Internet per motivi personali. D'altra parte, il gruppo di lavoro ritiene che vietare totalmente l'uso di Internet a scopo personale sia sconsigliabile, perché "poco pratico e non molto realistico poiché non tiene conto della misura in cui Internet può essere d'aiuto ai dipendenti nella loro vita quotidiana". Il gruppo di lavoro consiglia comunque l'adozione di misure atte a prevenire gli abusi dell'utilizzo di Internet, piuttosto che volte a individuare i casi di abuso.

In questa ottica è consigliata l'adozione di strumenti (come i servizi di web filtering, esterni o integrati con il firewall) in grado di bloccare l'accesso a determinati siti o categorie di siti, introducendo avvisi a fronte dei tentativi di accesso bloccati.

Anche per l'uso di Internet è necessario informare preventivamente il lavoratore dell'esistenza di controlli sul suo computer. Il gruppo di lavoro, a questo proposito, ritiene che in molti casi non sia necessario visualizzare il contenuto dei siti visitati, ma sia sufficiente verificare la durata della navigazione o l'URL dei siti visitati più di frequente da un'area dell'azienda. Qualora da tali verifiche generali dovessero emergere abusi o illeciti da parte dei lavoratori, il datore di lavoro potrà procedere a controlli più approfonditi.

In generale, è consigliabile che il datore di lavoro agisca con prudenza prima di contestare un'infrazione a un lavoratore, tenendo conto che errori di battitura, risposte dei motori di ricerca, collegamenti ipertestuali ed eventuale malware possano condurre a siti e pagine web indesiderati. In ogni caso, il datore di lavoro dovrà permettere al lavoratore di difendersi dalle contestazioni mosse nei suoi confronti, nel rispetto dello Statuto dei Lavoratori (è anche opportuno verificare che eventuali accessi impropri a Internet siano stati effettivamente eseguiti tramite l'account del lavoratore e che sul computer non siano presenti malware - come adware/spyware e simili - che lascino false tracce di navigazione; anche sotto questo aspetto la prevenzione è di gran lunga preferibile alle indagini dopo il fatto).

Il datore di lavoro dovrà informare preventivamente il lavoratore sui limiti e le condizioni entro i quali sia eventualmente consentito l'uso di Internet per scopi privati, precisando orari e tempi per l'suo privato, le categorie di siti precluse e quale materiale non può essere visionato, scaricato o copiato, spiegando in dettaglio le motivazioni di tali limitazioni.

Stante che è preferibile introdurre filtri web piuttosto che divieti di navigazione, i lavoratori dovranno essere informati sui sistemi adottati per impedire l'accesso a determinati siti/gruppi di siti e per individuare i casi i abuso. Dovranno anche essere comunicate le modalità di esecuzione dei controlli, le aree oggetto dei controlli e la possibilità di eseguire controlli individuali nel caso siano rilevate infrazioni. Anche in tal caso i lavoratori dovranno essere informati sul ruolo delle rappresentanze sindacali nell'adozione della policy aziendale.

Codici deontologici ed etici

5.8.2.5: Conoscere i principali codici di riferimento: codici deontologici, codici etici (casi studiati: ACM, BCS, IEEE, etc)

In questa sezione sono presi in considerazione i codici deontologici proposti da alcune delle maggiori associazioni professionali a livello internazionale. Se ne possono ricavare alcuni principi fondamentali che dovrebbero essere applicati anche dai professionisti di sicurezza informatica.

Il codice deontologico della Association for Computing Machinery (ACM)

L'ACM, fondata nel 1947, è una delle più antiche associazioni di professionisti informatici e condivide con l'IEEE Computer Society, pressoché coetanea, la leadership nel settore.

Il codice deontologico dell'ACM (www.acm.org/constitution/code.html) consiste di 24 principi che dovrebbero

essere rispettati nello svolgimento della propria attività professionale, suddivisi in sezioni e descritti in dettaglio (imperativi morali generali, specifiche responsabilità morali, imperativi di leadership organizzativa e conformità con il codice).

L'articolo 1.1 impegna il membro ACM a contribuire al benessere della società e dell'umanità, proteggendo i diritti umani fondamentali e rispettando la diversità delle culture.

L'articolo 1.2 (evita di danneggiare gli altri) responsabilizza gli operatori del settore di fronte a ogni tipo di danno, diretto o indiretto, che può derivare dalle proprie o altrui attività. Non solo il professionista non deve compiere azioni dannose (direttamente o come conseguenza di azioni lecite), ma ha l'obbligo di segnalare rischi e indizi di pericolo osservati nel proprio ambiente di competenza (per esempio le violazioni alle politiche di sicurezza aziendali).

L'articolo 1.3 (sii onesto e degno di fiducia) impegna il professionista non solo a operare con diligenza e buona fede ma anche a dichiarare apertamente le proprie competenze e i propri limiti.

L'articolo 1.4 impegna i membri a essere corretti e a evitare attivamente qualsiasi discriminazione.

Gli articoli 1.5 e 1.6 vincolano il professionista a onorare i diritti di proprietà, compresi copyright e brevetti, e a non assumere il merito per le opere altrui, anche quando non soggette a protezione legale.

L'articolo 1.7 (rispetta la privacy altrui) impegna il professionista a utilizzare gli strumenti di raccolta e analisi delle informazioni (che possono includere le idee e il comportamento altrui) usando ogni precauzione perché tali informazioni non possano essere utilizzate per fini estranei alla protezione di reti e sistemi.

L'articolo 1.8 (onora la riservatezza) vincola il professionista al dovere di riservatezza delle informazioni sia in conformità agli impegni presi esplicitamente sia evitando di divulgare informazioni private raccolte accidentalmente ed estranee ai doveri professionali.

L'articolo 2.1 è un impegno a perseguire la qualità e l'eccellenza del proprio lavoro come obbligo prioritario di un professionista. Nel campo della sicurezza, tale articolo assume un'importanza fondamentale. A complemento di tale principio, l'articolo 2.2 vincola al continuo aggiornamento professionale.

L'articolo 2.3 impegna il professionista alla conoscenza e al rispetto delle leggi applicabili al suo campo di attività.

L'articolo 2.4 afferma l'utilità delle "peer review", cioè della pratica di sottoporre il proprio lavoro alla valutazione di altri membri della comunità che possono suggerire miglioramenti e correzioni.

L'articolo 2.5 impone di fornire al cliente valutazioni complete e approfondite dei sistemi, dei fattori di rischio e delle conseguenze potenziali.

L'articolo 2.6 vincola il professionista a onorare i contratti, gli accordi e le responsabilità che gli sono state assegnate.

L'articolo 2.7 invita i professionisti a condividere la propria conoscenza tecnica con il pubblico, migliorando la comprensione dell'informatica, correggendo le false informazioni e rendendo noti gli impatti e le limitazioni connessi all'uso dei computer (aspetti che diventano una sorta di dovere morale per gli esperti di sicurezza).

L'articolo 2.8 raccomanda ai professionisti di accedere a sistemi e reti solo se autorizzati a farlo

La terza sezione riguarda chi ha mansioni direttive e s'ispira al codice etico dell'IFIP (International Federation for Information Processing), un'organizzazione multinazionale non governativa e non profit nel campo delle tecnologie ICT e delle scienze, riconosciuta dall'ONU e da altri enti internazionali.

L'articolo 3.1, preso atto che ogni tipo di organizzazione ha un impatto sul pubblico, richiama i membri di qualsiasi unità organizzativa ad accettare la responsabilità verso la società. I leader dovrebbero incoraggiare piena partecipazione in tal senso, adottando procedure organizzative e atteggiamenti orientati alla qualità e al benessere della collettività.

L'articolo 3.2 ricorda ai leader delle organizzazioni che i sistemi informativi dovrebbero migliorare la qualità della vita nell'ambiente di lavoro. Quando si realizza un sistema computerizzato - e ciò vale anche per le misure di sicurezza - si deve tenere in considerazione la salute, la dignità e lo sviluppo personale e professionale dei lavoratori.

L'articolo 3.3 richiede alla leadership di definire chiaramente quali sono gli utilizzi leciti e illeciti delle risorse informatiche aziendali. Dato che i computer possono essere usati sia a beneficio sia a danno di un'organizzazione, il loro uso appropriato dovrebbe essere reso noto e supportato. Le regole sull'utilizzo delle risorse informatiche dovrebbero essere limitate per numero e complessità, ma una volta stabilite dovrebbero essere fatte applicare integralmente.

L'articolo 3.4 chiede che gli utenti di un sistema abbiano voce in capitolo durante la fase di valutazione dei requisiti; dopo la realizzazione, si dovrebbe verificare che il sistema risponda a tali requisiti.

L'articolo 3.5 vincola i progettisti e gli implementatori di un sistema a tutelare la privacy e la dignità degli utenti e delle altre parti interessate.

L'articolo 3.6 incoraggia il professionista a creare le opportunità, all'interno dell'organizzazione, per far conoscere i principi e le limitazioni dei sistemi informatici, facilitare la partecipazione del personale e migliorarne le conoscenze informatiche.

I due articoli della quarta sezione impegnano i membri dell'associazione a difendere e promuovere i principi del codice. L'adesione è una questione etica, quindi volontaria, ma in caso di gravi violazioni si può essere espulsi dall'associazione.

Il codice deontologico dell'Institute of Electrical and Electronic Engineers (IEEE)

L'IEEE è la più grande associazione mondiale di tecnici e ingegneri elettrotecnici ed elettronici ed è anche la più antica: benché abbia assunto il nome attuale solo nel 1963, la sua origine risale al 1946, come dimostrano i festeggiamenti del 2006 per il 60° anniversario.

Il codice deontologico dell'IEEE (www.ieee.org/portal/pages/about/whatis/code.html) è molto più breve di quello dell'ACM e non è specifico per i professionisti informatici. Consiste di un decalogo che impegna i membri ad accettare le responsabilità per le proprie scelte tecnologiche e per agire in direzione del massimo bene per la collettività.

Codice Etico dell'IEEE

Noi, membri dell'IEEE, riconoscendo l'importanza delle nostre tecnologie nell'influenzare la qualità della vita di tutto il mondo e accettando la responsabilità personale nei confronti della nostra professione, dei suoi membri e delle comunità che serviamo, con ciò ci impegniamo a osservare il massimo livello di condotta etica e professionale e promettiamo:

1. di accettare la responsabilità di prendere decisioni coerenti con la sicurezza, salute e benessere del pubblico e di rivelare tempestivamente fattori che potrebbero recare danno al pubblico o all'ambiente;

2. di evitare reali o apparenti conflitti d'interesse ogniqualvolta possibile e di rivelarli alle parti interessate quando esistano;

3. di essere onesto e realistico nel formulare affermazioni o valutazioni basate sui dati disponibili;

4. di rifiutare ogni forma di corruzione;
5. di migliorare la comprensione della tecnologia, delle sue applicazioni appropriate e delle potenziali conseguenze;
6. di mantenere e migliorare la nostra competenza tecnica e di assumere incarichi tecnologici per altri solo se qualificato per addestramento o esperienza o dopo completa rivelazione delle limitazioni pertinenti;
7. di cercare, accettare e offrire critica onesta del lavoro tecnico, di riconoscere e correggere gli errori e di assegnare giusto credito ai contributi altrui;
8. di trattare correttamente tutte le persone indipendentemente da fattori come razza, religione, genere, disabilità, età o provenienza;
9. di evitare di danneggiare altri, le loro proprietà, reputazione o impiego attraverso azioni false o dolose;
10. di assistere i colleghi e i collaboratori nel loro sviluppo professionale e di aiutarli a seguire questo codice etico.

Consiglio direttivo dell'IEEE, febbraio 2006

Il codice deontologico per lo sviluppo del software

L'IEEE e l'ACM hanno sviluppato congiuntamente un codice deontologico per lo sviluppo del software, reperibile presso www.acm.org/serving/se/code.htm. Consiste di otto principi fondamentali, riassunti in poche righe nella versione corta e ampliati in sottoarticoli nella versione completa. Gli argomenti delle otto sezioni sono: Pubblico, Cliente e Datore di lavoro, Prodotto, Giudizio, Gestione, Professione, Colleghi e Sé stessi.

Il primo principio impone agli sviluppatori di software di agire costantemente nel pubblico interesse. Lo sviluppatore deve accettare la responsabilità per il proprio lavoro, tenere in considerazione gli interessi di tutte le parti in causa e il bene collettivo, approvare il software solo se è sicuro, è conforme alle specifiche, non reca danno alla qualità della vita e alla privacy e supera i test. Lo sviluppatore deve comunicare eventuali pericoli derivanti dall'uso del software e collaborare agli sforzi per risolverne i problemi. Deve essere corretto e onesto nelle sue affermazioni e contribuire all'informazione e all'istruzione del pubblico.

Il secondo articolo specifica che il professionista, fermo restando il pubblico interesse, deve agire nel migliore interesse del cliente o datore di lavoro. Lo sviluppatore deve fornire servizio nella sua sfera di competenza, non deve usare software ottenuto o conservato illegalmente, deve usare le risorse del cliente nei modi autorizzati, deve basare il proprio lavoro su documenti approvati, deve mantenere il segreto professionale, deve informare il cliente di ogni fattore che può intralciare o far fallire il lavoro o causare problemi per la collettività. Non deve accettare lavori che possano interferire con quello commissionato dal cliente principale e non deve promuovere interessi contrari a quelli del cliente se non per una causa etica superiore.

Il terzo principio vincola gli sviluppatori a perseguire nel loro lavoro il massimo standard professionale possibile, compatibilmente con i costi e i tempi di sviluppo concordati con il cliente e con il coinvolgimento degli utenti e del pubblico. Lo sviluppatore deve valutare se è qualificato per il progetto e assicurare che gli obiettivi siano raggiungibili, deve considerare gli aspetti di contorno (etici, economici, culturali, legali e ambientali), deve utilizzare metodi di lavoro e standard professionali appropriati, deve impegnarsi a comprendere pienamente le specifiche del software, assicurandosi che siano ben documentate e approvate, deve assicurare una stima realistica delle risorse necessarie (tempo, costo, personale) e dei risultati. Deve assicurare adeguate fasi di testing, debugging e documentazione del software, usare informazioni ottenute in modo etico e legale, usare informazioni aggiornate, preservare l'integrità dei dati e la privacy delle persone coinvolte. Anche nella fase di manutenzione lo sviluppatore dovrebbe dimostrare lo stesso livello di professionalità dedicato allo sviluppo.

Il quarto principio chiede agli sviluppatori di mantenere l'integrità e indipendenza del loro giudizio professionale. Lo sviluppatore non deve perdere mai di vista i valori umani, deve approvare solo documenti preparati sotto la sua supervisione o che è in grado di valutare, deve fornire il proprio giudizio tecnico con obiettività, deve rimanere estraneo a qualsiasi pratica corruttiva, deve rivelare i possibili conflitti d'interesse che non sia possibile evitare e deve rifiutarsi di partecipare ad attività dove qualche parte in causa abbia conflitti d'interesse non rivelati.

Il quinto principio verte intorno alla gestione etica dello sviluppo e della manutenzione del software. I manager del progetto devono promuovere procedure che perseguano la qualità e la riduzione dei rischi, assicurare che gli sviluppatori siano al corrente degli standard a cui sono tenuti, applicare le politiche e procedure di sicurezza interna, assegnare il lavoro in base alla competenza professionale e alle potenzialità del personale, stimare in modo realistico costi, tempi, risorse necessarie, qualità, risultati e valutare il relativo margine d'incertezza, attrarre gli sviluppatori potenziali attraverso una descrizione accurata delle condizioni di lavoro, offrire una giusta remunerazione, chiarire gli aspetti di proprietà intellettuale del software sviluppato. Il management deve inoltre definire la procedura da adottare in caso di violazioni del codice (contestazione e difesa), astenersi dal chiedere a uno sviluppatore azioni contrarie al codice e dal comminare punizioni a chiunque esprima preoccupazioni etiche riguardanti un progetto.

Il sesto principio impegna a difendere l'integrità e la reputazione della professione coerentemente con l'interesse pubblico. Lo sviluppatore dovrebbe contribuire a creare un ambiente organizzativo che agisce in modo etico, promuovere la conoscenza dell'ingegneria del software, estendere la propria competenza partecipando ad attività scientifiche e alle organizzazioni professionali, aiutare i colleghi ad applicare il codice, non anteporre i propri interessi a quelli della professione o del cliente, rispettare le leggi applicabili al loro lavoro, essere onesti e precisi nelle dichiarazioni relative al software a cui stanno lavorando e assumersi la responsabilità di rilevare, correggere e documentare gli errori. Lo sviluppatore dovrebbe rendere pubblico il suo impegno a rispettare il codice, evitare di associarsi ad aziende e colleghi che violano il codice, comunicare il proprio punto di vista - quando possibile - alle persone coinvolte in gravi violazioni e nel caso sia impossibile, controproducente o pericoloso, segnalare le violazioni alle autorità.

Il settimo principio promuove un atteggiamento corretto e collaborativo verso i colleghi. Uno sviluppatore dovrebbe incoraggiare i colleghi ad aderire al codice, assisterli nel loro sviluppo professionale, dare il giusto credito al lavoro altrui senza prendersene i meriti, valutare il lavoro altrui in modo onesto, obiettivo e documentato, consentire ai colleghi di esprimere opinioni, preoccupazioni e lamentele, assistere i colleghi nel conoscere e applicare le pratiche standard di lavoro, tra cui le misure di sicurezza, non intervenire indebitamente nella carriera di un collega a meno che l'interesse del cliente o del pubblico non inducano a verificarne la competenza. In situazioni che esulano dalla sua area di competenza, lo sviluppatore dovrebbe chiedere consiglio a esperti di tali aree.

L'ottavo e ultimo principio riguarda gli obblighi di un professionista verso se stesso, attraverso il costante apprendimento e la promozione di un approccio etico verso la professione. Uno sviluppatore deve approfondire la conoscenza delle fasi di sviluppo e del processo di management dei progetti, deve migliorare la capacità di realizzare software affidabile e funzionale con tempi e costi ragionevoli e una documentazione accurata, deve migliorare la comprensione del software su cui lavora e dell'ambiente in cui sarà utilizzato, deve migliorare la conoscenza degli standard e delle leggi riguardanti il software, deve conoscere e applicare sempre meglio il codice al suo lavoro.

5.8.2.6: Conoscere terminologia e aspetti essenziali dell'etica hacker

Inoltre deve trattare gli altri senza farsi influenzare da pregiudizi, deve evitare d'influenzare gli altri verso comportamenti contrari al codice e deve riconoscere che violare il codice è incompatibile con l'essere un professionista dello sviluppo del software.

Il codice deontologico dell'Information Systems Audit and Control Association (ISACA)

L'ISACA è l'associazione internazionale degli auditor informatici e la relativa certificazione CISA (Certified Information Systems Auditor è una delle più valide a livello internazionale, con oltre 44.000 auditor - marzo 2006). In Italia esistono due Capitoli dell'ISACA a Milano e a Roma (vedi elenco presso www.isaca.org/Content/NavigationMenu/About_ISACA/Chapters/ISACA_Chapters_in_Africa_and_Europe.htm#italy).

Il Codice di Etica Professionale di ISACA (www.isaca.org/Template.cfm?Section=Code_of_Professional_Ethics&Template=/TaggedPage/TaggedpageDisplay.cfm&TPLID=14&ContentID=5009) consiste di sette brevi articoli. Esso incoraggia i membri a: 1) supportare l'implementazione di standard, procedure e controlli per i sistemi informativi; 2) eseguire i propri compiti con obiettività, diligenza e cura professionale, secondo gli standard e le pratiche della professione; 3) agire nell'interesse delle parti coinvolte in modo legale e onesto, mantenendo alti standard di condotta ed evitando azioni che discreditino la professione; 4) mantenere il segreto professionale e non usare le informazioni acquisite nello svolgimento dei propri compiti per beneficio personale; 5) mantenere la competenza nel proprio campo e intraprendere solo attività di cui si abbia competenza professionale; 6) informare le parti interessate dei risultati del lavoro svolto, rivelando tutti i fatti significativi noti; 7) supportare l'istruzione professionale delle parti interessate affinché migliorino la propria comprensione della sicurezza e del controllo dei sistemi informativi.

Il codice deontologico dei Certified Information Systems Security Professional (CISSP)

La certificazione CISSP offerta da (ISC)2, che significa International Information Systems Security Certification Consortium, è la più prestigiosa certificazione indipendente nel campo della sicurezza dell'informazione. Anch'essa ha un codice etico (www.cissp.com/cissps/ethics_code.asp) a cui tutti i professionisti CISSP sono strettamente vincolati, come condizione per mantenere il proprio stato.

Il codice s'ispira a quattro regole fondamentali: 1) proteggi la società, il bene comune e l'infrastruttura; 2) agisci in modo onorevole, con giustizia, in modo responsabile e nel rispetto della legalità; 3) presta servizio diligente e competente alle parti interessate; 4) fai progredire e proteggi la professione.

Il codice inizia con un preambolo che vincola ad alti standard etici di comportamento, per il bene della collettività, delle parti interessate e dei colleghi; la stretta adesione al codice è una delle condizioni per ricevere la certificazione.

Dopo l'enunciazione delle quattro regole, o canoni, segue l'enunciazione di una serie di obiettivi che il comitato autore del codice ha ritenuto di dover perseguire e che sono inclusi a scopo informativo, come consigli di comportamento corretto (per esempio incoraggiare la ricerca, l'insegnamento, l'ampliamento della professione) e di comportamento da evitare (creare allarme o falsa rassicurazione, consentire pratiche scorrette, attaccare sistemi vulnerabili, associarsi a non professionisti, dilettanti e criminali). Seguono le quattro regole, ciascuna resa più esplicita da una serie di principi di comportamento che ricalcano, in modo breve e sintetico, i principi esposti dai codici esaminati in precedenza. L'operato di un CISSP dovrebbe essere volto a mantenere l'integrità dei sistemi informativi, promuovere la conoscenza delle misure di sicurezza, scoraggiare le pratiche insicure, rispettare la legge e gli accordi, usare prudenza e onestà, non fornire servizi di cui non si è competenti, evitare conflitti d'interesse, mantenere ed espandere la propria competenza, agire nell'interesse della professione e dei colleghi.

Hacking etico

Tra le tante definizioni della parola hacker, che si sono evolute nel corso del tempo con ramificazioni non sempre attendibili, possiamo ritenere appropriata quella seguente.

Un hacker è una persona che s'impegna ad affrontare sfide intellettuali per aggirare o superare creativamente le limitazioni che gli vengono imposte, non limitatamente ai suoi ambiti d'interesse (che di solito comprendono l'informatica e l'elettronica), ma in tutti gli aspetti della vita.

Un luogo comune diffuso dai media vede il termine hacker associato ai crimini informatici, ma in tal caso è appropriato il temine cracker: colui che entra abusivamente nei sistemi altrui allo scopo di danneggiarli (cracking), lasciare una traccia del proprio passaggio, utilizzarli come teste di ponte per altri attacchi oppure sfruttare le loro capacità di calcolo o l'ampiezza di banda in rete.

Per distinguere hacker da cracker, talvolta l'hacker viene chiamato Hacker etico (animato da buone intenzioni) per distinguerlo dal cracker, che è anche chiamato Black hat (cappello nero) nella scia dei vecchi film western di Hollywood, che a beneficio del pubblico distinguevano i buoni (col cappello bianco) dai cattivi (col cappello nero).

Un ethical hacker è colui che, debitamente autorizzato, attacca un sistema informativo per individuarne le vulnerabilità. Molte grandi aziende hanno assunto questo tipo di figura; negli USA l'International Council of Electronic Commerce Consultants (EC-Council) fornisce, previo esame a pagamento, la certificazione CEH (Certified Ethical Hacker) e decine di grandi aziende e organizzazioni statali e militari hanno fatto certificare un loro esperto in sicurezza. Intense School, in Florida, è un esempio di "hacker college" che prepara gli studenti a superare l'esame CEH. La scuola tiene ogni anno circa 200 corsi di information security, a dimostrazione che i buoni esperti di sicurezza devono saper indossare i panni di un hacker.

L'ethical hacking è un servizio di ricerca delle vulnerabilità di reti e sistemi, basato sulle tecniche e sugli strumenti usati dai cracker, al fine d'individuare e attuare le contromisure necessarie a proteggere adeguatamente le risorse informatiche. Il servizio è svolto sia dall'esterno, tramite Internet o via rete wireless, sia dall'interno, attraverso la LAN aziendale.

L'attività di ethical hacking viene svolta generalmente attraverso attacchi simulati alla rete aziendale che prendono il nome di penetration test o security probe e sono attuati da specialisti di tecniche anti-intrusione. Tali attività sono talvolta condotte da gruppi di professionisti che sono chiamati anche Tiger Team, dal nome delle squadre che, nelle forze armate USA, avevano il compito di saggiare la sicurezza delle installazioni amiche, lasciando tracce del loro passaggio.

Gli ethical hacker, consulenti o dipendenti di aziende di sicurezza informatica, possiedono una varietà di competenze e utilizzano uno spettro di strumenti ampiamente documentato in libri e siti sull'argomento. Un campione di strumenti d'indagine, tutti OpenSource, potrebbe essere: whois, dig, traceroute, tcptraceroute, nmap, telnet, netcat, nikto, hydra, nessus, Kismet, Airsnort, Cain&Abel, ma ce ne sono tanti altri. Tuttavia, il requisito primario di un hacker etico non è tecnico (l'abilità tecnica è necessaria, ma non sufficiente), bensì l'essere degno di fiducia. Mentre mette alla prova la sicurezza informatica di un cliente, l'hacker eti-

co può scoprire informazioni segrete, che se divulgate potrebbero motivare veri cracker a compiere intrusioni, con possibili danni economici per il cliente. Inoltre la sensibilità delle informazioni con cui l'ethical hacker viene a contatto richiede che i sistemi informatici utilizzati dall'ethical hacker siano a loro volta a prova di intrusione. Questo è un caso in cui il detto che il ciabattino ha le scarpe bucate non è applicabile. Il contratto tra il cliente e l'hacker etico, oltre ad autorizzare l'intrusione e a specificare i sistemi interessati e i tempi e modalità d'azione, dovrà includere una serie di requisiti di sicurezza da parte dello stesso hacker etico.

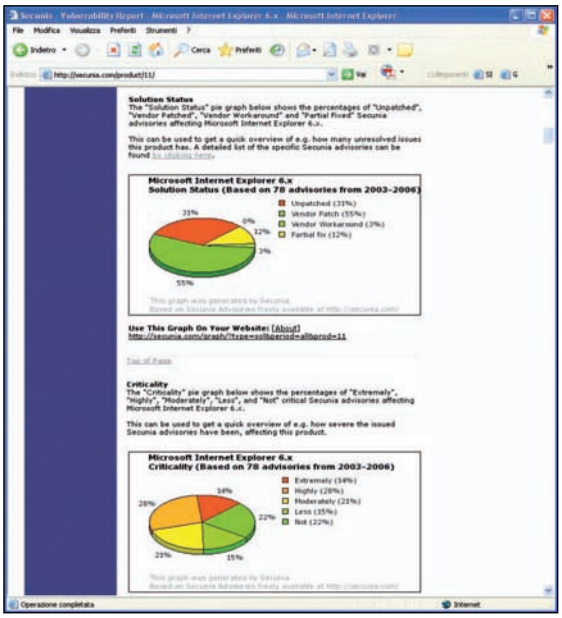
Gli accordi contrattuali per definire esattamente l'attività di un hacker etico sono d'importanza fondamentale, anche per evitare il rischio di risvolti illegali. L'articolo 615 ter del Codice Penale italiano punisce chiunque si introduce abusivamente in un sistema informatico o telematico protetto da misure di sicurezza o vi si mantiene contro la volontà espressa o tacita di chi ha il diritto di escluderlo. Le attività di ethical hacking sono svolte con il consenso di chi detiene il "diritto di esclusione" citato dalla legge, quindi non sono perseguibili a condizione che non eccedano i termini contrattuali concordati tra cliente e fornitore del servizio.

Per evitare malintesi e inconvenienti, nella prassi l'ethical hacker e il cliente stipulano un contratto che disciplina ogni aspetto dell'attività di ethical hacking e che pone il consulente al riparo da eventuali procedimenti o responsabilità penale. Tale contratto è anche detto "get free out of jail card" (cartolina per uscire di prigione gratis). Non si può infatti escludere che qualche addetto alla sicurezza, rilevando un'intrusione particolarmente devastante, avvisi le autorità, mettendo in moto il meccanismo investigativo e giudiziario. Generalmente, è preferibile che il minor numero di persone possibile sia al corrente dell'attacco simulato, per evitare che vengano attivate protezioni e disattivate risorse, alterando lo stato abituale dei sistemi. C'è anche una ragione meno ovvia, per non avvertire il personale: specialmente in una grande azienda, c'è il rischio che la notizia dell'attacco simulato arrivi alle orecchie di un cracker, che potrebbe sfruttare l'attacco dell'ethical hacker per preparare un attacco realmente dannoso. L'accordo tra cliente ed ethical hacker deve specificare con precisione i sistemi, le reti, gli indirizzi, le risorse da attaccare per verificarne le misure di difesa. Può essere concordato un orario al di fuori delle ore di lavoro, per evitare danni alla produzione, ma in linea di massima è preferibile che l'attacco si svolga "senza limiti" all'efficacia dei tentativi di penetrazione; se non lo fa l'ethical hacker, potrebbe farlo un cracker e l'azienda non saprebbe prevederne l'esito. Un altro criterio che il cliente non digerisce volentieri è la durata dell'attacco dopo la penetrazione nella rete e nei sistemi. Dovrebbe essere scoraggiato l'atteggiamento prudenziale di interrompere l'attacco dopo i primi cedimenti, perché impedirebbe all'ethical hacker di scoprire tutte le vulnerabilità e le informazioni rilevanti. E' comunque necessario che l'ethical hacker fornisca al cliente un quadro accurato e realistico dei rischi potenziali del suo attacco.

Si racconta di attacchi dei Tiger Team militari che, dopo un successo, hanno causato scossoni negli organigrammi; negli ambienti civili a volte serve uno scossone che riveli le falle, smascheri le false sicurezze e l'indifferenza e permetta all'azienda di affrontare le responsabilità per la sicurezza previste anche dalla legge. Il personale può reagire a un'ispezione a sorpresa come se fosse una minaccia personale, perciò il management aziendale deve essere preparato a tranquillizzare gli animi (senza peraltro essere avvertito in anticipo).

L'hardware e soprattutto il software sono soggetti a errori e vulnerabilità, come è stato dimostrato in primo luogo da Microsoft (con le frequenti patch di Windows e degli altri prodotti) e ormai anche da molti altri produttori, che periodicamente inviano gli aggiornamenti online. Ciò vale per i sistemi operativi (come le distribuzioni Linux e Mac OS) e per le applicazioni (per esempio database e office automation). Siti come secunia.com, sans.org e securityfocus.com tengono un costante monitoraggio delle principali vulnerabilità e ne segnalano la gravità sia sul sito sia attraverso e-mail newsletter. Per esempio, in marzo 2006, il 31% delle 78 vulnerabilità di Internet Explore 6.x censite da Secunia tra il 2003 e il 2006 era privo di correzione; le 78 falle erano giudicate per il 14% estremamente critiche e per il 28% altamente critiche.

La homepage di *Secunia.com*



Numero e gravità *delle falle di Internet Explorer 6 secondo Secunia.com*

Quando un ricercatore indipendente riporta in dettaglio una vulnerabilità hardware o software, si dice che essa ha avuto full disclosure, cioè piena rivelazione. Ciò spesso è criticato anche aspramente dai produttori, che non amano essere accusati (talvolta a buon diritto) di produrre software insicuro. La maggiore motivazione dell'opposizione alle full disclosure è che incoraggiano lo sfruttamento delle falle da parte dei cracker prima che sia disponibile una patch per correggere l'errore o almeno turare la falla.

La responsible disclosure (rivelazione responsabile), di-

versamente dalla full disclosure, si limita a pubblicare liste di vulnerabilità senza i dettagli tecnici che potrebbero favorirne lo sfruttamento.

Infine, la non disclosure consiste nel rilasciare la patch per un determinato prodotto senza indicare in dettaglio la vulnerabilità; questa la pratica consueta dei produttori di software, in parte giustificata dal fatto che molti clienti non applicano tutti gli aggiornamenti (o non lo fanno prontamente), quindi sarebbero facili vittime dei cracker che sfruttassero i dettagli tecnici della vulnerabilità appena corretta.

5.8.2.7: Conoscere le principali forme di crimini informatici

Crimine informatico

Le tecnologie informatiche e il loro utilizzo distorto, a scopo dannoso, si sono evoluti più rapidamente degli ordinamenti giuridici, che spesso si sono trovati impreparati ad affrontare nuove tipologie di reati. Non potendosi applicare, a livello penale, analogie con altri tipi di reato, i crimini informatici inizialmente non sono stati perseguibili attraverso le leggi vigenti. Per tale motivo, la Raccomandazione R 89/9 del 13/9/1989 del Comitato dei ministri del Consiglio d'Europa, avente per soggetto la criminalità informatica, invitava gli stati membri, in occasione della promulgazione di nuove leggi o di revisione di quelle esistenti, a seguire i principi enunciati dal rapporto sulla criminalità informatica del comitato europeo sui problemi criminali.

Il legislatore italiano, venendo incontro a tali indicazioni, con la legge 547 del 23/12/1993 ha aggiornato il Codice Penale inserendo nuove fattispecie di crimine, relative al campo informatico, che hanno introdotto nuovi concetti giuridici e nuove categorie di beni tutelati dalla legge.

La maggior parte delle nuove fattispecie criminose introdotte dalla legge 547/93 prevede un'aggravante specifica quando il reato è commesso da un "operatore" del sistema, visto che tale figura, avendo ampio o totale accesso alle risorse del sistema, ha un livello di responsabilità pari alla posizione di vantaggio che potrebbe usare per compiere azioni criminose.

Accesso abusivo a un sistema informatico o telematico, art. 615 ter C.P.

La legge sui crimini informatici ha introdotto il nuovo bene giuridico, protetto dalla legge penale, di "domicilio informatico", in virtù del quale, i sistemi informatici e telematici non sono più semplici strumenti, ma spazi in cui il soggetto ha il diritto di esercitare le proprie attività, con la facoltà di escludere i soggetti terzi non graditi. Viene quindi punito chiunque si introduce abusivamente in un sistema informatico o telematico o vi si mantiene contro la volontà tacita o espressa di chi ha il diritto di escluderlo.

La sanzione prevede aggravanti nel caso di abuso della qualità di operatore del sistema e qualora dal fatto derivi la distruzione o il danneggiamento del sistema o l'interruzione totale o parziale del suo funzionamento, ovvero la distruzione o il danneggiamento dei dati, delle informazioni o dei programmi in esso contenuti.

Detenzione abusiva di codici d'accesso a sistemi informatici o telematici, art. 615 quater C.P.

Viene punito chiunque, al fine di procurare a sé o ad altri un profitto o di arrecare ad altri un danno, abusivamente si procura, riproduce, diffonde, comunica o consegna codici, parole chiave o altri mezzi idonei all'accesso a un sistema informatico o telematico, protetto da misure di sicurezza, o comunque fornisce indicazioni o istruzioni idonee a tale scopo. E' prevista un'aggravante se il fatto è commesso con abuso della qualità di operatore del sistema.

Diffusione di programmi diretti a danneggiare o interrompere un sistema informatico, art. 615 quinquies C.P.

Viene punito chiunque diffonde, comunica o consegna un programma informatico da lui stesso o da altri redatto, avente per scopo o per effetto il danneggiamento di un sistema informatico o telematico, dei dati o dei programmi in esso contenuti o ad esso pertinenti, ovvero l'interruzione, totale o parziale, o l'alterazione del suo funzionamento.

Violazione, sottrazione e soppressione di corrispondenza, art. 616 C.P.

Viene punito chiunque prende cognizione del contenuto di una corrispondenza chiusa, a lui non diretta, ovvero sottrae o distrae, al fine di prenderne o di farne ad altri prendere cognizione, una corrispondenza chiusa o aperta, a lui non diretta, ovvero, in tutto o in parte, la distrugge o la sopprime. Se il colpevole, senza giusta causa, rivela, in tutto o in parte, il contenuto della corrispondenza, è punito se dal fatto deriva un danno e il fatto stesso non costituisce più grave reato.

Per corrispondenza si intende quella epistolare, telegrafica, telefonica, informatica o telematica ovvero effettuata con ogni altra forma di comunicazione a distanza.

Intercettazione, impedimento o interruzione illecita di comunicazioni informatiche o telematiche, art. 617 quater C.P.

Viene punito chiunque in modo fraudolento intercetta comunicazioni relative a un sistema informatico o telematico o intercorrenti tra più sistemi, ovvero le impedisce o le interrompe. Salvo che il fatto costituisca più grave reato, la stessa pena si applica a chiunque rivela, mediante qualsiasi mezzo di informazione al pubblico, in tutto o in parte, il contenuto di tali comunicazioni. E' prevista un'aggravante se il fatto è commesso con abuso della qualità di operatore del sistema.

Installazione di apparecchiature atte a intercettare, impedire o interrompere comunicazioni informatiche o telematiche, art. 617 quinquies C.P.

Viene punito chiunque, fuori dai casi consentiti dalla legge, installa apparecchiature atte a intercettare, impedire o interrompere comunicazioni relative a un sistema informatico o telematico ovvero intercorrenti tra più sistemi. E' prevista un'aggravante se il fatto è commesso con abuso della qualità di operatore del sistema.

Falsificazione, alterazione o soppressione del contenuto di comunicazioni informatiche o telematiche, art. 617 sexies C.P.

Chiunque, al fine di procurare a sé o ad altri un vantaggio o di arrecare ad altri un danno, forma falsamente ovvero altera o sopprime, in tutto o in parte, il contenuto, anche occasionalmente intercettato, di taluna delle comunicazioni relative a un sistema informatico o telematico o intercorrenti fra più sistemi, è punito qualora ne faccia uso o lasci che altri ne facciano uso. E' prevista un'aggravante se il fatto è commesso con abuso della qualità di operatore del sistema.

Danneggiamento di sistemi informatici e telematici, art. 635 bis C.P.

Viene punito chiunque distrugge, deteriora o rende,

in tutto o in parte, inservibili sistemi informatici o telematici altrui, ovvero programmi, informazioni o dati altrui. E' prevista un'aggravante se il fatto è commesso con abuso della qualità di operatore del sistema.

Frode informatica, art. 640 ter C.P.

L'ordinamento punisce chiunque, alterando in qualsiasi modo il funzionamento di un sistema informatico o telematico o intervenendo senza diritto con qualsiasi modalità su dati, informazioni o programmi contenuti in un sistema informatico o telematico o ad esso pertinenti, procura a sé o ad altri un ingiusto profitto con altrui danno. E' prevista un'aggravante se il fatto è commesso con abuso della qualità di operatore del sistema.

Altri reati via Internet

I crimini informatici sopra citati, caratterizzati da pratiche illecite da parte di soggetti con adeguate conoscenze tecniche, non sono le uniche fattispecie di reati che possono essere commessi attraverso Internet o le reti telematiche. La tutela dei minori e la lotta contro la pedofilia sono esempi di attività di contrasto di crimini che sfruttano Internet per lo scambio illegale di informazioni.

A tale proposito, il Codice Penale è stato aggiornato con la legge 269/2998 che ha introdotto nuove fattispecie di reato in materia di pornografia minorile.

Ai sensi dell'art. 600 ter, è punito chiunque, al di fuori delle ipotesi di sfruttamento di minori di anni diciotto, al fine di realizzare esibizioni pornografiche, di produzione e di commercio di materiale pornografico, con qualsiasi mezzo, anche per via telematica, distribuisce, divulga o pubblicizza il materiale pornografico ovvero distribuisce o divulga notizie o informazioni finalizzate all'adescamento o allo sfruttamento sessuale di minori degli anni diciotto

Nel quadro di riferimento per la formulazione dei crimini informatici va citata la Convenzione di Budapest del Consiglio d'Europa del 23 novembre 2001, sottoscritta anche dall'Italia, che rappresenta il primo tentativo di disciplina dei reati informatici a livello europeo. Ad essa seguono la decisione quadro del Consiglio d'Europa relativa agli attacchi contro i sistemi di informazione del 19 aprile 2002 e la decisione quadro 2004/68 del Consiglio d'Europa del 22 dicembre 2003 relativa alla lotta contro lo sfruttamento sessuale dei bambini e della pedopornografia infantile.

Infine, un intero capitolo potrebbe essere dedicato alle vicende legate alla legislazione del diritto d'autore, che è stata oggetto di scontri e polemiche fra le parti interessate. Con la legge Urbani (Decreto legge 72 del 22 marzo 2004 convertito in legge con modificazioni dalla legge 128 del 21 maggio 2004) è stato modificato l'art. 171 ter della Legge sul diritto d'autore, introducendo una specifica sanzione per chiunque, a scopo di profitto, comunica al pubblico, immettendola in un sistema di reti telematiche, mediante connessioni di qualsiasi genere, un'opera dell'ingegno protetta da diritto d'autore o parte di essa in violazione dell'art. 16 della Legge sul diritto d'autore. La criticata legge Urbani è stata solo la prima di una serie di normalizzazioni che secondo i detrattori difendono più gli interessi delle corporation che quelli dei cittadini.

Siti e mailing list di sicurezza informatica

Quello che segue è solo un piccolo campione utile come punto di partenza. Esistono innumerevoli siti e mailing list dedicati alla sicurezza informatica, alla preparazione per le certificazioni e al diritto nel mondo informatico e telematico. Una ricerca con Google e le parole chiave opportune fornirà un panorama aggiornato delle aree di interesse.

Legislazione
ICTLEX www.ictlex.net
Testi, documenti, normativa e giurisprudenza su Internet e quello che le ruota attorno
NewLaw, www.newlaw.it
Novità giuridiche ed economiche dell'information technology
InterLex, www.interlex.it
Periodico plurisettimanale di carattere informativo, scientifico e culturale giuridico
MediaLaw, www.medialaw.it
Rivista tematica su diritto dell'informazione e dell'informatica, privacy e diritto d'autore
NetJus, www.netjus.org
Diritto dell'informatica e informatica giuridica
Italian Cyberspace Law Conference, www.iclc.org
Evento annuale dedicato al diritto delle nuove tecnologie, dell'informatica e delle telecomunicazioni

Siti istituzionali
Consiglio d'Europa, www.coe.int
La più vecchia (1949) organizzazione politica del continente
Garante per la protezione dei dati personali, www.garanteprivacy.it
Protezione dei dati personali in ogni settore della vita sociale, economica e culturale
Centro Nazionale per l'Informatica nella Pubblica Amministrazione, www.cnipa.it
Supporto alla pubblica amministrazione nell'utilizzo efficace dell'informatica

Associazioni di categoria
ACM, Association for Computing Machinery, www.acm.org
IEEE, Institute of Electrical and Electronic Engineers, www.ieee.org
IEEE Computer Society, www.computer.org
ISACA, Information Systems Audit and Control Association, www.isaca.org
(ISC)2, International Information Systems Security Certification Consortium, www.isc2.org
CSI, Computer Security Institute, www.gocsi.com
SANS (SysAdmin, Audit, Network, Security) Institute, www.sans.org
CLUSIT, Associazione Italiana per la Sicurezza Informatica, www.clusit.it

Certificazioni e materiali di studio
Certificazione CISSP, www.cissp.com
Global Information Assurance Certification, www.giac.org

Mailing list
Una quarantina di mailing list di sicurezza, inclusa la nota BugTraq: www.securityfocus.com/archive
Cryptogram, email newsletter mensile di Bruce Schneier: www.schneier.com/crypto-gram.html
Una decina di newsletter di SANS: www.sans.org/newsletters
Mailing list in italiano MI (sicurezza informatica) e Lex (diritto nell'ICT): www.sikurezza.org/wiki/Main/Liste

Etica e privacy della biometria

Negli anni recenti lo sviluppo delle tecnologie biometriche e la richiesta di strumenti di autenticazione più efficaci validi anche su vasta scala hanno accelerato la diffusione di applicazioni biometriche. Queste sono basate per lo

5.8.2.8: Conoscere le mailing-list e URL principali relativi alle aree della sicurezza informatica

5.8.2.9: Essere consapevoli degli aspetti etici e di tutela della privacy relativi alla biometria

più sul riconoscimento di caratteristiche fisiche, come le impronte digitali, la geometria della mano, la forma dell'iride o della retina, la voce o il volto.

La biometria pone una minaccia per la privacy, perché il suo utilizzo porta a una perdita di autonomia dell'individuo, fornisce allo stato gli strumenti di monitoraggio dei cittadini e solleva obiezioni di natura filosofica, culturale e religiosa. D'altra parte, la biometria può essere usata per proteggere l'integrità delle informazioni e per impedire il furto d'identità. I governi e le organizzazioni internazionali hanno quindi un ruolo importante nel regolamentare l'uso delle tecnologie biometriche, in particolare la raccolta e la diffusione dei dati biometrici.

La privacy consiste di tre componenti: segretezza, anonimato e solitudine. In una scena ideale di privacy perfetta, nessuno ha informazioni su X, nessuno presta attenzione a X e nessuno ha accesso fisico a X (R. Gavison, "Privacy and the limits of the law", Yale Law Journal, 1980). Un quarto di secolo fa tale visione era facilmente condivisibile. La recrudescenza delle azioni terroristiche ha spostato il punto di vista delle popolazioni colpite, inclini (o persuasi dai media) a rinunciare a una quota significativa dei propri diritti civili in cambio di maggiore sicurezza. D'altra parte, tale atteggiamento rischia d'innescare un feedback positivo tra eventi allarmanti e restrizioni dei diritti umani e civili, declinato in modi diversi a seconda delle condizioni politiche e sociali degli stati. Per esempio, negli Stati Uniti l'evento dell'11 settembre ha motivato, tra le molte iniziative, l'adozione del controllo delle impronte digitali all'immigrazione, il progetto del passaporto biometrico, lo sviluppo del riconoscimento facciale e via dicendo. Misure che oggi sarebbero considerate impopolari e degne del grande fratello orwelliano, sono da anni nel cassetto, pronte all'uso in caso di necessità.

R. Clarke ("Human Identification in Information Systems: Management Challenges and Public Policy Issues", Information Technology and People, dic. 1994) ha osservato che qualunque mezzo ad alta integrità per il riconsocimento umano, come gli strumenti biometrici, rappresenta una minaccia per le libertà civili perché costituisce la base per uno schema generalizzato d'identificazione che fornirebbe un enorme potere sulla popolazione. L'intero comportamento umano diverrebbe trasparente per lo stato e ogni nonconformismo e dissenso potrebbe essere imbavagliato. La storia ha dimostrato che informazioni personali raccolte inizialmente per uno scopo limitato, in seguito, a fronte di eventi che hanno giustificato lo stato di necessità, sono state utilizzate a scopo restrittivo e repressivo. Un esempio è il censimento degli stranieri, l'insorgere di ostilità o conflitti bellici e la conseguente detenzione.

Alla luce dell'esperienza, è diffuso il timore che informazioni biometriche raccolte per salvaguardare gli interessi dei cittadini e inizialmente utilizzate per scopi limitati (contrasto alle frodi, sicurezza aeroportuale, protezione dei bambini), gradualmente verrebbero diffuse e utilizzate per scopi diversi da quelli dichiarati in origine. Le leggi stesse verrebbero modificate di conseguenza. Il giudice americano L. Brandeis dichiarò nel 1927: "L'esperienza ci dovrebbe insegnare a stare in guardia per proteggere la libertà soprattutto quando i propositi del governo sono benevoli. Gli uomini nati per la libertà sono vigili per natura e pronti a respingere le invasioni della loro libertà da parte di governanti male intenzionati. I maggiori pericoli per la libertà sono in agguato sotto forma di insidiosa impercettibile invasione da parte di uomini zelanti, apparentemente di buone intenzioni, ma privi di comprensione". La predizione di Brendeis si è avverata periodicamente, per esempio quando il Social Security Number americano, istituito con l'esplicita clausola "Not for identification" (da non usare per l'identificazione dei cittadini), nel 1961 fu trasformato dall'IRS (l'ufficio delle imposte USA) in uno strumento di identificazione simile al nostro codice fiscale. Oggi l'SSN è pressoché indispensabile per la maggior parte delle transazioni che coinvolgono credito, assicurazioni, impiego, patente di guida, cure mediche eccetera; il passo successivo è la carta d'identità biometria. Tale avanzamento lento e strisciante delle funzioni di controllo, così graduale da passare inosservato, è chiamato "function creep" e inizia sempre con un'iniziativa apparentemente desiderabile e innocua.

Anche in Europa l'uso generalizzato e incontrollato della biometria solleva preoccupazioni per la minaccia ai diritti e alle libertà fondamentali dei cittadini. La legge italiana sulla privacy (196/2003) all'articolo 37 prevede che i titolari del trattamento dei dati personali (anche biometrici) debbano notificare tale trattamento al garante per la tutela dei dati personali.

A livello europeo, il Gruppo di lavoro per la protezione degli individui per quanto riguarda il trattamento dei dati personali, il 1° agosto 2003, ha adottato il "Documento di lavoro sulla biometria" nel quale fissa i principi da osservare per un corretto trattamento dei dati biometrici in relazione alla direttiva CE 95/46.

Il gruppo di lavoro definisce come sistemi biometrici le applicazioni di tecnologie biometriche che permettono l'identificazione e/o l'autenticazione/verifica automatica di un individuo. L'elemento biometrico è considerato universale (presente in tutte le persone), unico (distintivo di ciascuna persona) e permanente (valido nel tempo). Il gruppo di lavoro distingue le tecniche biometriche in due categorie: di tipo fisico e fisiologico (come le impronte digitali) e di tipo comportamentale (come la firma autografa).

Nella fase di "iscrizione" i dati biometrici vengono raccolti ed elaborati in un modello ridotto archiviato in formato digitale. Dato che alcuni dati biometrici grezzi possono rivelare informazioni sensibili (razza, etnia, salute), in tali casi si devono applicare le norme che li tutelano.

I dati biometrici possono essere registrati su vari tipi di supporto, come hard disk di un database centralizzato o dispositivi da portare con sé (token USB, Smart Card, schede ottiche). A scopo di autenticazione (dimostrare che si è chi si dichiara di essere), non occorre memorizzare i dati di riferimento in un database centralizzato; ciò è invece necessario per l'identificazione (scoprire l'identità dell'individuo).

Il gruppo di lavoro fornisce una serie di principi fondamentali per il trattamento di dati biometrici.

Principio della finalità

Per contrastare abusi e il function creep sopra citato, è necessario innanzitutto che sia determinato lo scopo del rilevamento e trattamento dei dati biometrici.

Il gruppo di lavoro ritiene che ai fini del controllo degli accessi tramite autenticazione siano da preferire i sistemi biometrici non basati sull'archiviazione dei dati biometrici di riferimento (per esempio in un database o nel dispositivo di controllo). Visto che l'autenticazione richiede solo la corrispondenza tra il campione biometrico rilevato al momento e il campione di riferimento conservato in una Smart Card o altro dispositivo mobile affidato all'interessato, non c'è ragione di cedere a terzi il campione di riferimento, con il rischio di uso illecito.

Ne segue che il trattamento dei dati biometrici è vietato se incompatibile con lo scopo dichiarato per il loro utilizzo. Per esempio, dati destinati all'autenticazione non possono essere usati a fini di sorveglianza.

Si deve tenere conto anche della facilità con cui certe categorie di dati biometrici sono rilevabili all'insaputa dei soggetti interessati. Sono documentate le modalità di rilevamento e riproduzione di impronte digitali e scansioni dell'iride capaci di ingannare i dispositivi correnti, che il più delle volte non utilizzano tecniche costose e sofisticate di riconoscimento di un organo vivo. Di conseguenza, una eventuale raccolta centralizzata di dati biometrici aumen-

terebbe ulteriormente il rischio di utilizzo illegale dei dati per tracciare profili di comportamento degli interessati e il rischio di diffusione dei dati biometrici allo scopo di commettere truffe, effrazioni e altre azioni criminali. Considerando che i dati biometrici durano per la vita, diversamente da un password o da una coppia di chiavi, il rischio per la privacy (in particolare il furto d'identità) è consistente. Un modo per limitarlo è limitare l'interoperabilità di sistemi diversi che utilizzano dati biometrici.

Principio di proporzionalità

I dati biometrici raccolti non devono contenere più informazioni di quante siano necessarie allo scopo d'identificare o autenticare le persone. I dati superflui dovrebbero essere eliminati il prima possibile.

D'altra parte, i sistemi biometrici potrebbero servire a difesa della privacy quando permettono di diminuire il trattamento di altri dati personali quali il nome, l'indirizzo, la residenza, eccetera.

Principio di lealtà della raccolta e dell'informazione

I dati biometrici devono essere trattati e soprattutto rilevati in modo leale. Il responsabile del trattamento deve comunicare alla persona interessata la finalità del trattamento e l'identità di chi ne è responsabile. Devono essere evitati i sistemi che raccolgono dati biometrici all'insaputa dei soggetti interessati. In particolare, si deve tenere conto che i sistemi basati sul riconoscimento a distanza del volto, la rilevazione delle impronte digitali, la registrazione della voce (e potremmo aggiungere il rilevamento dell'iride, anche a distanza) presentano maggiori rischi da tale punto di vista.

Misure di sicurezza

Questa sezione comprende una serie di regole che devono essere conosciute e applicate da qualunque organizzazione interessata all'installazione di sistemi biometrici.

Il responsabile della custodia e del trattamento dei dati biometrici deve provvedere ad adottare misure di sicurezza idonee a garantire la protezione dei dati personali dalla perdita o distruzione accidentale o illecita, dall'alterazione, dalla diffusione o dall'accesso non autorizzato. Tali misure includono ad esempio la cifratura dei modelli biometrici di riferimento, la protezione delle chiavi di cifratura e il controllo e protezione degli accessi, così da rendere pressoché impossibile risalire ai dati originali partendo dai modelli.

Il gruppo di lavoro valuta favorevolmente la possibilità di usare i dati biometrici come chiavi di cifratura. Questo permetterebbe di evitare la creazione di database di modelli biometrici, potenzialmente utilizzabili per fini illeciti. In tal modo, la decodifica dei dati sarebbe possibile solo attraverso una nuova rilevazione del campione biometrico presso la persona interessata.

Le misure di sicurezza devono essere adottate fin dalla fase di "iscrizione", quando i dati biometrici vengono trasformati in modelli o immagini. Il gruppo di lavoro ritiene che in questa fase sia altissimo il rischio di perdita di integrità, riservatezza e disponibilità dei dati, il che avrebbe conseguenze irreparabili per le persone interessate. Viste le loro caratteristiche, la sottrazione dei dati biometrici equivale a una sottrazione d'identità.

Secondo il gruppo di lavoro, anche gli errori dei sistemi biometrici possono avere pesanti conseguenze per gli interessati, portando al rifiuto erroneo di individui autorizzati e all'accettazione indebita di soggetti non autorizzati, rendendo particolarmente arduo, se non impossibile, accertare la verità. Affidarsi in modo scriteriato alle macchine per vietare in modo definitivo l'accesso ai viaggi aerei o l'ingresso in una nazione, come riportato dalle cronache (e temuto dal giudice Brandeis), è opera di "uomini zelanti, apparentemente di buone intenzioni, ma privi di comprensione".

Nell'ultimo articolo, il gruppo di lavoro incoraggia l'adozione di codici di condotta che recepiscano i principi di protezione dei dati e la direttiva 95/46 CE.

Un ottimo testo di riferimento riguardante la biometria è "Biometrics", di Woodward, Orlans e Higgins, McGraw-Hill/Osborne, 2003.

Normative europee

5.8.3 Normative europee

5.8.3.1: Conoscere gli aspetti legali della firma digitale, anche in relazione alle direttive della Comunità Europea

Nell'ordinamento giuridico italiano la firma digitale a crittografia asimmetrica (detta anche a chiave pubblica) è riconosciuta ed equiparata a tutti gli effetti alla firma autografa su carta. Il primo atto normativo in tal senso fu il DPR 513/1997 (Decreto del Presidente della Repubblica) in attuazione dell'art. 15 della legge 59/1997. Successivamente tale normativa fu trasposta nel DPR 445/2000 ("Disposizioni legislative in materia di documentazione amministrativa", il testo unico sulla documentazione amministrativa) più volte modificato negli anni successivi per conformare la normativa italiana a quella comunitaria contenuta nella Direttiva 1999/93/CE del Parlamento europeo e del Consiglio dell'Unione Europea del 13 dicembre 1999 relativa ad un quadro comunitario per le firme elettroniche.

Oggi la legge che disciplina la firma digitale è il Decreto Legislativo 7 marzo 2005, n. 82 "Codice dell'amministrazione digitale". L'articolo 1 del decreto include le seguenti definizioni:

q) firma elettronica: l'insieme dei dati in forma elettronica, allegati oppure connessi tramite associazione logica ad altri dati elettronici, utilizzati come metodo di autenticazione informatica;

r) firma elettronica qualificata: la firma elettronica ottenuta attraverso una procedura informatica che garantisce la connessione univoca al firmatario e la sua univoca autenticazione informatica, creata con mezzi sui quali il firmatario può conservare un controllo esclusivo e collegata ai dati ai quali si riferisce in modo da consentire di rilevare se i dati stessi siano stati successivamente modificati, che sia basata su un certificato qualificato e realizzata mediante un dispositivo sicuro per la creazione della firma, quale l'apparato strumentale usato per la creazione della firma elettronica;

s) firma digitale: un particolare tipo di firma elettronica qualificata basata su un sistema di chiavi crittografiche, una pubblica e una privata, correlate tra loro, che consente al titolare tramite la chiave privata e al destinatario tramite la chiave pubblica, rispettivamente, di rendere manifesta e di verificare la provenienza e l'integrità di un documento informatico o di un insieme di documenti informatici;

Il decreto 82/2005 prevede la possibilità di avere più tipi di firma elettronica qualificata, vale a dire più sistemi che consentano l'identificazione univoca del titolare, uno dei quali è la firma digitale a chiavi asimmetriche. Di fatto, la firma digitale è l'unico tipo di firma elettronica qualificata oggi utilizzato, perciò i due concetti tendono a coincidere.

In base all'art. 5, a decorrere dal 30/6/2007, le pubbliche amministrazioni centrali con sede nel territorio italiano consentono l'effettuazione dei pagamenti ad esse spettanti, a qualsiasi titolo dovuti, con l'uso delle tecnologie dell'informazione e della comunicazione.

Da notare che, per le regole tecniche di formazione, la trasmissione, la conservazione, la duplicazione, la riproduzione e la validazione, anche temporale, dei documenti informatici, si applica il DPCM del 13/1/2004 (Decreto del Presidente del Consiglio dei Ministri), che tra l'altro regola l'uso delle marche temporali che certificano le date dei documenti informatici.

L'articolo 21 del DL 82/2005 stabilisce, con un rimando al Codice Civile, che la firma digitale (o altra firma elettronica qualificata) è probatoria salvo querela per falso, equiparando il documento informatico sottoscritto con firma digitale alla scrittura privata con firma autografa.

La titolarità della firma digitale è garantita dagli enti certificatori accreditati presso il CNIPA (Centro Nazionale per l'Informatica nelle Pubbliche Amministrazioni, ex AIPA), che tengono registri delle chiavi pubbliche presso i quali si può verificare la titolarità del firmatario di un documento elettronico (verificando la validità del certificato digitale del titolare e dei certificati delle Certification Authority interessate). L'attività dei certificatori è disciplinata da decine di clausole di cui agli artt. 26-32.

L'acquisizione di una chiave privata è a pagamento e ha una scadenza, nonostante sia un mezzo legale per l'esercizio dei diritti naturali della persona.

La direttiva 99/93 CE è reperibile presso www.giustizia.it/cassazione/leggi/direttiva93_99.html.

Gli effetti giuridici della firma sono sintetizzati nell'art. 5 della direttiva:

Direttiva 99/93 CE, Articolo 5 - Effetti giuridici delle firme elettroniche

1. Gli Stati membri provvedono a che le firme elettroniche avanzate basate su un certificato qualificato e create mediante un dispositivo per la creazione di una firma sicura:
a. posseggano i requisiti legali di una firma in relazione ai dati in forma elettronica così come una firma autografa li possiede per dati cartacei; e
b. siano ammesse come prova in giudizio.
2. Gli Stati membri provvedono affinché una firma elettronica non sia considerata legalmente inefficace e inammissibile come prova in giudizio unicamente a causa del fatto che è
- in forma elettronica, o
- non basata su un certificato qualificato, o
- non basata su un certificato qualificato rilasciato da un prestatore di servizi di certificazione accreditato, ovvero
- non creata da un dispositivo per la creazione di una firma sicura.

Confrontiamo la norma europea con il DPR 445/2000 (Testo unico delle disposizioni legislative e regolamentari in materia di documentazione amministrativa, www.parlamento.it/leggi/deleghe/00443dla.htm) e con il DL 82/2005 (Codice dell'amministrazione digitale, www.camera.it/parlam/leggi/deleghe/testi/05082dl.htm):

DPR 445/2000, Art. 10 (R) Forma ed efficacia del documento informatico

1. Il documento informatico ha l'efficacia probatoria prevista dall'articolo 2712 del codice civile, riguardo ai fatti ed alle cose rappresentate.

2. Il documento informatico, sottoscritto con firma elettronica, soddisfa il requisito legale della forma scritta. Sul piano probatorio il documento stesso è liberamente valutabile, tenuto conto delle sue caratteristiche oggettive di qualità e sicurezza. Esso inoltre soddisfa l'obbligo previsto dagli articoli 2214 e seguenti del codice civile e da ogni altra analoga disposizione legislativa o regolamentare.

3. Il documento informatico, quando è sottoscritto con firma digitale o con un altro tipo di firma elettronica avanzata, e la firma è basata su di un certificato qualificato ed è generata mediante un dispositivo per la creazione di una firma sicura, fa inoltre piena prova, fino a querela di falso, della provenienza delle dichiarazioni da chi l'ha sottoscritto.

4. Al documento informatico, sottoscritto con firma elettronica, in ogni caso non può essere negata rilevanza giuridica né ammissibilità come mezzo di prova unicamente a causa del fatto che è sottoscritto in forma elettronica ovvero in quanto la firma non è basata su di un certificato qualificato oppure non è basata su di un certificato qualificato rilasciato da un certificatore accreditato o, infine, perché la firma non è stata apposta avvalendosi di un dispositivo per la creazione di una firma sicura.

5. Le disposizioni del presente articolo si applicano anche se la firma elettronica è basata su di un certificato qualificato rilasciato da un certificatore stabilito in uno Stato non facente parte dell'Unione europea, quando ricorre una delle seguenti condizioni:

a) il certificatore possiede i requisiti di cui alla direttiva 1999/93/CE del Parlamento europeo e del Consiglio, del 13 dicembre 1999, ed è accreditato in uno Stato membro;

b) il certificato qualificato è garantito da un certificatore stabilito nella Comunità europea, in possesso dei requisiti di cui alla medesima direttiva;

c) il certificato qualificato, o il certificatore, è riconosciuto in forza di un accordo bilaterale o multilaterale tra la Comunità e Paesi terzi o organizzazioni internazionali.

6. Gli obblighi fiscali relativi ai documenti informatici ed alla loro riproduzione su diversi tipi di supporto sono assolti secondo le modalità definite con decreto del Ministro dell'economia e delle finanze.

DL 82/2005
Art.24, Firma digitale

1. La firma digitale deve riferirsi in maniera univoca ad un solo soggetto ed al documento o all'insieme di documenti cui è apposta o associata.

2. L'apposizione di firma digitale integra e sostituisce l'apposizione di sigilli, punzoni, timbri, contrassegni e marchi di qualsiasi genere ad ogni fine previsto dalla normativa vigente.

3. Per la generazione della firma digitale deve adoperarsi un certificato qualificato che, al momento della sottoscrizione, non risulti scaduto di validità ovvero non risulti revocato o sospeso.

4. Attraverso il certificato qualificato si devono rilevare, secondo le regole tecniche stabilite ai sensi dell'articolo 71, la validità del certificato stesso, nonché gli elementi identificativi del titolare e del certificatore e gli eventuali limiti d'uso.

Art. 25. Firma autenticata

1. Si ha per riconosciuta, ai sensi dell'articolo 2703 del codice civile, la firma digitale o altro tipo di firma elettronica qualificata autenticata dal notaio o da altro pubblico ufficiale a ciò autorizzato.

2. L'autenticazione della firma digitale o di altro tipo di firma elettronica qualificata consiste nell'attestazione, da parte del pubblico ufficiale, che la firma è stata apposta in sua presenza dal titolare, previo accertamento della sua identità personale, della validità del certificato elettronico utilizzato e del fatto che il documento sottoscritto non è in contrasto con l'ordinamento giuridico.

3. L'apposizione della firma digitale o di altro tipo di firma elettronica qualificata da parte del pubblico ufficiale ha l'efficacia di cui all'articolo 24, comma 2.

4. Se al documento informatico autenticato deve essere allegato altro documento formato in originale su altro tipo di supporto, il pubblico ufficiale può allegare copia informatica autenticata dell'originale, secondo le disposizioni dell'articolo 23, comma 5.

Il principio europeo di non negare rilevanza giuridica a un documento informatico sottoscritto con firma elettro-

nica semplice o basata su un certificato non rilasciato da certificatore accreditato, recepito dal Testo unico, in Italia ha lasciato aperte varie interpretazioni sulla rilevanza giuridica e sul valore probatorio di tali firme: la prima prefigura l'assenza di prova legale del documento (con efficacia rimessa alla valutazione del giudice); una seconda equipara tale firma alla firma cartacea non riconosciuta (quindi il documento è disconoscibile); una terza nega rilevanza giuridica alla firma elettronica semplice, ritenendo giuridicamente rilevanti solo le firme avanzata, qualificata e digitale (in contrasto con la norma europea e il testo unico).

In sostanza, solo la firma digitale basata su un certificato qualificato ha i requisiti tecnici per essere è riconosciuta e non ripudiabile.

La firma elettronica basata su un certificato qualificato rilasciato da un certificatore residente in uno stato non facente parte dell'Unione europea è valida se ricorre una delle seguenti condizioni:

1. il certificatore possiede i requisiti di cui alla direttiva 99/93 CE ed è accreditato in uno stato membro;
2. il certificato qualificato è garantito da un certificatore residente nella Comunità europea e in possesso dei requisiti di cui alla 99/93;
3. il certificato qualificato o il certificatore è riconosciuto in virtù di un accordo bilaterale o multilaterale tra la Comunità e paesi terzi od organizzazioni internazionali.

Tra le applicazioni della firma digitale c'è anche l'archiviazione ottica dei documenti cartacei e informatici, in base all'art. 6 del DPR 445/2000 e alla delibera n.11 del 19/2/2004 (Regole tecniche per la riproduzione e conservazione di documenti su supporto ottico idoneo a garantire la conformità dei documenti agli originali, www.cnipa.gov.it/site/_contentfiles/01377100/1377105_DEL11_2004.pdf).

Tutela e trattamento dei dati personali

La direttiva 95/46 CE relativa alla tutela, al trattamento e alla libera circolazione dei dati personali (http://www.garanteprivacy.it/garante/document?ID=432175) ha determinato l'introduzione, nella legislazione dei paesi membri, di una serie di principi a tutela della riservatezza dei dati personali. Di conseguenza, la tutela della privacy è diventata un diritto fondamentale della persona, che ha facoltà di controllare come terzi (persone fisiche o giuridiche) conservano e trattano i dati personali che la riguardano.

La direttiva 95/46 CE è stata recepita dal decreto legislativo 196/2003 (Codice in materia di protezione dei dati personali, altrimenti detto Codice della privacy), aggiornato da una serie di provvedimenti (sono elencati quelli noti al 29 marzo 2006):

- legge 23 febbraio 2006, n.51 di conversione con modificazioni, del decreto-legge 30 dicembre 2005, n. 273
- legge 31 luglio 2005, n. 155, di conversione con modificazioni, del decreto-legge 27 luglio, n. 144
- legge 1° marzo 2005, n. 26, di conversione, con modificazioni, del decreto-legge 30 dicembre 2004, n. 314;
- legge 27 dicembre 2004, n. 306, di conversione del decreto-legge 9 novembre 2004, n. 266;
- legge 27 luglio 2004, n. 188, di conversione del decreto-legge 24 giugno 2004, n. 158;
- legge 26 maggio 2004, n. 138, di conversione, con modificazioni, del decreto-legge 29 marzo 2004, n. 81;
- legge 26 febbraio 2004, n. 45, di conversione, con modificazioni, del decreto-legge 24 dicembre 2003, n. 354;
- decreto legislativo 22 gennaio 2004, n. 42.

L'art. 4 del Codice della privacy definisce i dati personali. Un dato personale è qualunque informazione relativa a persona fisica, persona giuridica, ente od associazione, identificati o identificabili, anche indirettamente, mediante riferimento a qualsiasi altra informazione, ivi compreso un numero di identificazione personale.

I dati personali che richiedono particolare protezione sono detti dati sensibili e sono definiti come i dati personali idonei a rivelare l'origine razziale ed etnica, le convinzioni religiose, filosofiche o di altro genere, le opinioni politiche, l'adesione a partiti, sindacati, associazioni od organizzazioni a carattere religioso, filosofico, politico o sindacale, nonché i dati personali idonei a rivelare lo stato di salute e la vita sessuale.

Un altro concetto fondamentale è quello di trattamento, definito come qualunque operazione o complesso di operazioni, effettuati anche senza l'ausilio di strumenti elettronici, concernenti la raccolta, la registrazione, l'organizzazione, la conservazione, la consultazione, l'elaborazione, la modificazione, la selezione, l'estrazione, il raffronto, l'utilizzo, l'interconnessione, il blocco, la comunicazione, la diffusione, la cancellazione e la distruzione di dati, anche se non registrati in una banca di dati.

I soggetti principali previsti dalla normativa sulla privacy sono il titolare, il responsabile, l'incaricato del trattamento e l'interessato.

Il titolare è la persona fisica, la persona giuridica, la pubblica amministrazione e qualsiasi altro ente, associazione od organismo cui competono, anche unitamente ad altro titolare, le decisioni in ordine alle finalità, alle modalità del trattamento di dati personali e agli strumenti utilizzati, ivi compreso il profilo della sicurezza.

Il responsabile è la persona fisica, la persona giuridica, la pubblica amministrazione e qualsiasi altro ente, associazione od organismo preposti dal titolare al trattamento di dati personali.

Il titolare o il responsabile del trattamento devono nominare come incaricati le persone autorizzate a eseguire le operazioni di trattamento. Gli incaricati sono definiti come le persone fisiche autorizzate a compiere operazioni di trattamento dal titolare o dal responsabile.

E' infine definito come interessato la persona fisica, la persona giuridica, l'ente o l'associazione cui si riferiscono i dati personali.

La normativa a tutela della privacy si basa su alcuni principi fondamentali

Principio del buon trattamento

In base a questo principio (vedi art. 11), i dati personali oggetto del trattamento devono essere: trattati in modo lecito e secondo correttezza; raccolti e registrati per scopi determinati, espliciti e legittimi, e utilizzati in altre operazioni del trattamento in termini compatibili con tali scopi; esatti e, se necessario, aggiornati; pertinenti, completi e non eccedenti rispetto alle finalità per le quali sono raccolti o successivamente trattati; conservati in una forma che consenta l'identificazione dell'interessato per un periodo di tempo non superiore a quello necessario agli scopi per i quali essi sono stati raccolti o successivamente trattati.

Controllo amministrativo sul corretto trattamento di dati

Previsto dalla legge comunitaria e ripreso dalla normativa italiana, questo principio ha determinato la nascita di un'authority amministrativa (in Italia il Garante per la protezione dei dati personali) con compiti di vigilanza sul corretto trattamento dei dati personali da parte di privati e aziende.

Oltre ad avere il potere di prendere provvedimenti anche di tipo sanzionatorio in caso di violazioni, l'authority ha il compito di stendere regolamenti, codici disciplinari e policy di validità generale, di autorizzare particolari trattamenti di dati sensibili e di fissare i criteri e i limiti, anche attraverso

5.8.3.2: Conoscere la legge a tutela e trattamento dei dati personali (Direttiva Europea 95/46), e relative implicazioni

campagne di educazione e sensibilizzazione, entro i quali i trattamenti dei dati possono considerarsi leciti.

Obbligo informativo

In base a tale principio (vedi art. 13), chiunque esegua trattamenti di dati personali deve informare oralmente o per iscritto gli interessati circa: le finalità e le modalità del trattamento cui sono destinati i dati; la natura obbligatoria o facoltativa del conferimento dei dati; le conseguenze di un eventuale rifiuto di rispondere; i soggetti o le categorie di soggetti ai quali i dati personali possono essere comunicati o che possono venirne a conoscenza in qualità di responsabili o incaricati, e l'ambito di diffusione dei dati medesimi; i diritti di cui all'articolo 7; gli estremi identificativi del titolare e, se designati, del rappresentante nel territorio dello Stato ai sensi dell'articolo 5 e del responsabile. Le eccezioni all'obbligo dell'informativa sono assai limitate e previste dall'art. 13 (un esempio è quando i dati sono trattati in base a un obbligo previsto dalla legge, da un regolamento o dalla normativa comunitaria).

Principio del consenso

Salvo alcuni casi previsti, come un obbligo di legge o contrattuale, il titolare della raccolta e trattamento dei dati personali deve ottenere il consenso esplicito dell'interessato. Il consenso deve essere scritto qualora il trattamento riguardi dati sensibili.

Diritto alla riservatezza

Ai sensi dell'art. 7, l'interessato ha diritto di ottenere la conferma dell'esistenza o meno di dati personali che lo riguardano, anche se non ancora registrati, e la loro comunicazione in forma intelligibile.

In particolare, l'interessato ha il diritto di ottenere l'indicazione: dell'origine dei dati personali; delle finalità e modalità del trattamento; della logica applicata in caso di trattamento effettuato con l'ausilio di strumenti elettronici; degli estremi identificativi del titolare, dei responsabili e del rappresentante designato ai sensi dell'articolo 5, comma 2; dei soggetti o delle categorie di soggetti ai quali i dati personali possono essere comunicati o che possono venirne a conoscenza in qualità di rappresentante designato nel territorio dello Stato, di responsabili o incaricati.

L'interessato ha inoltre diritto di ottenere: l'aggiornamento, la rettificazione ovvero, quando vi ha interesse, l'integrazione dei dati; la cancellazione, la trasformazione in forma anonima o il blocco dei dati trattati in violazione di legge, compresi quelli di cui non è necessaria la conservazione in relazione agli scopi per i quali i dati sono stati raccolti o successivamente trattati; l'attestazione che le operazioni di cui alle lettere a) e b) sono state portate a conoscenza, anche per quanto riguarda il loro contenuto, di coloro ai quali i dati sono stati comunicati o diffusi, eccettuato il caso in cui tale adempimento si rivela impossibile o comporta un impiego di mezzi manifestamente sproporzionato rispetto al diritto tutelato.

Infine, l'interessato ha diritto di opporsi, in tutto o in parte: per motivi legittimi al trattamento dei dati personali che lo riguardano, ancorché pertinenti allo scopo della raccolta; al trattamento di dati personali che lo riguardano a fini di invio di materiale pubblicitario o di vendita diretta o per il compimento di ricerche di mercato o di comunicazione commerciale.

Circolazione limitata dei dati

Introdotto nella legislazione comunitaria e ripreso dalla normativa italiana, questo principio ispira gli articoli sulla circolazione delle informazioni. I dati personali, salvo alcune precise eccezioni, non possono essere comunicati a terzi né tantomeno diffusi ad ampio raggio senza il consenso dell'interessato. I dati sensibili e giudiziari in nessun caso possono essere diffusi.

Mentre la circolazione dei dati all'interno dell'Unione europea non deve essere ostacolata dalle normative in materia di dati personali (vedi art. 42), la circolazione dei dati al di fuori dell'Unione è consentita solo nei casi previsti dagli artt. 43 e 44 del codice della privacy. Negli artt. 25 e 26 della direttiva 95/46 CE, la Commissione europea ha vietato il trasferimento dei dati personali verso paesi che non assicurano un livello adeguato di tutela dei dati personali.

Sicurezza

I dati personali devono essere protetti da misure di sicurezza allo scopo di garantirne la riservatezza, l'integrità e la disponibilità. Si veda la sezione 5.8.2.2 circa le misure minime di sicurezza imposte dal codice della privacy.

A tutela dei cittadini e delle aziende interessati al trattamento dei dati che li riguardano, il codice della privacy prevede sanzioni sia in sede amministrativa (in particolare in caso di omessa o inidonea informativa all'interessato, omessa o incompleta notificazione, omessa informazione o esibizione al Garante), sia in sede penale (in particolare in caso di trattamento illecito di dati, falsità nelle dichiarazioni e notificazioni al Garante, mancata applicazione delle misure di sicurezza, inosservanza di provvedimenti del garante).

In caso di violazione, è ipotizzabile un risarcimento del danno in base all'art. 2050 del Codice civile, che prevede la responsabilità per le attività pericolose e al quale si applica il ribaltamento dell'onere della prova: è la società responsabile del trattamento dei dati che deve provare di aver posto in essere tutte le misure e precauzioni idonee atte a evitare il danno.

5.8.3.3: Conoscere gli aspetti legali generali relativi all'evidenza di reato e alle perizie informatiche giudiziarie (Computer Forensics)

Informatica forense

Man mano che le informazioni hanno acquisito crescente importanza per le aziende, fino a superare in alcuni settori il valore dei beni materiali, gli attacchi alla loro sicurezza (integrità, riservatezza, disponibilità) si sono moltiplicati. Ne è derivata una duplice esigenza: proteggere le informazioni da danni e abusi causati sia dall'interno sia dall'esterno dell'organizzazione e dotarsi degli strumenti e procedure che consentano di identificare i responsabili di tali atti e di documentarne le azioni con efficacia probatoria.

La legge 397/2000 (Disposizioni in materia di indagini difensive) ha introdotto nel Codice di procedura penale le nuove disposizioni in materia di indagini difensive, con l'obiettivo di parificare l'attività difensiva all'attività investigativa dell'autorità giudiziaria (in particolare del Pubblico Ministero), dando ad esse uguale valore probatorio in sede processuale. Sono state inoltre definite le modalità con cui i difensori possono procedere alla raccolta delle prove.

L'art. 391-nonies (Attività investigativa preventiva), inserito nel Codice di procedura penale dalla legge 397/2000, stabilisce che l'attività investigativa prevista dall'articolo 327-bis, con esclusione degli atti che richiedono l'autorizzazione o l'intervento dell'autorità giudiziaria, può essere svolta anche dal difensore che ha ricevuto apposito mandato per l'eventualità che s'instauri un procedimento penale.

L'art. 327-bis. (Attività investigativa del difensore), anch'esso introdotto dalla 397/2000, stabilisce che:

1. Fin dal momento dell'incarico professionale, risultante da atto scritto, il difensore ha facoltà di svolgere investigazioni per ricercare ed individuare elementi di prova a favore del proprio assistito, nelle forme e per le finalità stabilite nel titolo VI-bis del Codice di procedura penale.

2. La facoltà indicata al punto 1 può essere attribuita per l'esercizio del diritto di difesa, in ogni stato e grado del pro-

cedimento, nell'esecuzione penale e per promuovere il giudizio di revisione.

3. Le attività previste dal punto 1 possono essere svolte, su incarico del difensore, dal sostituto, da investigatori privati autorizzati e, quando sono necessarie specifiche competenze, da consulenti tecnici.

Quanto detto significa che anche un soggetto che si ritiene offeso da un reato può affidare un mandato a un difensore per compiere indagini al fine di accertare la sussistenza delle prove necessarie e per decidere se presentare una successiva denuncia o querela all'autorità giudiziaria. D'altra parte, l'autorità giudiziaria e i difensori sono spesso impreparati ad affrontare le problematiche connesse con tecnologie in continua e rapida evoluzione, quali sono i mezzi di ricerca della prova informatica.

Sebbene siano in corso iniziative, come il progetto europeo AEEC (Admissibility of Electronic Evidence in Court) del 2005 sull'ammissibilità della prova elettronica, manca ancora un protocollo che definisca regole certe in base al quale i pubblici ministeri e i difensori possano procedere all'individuazione, analisi e presentazione dei dati in forma digitale, secondo modalità idonee a garantire che le informazioni raccolte siano accettate come prove in sede processuale.

Dato che nei moderni sistemi è difficile cancellare dati elettronici senza lasciare qualche traccia, dall'analisi di tali tracce (per esempio il file system, i file di log dei sistemi operativi e delle applicazioni e il registro di sistema di Windows), oltre che dei file, è spesso possibile ottenere informazioni importanti per provare la colpevolezza del responsabile di un reato informatico. Ciò è possibile a condizione che i dati siano raccolti e conservati in modalità adeguate per il loro utilizzo processuale e che sia rispettata una serie di requisiti riguardanti l'ambiente, il consulente tecnico (competenza, certificazioni, testimoni, presenza, capacità di sostenere il contraddittorio), le procedure, gli strumenti, la metodologia, la sicurezza, la ripetibilità, la presentazione e altro.

L'informatica forense (computer forensics) è la disciplina che si occupa della preservazione, dell'identificazione, dell'analisi e della documentazione dei computer o dei sistemi informativi al fine di evidenziare l'esistenza di prove nell'attività investigativa.

Dal punto di vista procedurale, l'obiettivo principale dell'informatica forense è la creazione di un protocollo di regole da seguire per le ricerca della prova informatica e relativa acquisizione e conservazione al fine di garantire che i risultati delle indagini abbiano valore anche in sede processuale.

Di fronte all'incompetenza tecnica dei giudici e alle obiezioni e all'aggressività oratoria degli accusatori e dei difensori, intenzionati a sminuire, invalidare o screditare le prove altrui, i relativi metodi e le condizioni di raccolta e conservazione, nonché le qualifiche del consulente tecnico di parte opposta, è facile comprendere che non bastano dei dati trovati su un hard disk per ottenere dal giudice la loro ammissione come prova a carico o a discarico.

Le attività di informatica forense possono riguardare diverse aree, tra cui le seguenti:

1. monitoraggio e analisi dei supporti di memorizzazione e delle periferiche;
2. visualizzazione di banche dati;
3. esame di immagini e sequenze audio e video;
4. monitoraggio e controllo delle attività svolte su reti interne ed esterne, inclusa Internet.

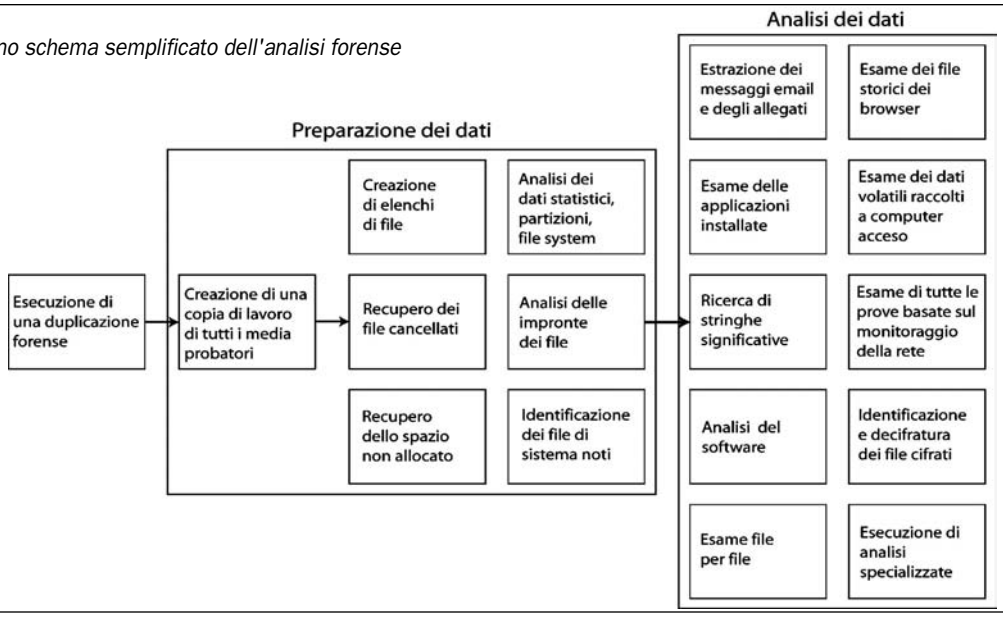
Tra i requisiti fondamentali di una prova informatica, affinché possa essere accettata in sede processuale, ci sono autenticità, pertinenza, accuratezza, completezza, integrità e non ripudiabilità. Inoltre, deve essere raccolta, documentata e presentata in modo convincente per essere ritenuta ammissibile e giuridicamente valida da un giudice che, non tecnicamente esperto, ha formato criteri più o meno soggettivi di accettabilità, a volte basati sull'uso di protocolli e strumenti usati di frequente in un certo ambito.

Alla base della procedura di analisi forense c'è una corretta procedura di raccolta e conservazione dei dati e l'utilizzo di strumenti di analisi che generino risultati riproducibili senza che vi sia alcuna alterazione dei supporti originali.

Nei casi di acquisizione delle prove su sistemi accesi (live response), quando le prove includono dati volatili che sarebbero perduti spegnendo il sistema, per prima cosa si provvede al loro salvataggio. Fanno parte di tale categoria i dati in memoria riguardanti gli utenti correnti, i processi e le applicazioni aperte e i relativi dati e le sessioni di comunicazione, inclusi i socket aperti. Si tenga anche conto che possono essere attive applicazioni o servizi che ripuliscono il sistema alla fine di una sessione del sistema operativo. Se necessario, può essere eseguito un esame in profondità sul sistema acceso, altrimenti si può eseguire un esame iniziale dei dati volatili e quindi la duplicazione dei media in un diverso ambiente di sistema, che non alteri i media stessi.

Come regola generale, le analisi non vengono effettuate

Uno schema semplificato dell'analisi forense



sui supporti originali sequestrati, ma su immagini degli hard disk perfettamente identiche catturate byte per byte (dette anche bitstream image) senza alterazione dell'originale. Per ogni immagine così registrata, possibilmente in presenza di testimoni, viene subito calcolata un'impronta informatica (hash) in modo che successivamente sia garantita l'integrità delle informazioni raccolte, che in tal modo non sono ripudiabili dalle parti interessate. Se occorre, può anche essere applicata una firma digitale per garantire che nessuno alteri l'hash. Il concetto di raccogliere prove non ripudiabili e di custodirle integre e al sicuro fino al processo si chiama Chain of Custody (catena della custodia). La custodia in maniera corretta (a prova di manomissione) delle prove e dei dati acquisiti è vitale al fine di evitare che il lavoro di indagine sia invalidato per un cavillo legale. Lavorando con prove pressoché immateriali, è facile distruggere una prova determinante con un semplice passo falso. Il lavoro inoltre può essere ostacolato dalle operazioni eseguite da utenti o amministratori di sistema prima del sopraluogo, che possono pregiudicare l'indagine.

Nella prassi giudiziaria, finché non verranno standardizzate e uniformate le regole per l'acquisizione delle prove informatiche, la pubblica accusa ritiene spesso attendibili anche prove mancanti dei requisiti citati, come le stampe di documenti (pagine Internet, messaggi e-mail, sessioni di chat e così via) e supporti di memorizzazione privi di sigillo o garanzia elettronica di intergità.

In base al principio del libero convincimento del giudice, anche gli organi giudicanti ritengono spesso attendibili tali prove. D'altra parte, una recente sentenza della Cassazione ha negato il valore di prova alla stampa di una pagina web perché priva di una garanzia di rispondenza all'originale e di un riferimento temporale.

Per tutte queste ragioni, è necessario che anche le imprese si dotino degli strumenti tecnologici e organizzativi necessari per monitorare (nel rispetto della privacy e dello Statuto dei lavoratori) le operazioni informatiche e riconoscere gli indicatori di un possibile reato mentre viene commesso. In tal modo, si possono raccogliere prove valide da utilizzare in sede processuale ad uso sia del Pubblico Ministero sia dei difensori. Tali attività richiedono l'intervento di personale interno, o di consulenti esterni, con adeguate competenze tecnologiche, organizzative e giuridiche (inclusa la familiarità con le pratiche accettate dal tribunale locale), in costante aggiornamento professionale e in contatto, anche attraverso i forum, con i colleghi della comunità informatica forense.

I motori di ricerca e le librerie online sono una ricca fonte di riferimenti sulle procedure, gli strumenti e le normative per l'informatica forense (computer forensics).

Esistono numerosi strumenti per la duplicazione e il ripristino dei dati, a partire dalle utility dd e dcfldd dei sistemi operativi di derivazione Unix. Oltre ai comandi di sistema, esistono utility Open Source come ODD (Open Data Duplicator), che fa parte dell'architettura Open Digital Evidence Search and Seizure Architecture (ODESSA). Esiste poi una serie di applicazioni commerciali, talvolta molto costose, come EnCase Forensics di Guidance Software, uno degli strumenti più utilizzati da organizzazioni governative e forze dell'ordine a livello internazionale (www.guidancesoftware.com).

Se da un lato non esistono ostacoli tecnici a utilizzare strumenti Open Source o a identificare procedure e strumenti al di fuori degli schemi abituali per la raccolta delle prove, in realtà c'è il rischio di non vedere ammesse le prove raccolte perché la procedura è incomprensibile al giudice o è demolita dalla controparte durante il processo.

Ciò premesso, un ambiente di sistema progettato appositamente per la raccolta di prove informatiche è Helix, una versione di Linux basata sulla distribuzione Knoppix Live CD (avviata da CD senza installare nulla su hard disk) che include molte applicazioni dedicate alla diagnosi dei problemi e alla raccolta di informazioni per uso forense (www.e-fense.com/helix/).

Tra gli strumenti in grado di recuperare i contenuti di un hard disk, anche nascosti o rovinati, citiamo R-Studio di R-Tools Technology (www.r-tt.com), che produce diverse applicazioni per il recupero e il ripristino dei dati.

Tra la abbondante letteratura sull'informatica forense, citiamo i seguenti testi e URL di riferimento:

"Incident Response and Computer Forensics", Seconda Edizione, K. Mandia e C. Prosise, McGraw-Hill/Osborne 2003
"File System Forensic Analysis", B. Carrier, Addison-Wesley Professional, 2005
"Real Digital Forensics: Computer Security and Incident Response", Jones, Bejtlich e Rose, Addison-Wesley Professional, 2005
"Digital Evidence and Computer Crime", Seconda Edizione, E. Casey, Academic Press, 2004
The Sleuth Kit (TSK), www.sleuthkit.org/sleuthkit/index.php
Forensic Tools, www.networkintrusion.co.uk/fortools.htm
Anti-Forensic Tools, www.networkintrusion.co.uk/foranti.htm
Open Source Digital Forensics, www.opensourceforensics.org/index.html
Computer Forensics, Cybercrime and Steganography Resources, www.forensics.nl
Documenti e libri di informatica forense, www.digitalevidence.org/papers/index.html
Forensic Focus, www.forensicfocus.com/computer-forensics-forums ■

ALLEGATO B

DISCIPLINARE TECNICO IN MATERIA DI MISURE MINIME DI SICUREZZA

(Artt. da 33 a 36 del codice)
Trattamenti con strumenti elettronici
Modalità tecniche da adottare a cura del titolare, del responsabile ove designato e dell'incaricato, in caso di trattamento con strumenti elettronici:
Sistema di autenticazione informatica
1. Il trattamento di dati personali con strumenti elettronici è consentito agli incaricati dotati di credenziali di autenticazione che consentano il superamento di una procedura di autenticazione relativa a uno specifico trattamento o a un insieme di trattamenti.
2. Le credenziali di autenticazione consistono in un codice per l'identificazione dell'incaricato associato a una parola chiave riservata conosciuta solamente dal medesimo oppure in un dispositivo di autenticazione in possesso e uso esclusivo dell'incaricato, eventualmente associato a un codice identificativo o a una parola chiave, oppure in una caratteristica biometrica dell'incaricato, eventualmente associata a un codice identificativo o a una parola chiave.
3. Ad ogni incaricato sono assegnate o associate individualmente una o più credenziali per l'autenticazione.
4. Con le istruzioni impartite agli incaricati è prescritto di adottare le necessarie cautele per assicurare la segretezza della componente riservata della credenziale e la diligente custodia dei dispositivi in possesso ed uso esclusivo

dell'incaricato.
5. La parola chiave, quando è prevista dal sistema di autenticazione, è composta da almeno otto caratteri oppure, nel caso in cui lo strumento elettronico non lo permetta, da un numero di caratteri pari al massimo consentito; essa non contiene riferimenti agevolmente riconducibili all'incaricato ed è modificata da quest'ultimo al primo utilizzo e, successivamente, almeno ogni sei mesi. In caso di trattamento di dati sensibili e di dati giudiziari la parola chiave è modificata almeno ogni tre mesi.
6. Il codice per l'identificazione, laddove utilizzato, non può essere assegnato ad altri incaricati, neppure in tempi diversi.
7. Le credenziali di autenticazione non utilizzate da almeno sei mesi sono disattivate, salvo quelle preventivamente autorizzate per soli scopi di gestione tecnica.
8. Le credenziali sono disattivate anche in caso di perdita della qualità che consente all'incaricato l'accesso ai dati personali.
9. Sono impartite istruzioni agli incaricati per non lasciare incustodito e accessibile lo strumento elettronico durante una sessione di trattamento.
10. Quando l'accesso ai dati e agli strumenti elettronici è consentito esclusivamente mediante uso della componente riservata della credenziale per l'autenticazione, sono impartite idonee e preventive disposizioni scritte volte a individuare chiaramente le modalità con le quali il titolare può assicurare la disponibilità di dati o strumenti elettronici in caso di prolungata assenza o impedimento dell'incaricato che renda indispensabile e indifferibile intervenire per esclusive necessità di operatività e di sicurezza del sistema. In tal caso la custodia delle copie delle credenziali è organizzata garantendo la relativa segretezza e individuando preventivamente per iscritto i soggetti incaricati della loro custodia, i quali devono informare tempestivamente l'incaricato dell'intervento effettuato.
11. Le disposizioni sul sistema di autenticazione di cui ai precedenti punti e quelle sul sistema di autorizzazione non si applicano ai trattamenti dei dati personali destinati alla diffusione.
Sistema di autorizzazione
12. Quando per gli incaricati sono individuati profili di autorizzazione di ambito diverso è utilizzato un sistema di autorizzazione.
13. I profili di autorizzazione, per ciascun incaricato o per classi omogenee di incaricati, sono individuati e configurati anteriormente all'inizio del trattamento, in modo da limitare l'accesso ai soli dati necessari per effettuare le operazioni di trattamento.
14. Periodicamente, e comunque almeno annualmente, è verificata la sussistenza delle condizioni per la conservazione dei profili di autorizzazione.
Altre misure di sicurezza
15. Nell'ambito dell'aggiornamento periodico con cadenza almeno annuale dell'individuazione dell'ambito del trattamento consentito ai singoli incaricati e addetti alla gestione o alla manutenzione degli strumenti elettronici, la lista degli incaricati può essere redatta anche per classi omogenee di incarico e dei relativi profili di autorizzazione.
16. I dati personali sono protetti contro il rischio di intrusione e dell'azione di programmi di cui all'art. 615-quinquies del codice penale, mediante l'attivazione di idonei strumenti elettronici da aggiornare con cadenza almeno semestrale.
17. Gli aggiornamenti periodici dei programmi per elaboratore volti a prevenire la vulnerabilità di strumenti elettronici e a correggerne difetti sono effettuati almeno annualmente. In caso di trattamento di dati sensibili o giudiziari l'aggiornamento è almeno semestrale.
18. Sono impartite istruzioni organizzative e tecniche che prevedono il salvataggio dei dati con frequenza almeno settimanale.
Documento programmatico sulla sicurezza
19. Entro il 31 marzo di ogni anno, il titolare di un trattamento di dati sensibili o di dati giudiziari redige anche attraverso il responsabile, se designato, un documento programmatico sulla sicurezza contenente idonee informazioni riguardo:
19.1. l'elenco dei trattamenti di dati personali;
19.2. la distribuzione dei compiti e delle responsabilità nell'ambito delle strutture preposte al trattamento dei dati;
19.3. l'analisi dei rischi che incombono sui dati;
19.4. le misure da adottare per garantire l'integrità e la disponibilità dei dati, nonché la protezione delle aree e dei locali, rilevanti ai fini della loro custodia e accessibilità;
19.5. la descrizione dei criteri e delle modalità per il ripristino della disponibilità dei dati in seguito a distruzione o danneggiamento di cui al successivo punto 23;
19.6. la previsione di interventi formativi degli incaricati del trattamento, per renderli edotti dei rischi che incombono sui dati, delle misure disponibili per prevenire eventi dannosi, dei profili della disciplina sulla protezione dei dati personali più rilevanti in rapporto alle relative attività, delle responsabilità che ne derivano e delle modalità per aggiornarsi sulle misure minime adottate dal titolare. La formazione è programmata già al momento dell'ingresso in servizio, nonché in occasione di cambiamenti di mansioni, o di introduzione di nuovi significativi strumenti, rilevanti rispetto al trattamento di dati personali;
19.7. la descrizione dei criteri da adottare per garantire l'adozione delle misure minime di sicurezza in caso di trattamenti di dati personali affidati, in conformità al codice, all'esterno della struttura del titolare;
19.8. per i dati personali idonei a rivelare lo stato di salute e la vita sessuale di cui al punto 24, l'individuazione dei criteri da adottare per la cifratura o per la separazione di tali dati dagli altri dati personali dell'interessato.
Ulteriori misure in caso di trattamento di dati sensibili o giudiziari
20. I dati sensibili o giudiziari sono protetti contro l'accesso abusivo, di cui all' art. 615-ter del codice penale, mediante l'utilizzo di idonei strumenti elettronici.
21. Sono impartite istruzioni organizzative e tecniche per la custodia e l'uso dei supporti rimovibili su cui sono memorizzati i dati al fine di evitare accessi non autorizzati e trattamenti non consentiti.
22. I supporti rimovibili contenenti dati sensibili o giudiziari se non utilizzati sono distrutti o resi inutilizzabili, ovvero possono essere riutilizzati da altri incaricati, non autorizzati al trattamento degli stessi dati, se le informazioni precedentemente in essi contenute non sono intelligibili e tecnicamente in alcun modo ricostruibili.
23. Sono adottate idonee misure per garantire il ripristino dell'accesso ai dati in caso di danneggiamento degli stessi o degli strumenti elettronici, in tempi certi compatibili con i diritti degli interessati e non superiori a sette giorni.
24. Gli organismi sanitari e gli esercenti le professioni sanitarie effettuano il trattamento dei dati idonei a rivelare lo stato di salute e la vita sessuale contenuti in elenchi, registri o banche di dati con le modalità di cui all'articolo 22, comma 6, del codice, anche al fine di consentire il trattamento disgiunto dei medesimi dati dagli altri dati personali che permettono di identificare direttamente gli interessati. I dati relativi all'identità genetica sono trattati esclusivamente all'interno di locali protetti accessibili ai soli incaricati dei trattamenti ed ai soggetti specificatamente autorizzati ad accedervi; il trasporto dei dati all'esterno dei locali riservati al loro trattamento deve avvenire in contenitori muniti di serratura o dispositivi equipollenti; il trasferimento dei dati in formato elettronico è cifrato.
Misure di tutela e garanzia

25. Il titolare che adotta misure minime di sicurezza avvalendosi di soggetti esterni alla propria struttura, per provvedere alla esecuzione riceve dall'installatore una descrizione scritta dell'intervento effettuato che ne attesta la conformità alle disposizioni del presente disciplinare tecnico.
26. Il titolare riferisce, nella relazione accompagnatoria del bilancio d'esercizio, se dovuta, dell'avvenuta redazione o aggiornamento del documento programmatico sulla sicurezza.
Trattamenti senza l'ausilio di strumenti elettronici
Modalità tecniche da adottare a cura del titolare, del responsabile, ove designato, e dell'incaricato, in caso di trattamento con strumenti diversi da quelli elettronici:
27. Agli incaricati sono impartite istruzioni scritte finalizzate al controllo ed alla custodia, per l'intero ciclo necessario allo svolgimento delle operazioni di trattamento, degli atti e dei documenti contenenti dati personali. Nell'ambito dell'aggiornamento periodico con cadenza almeno annuale dell'individuazione dell'ambito del trattamento consentito ai singoli incaricati, la lista degli incaricati può essere redatta anche per classi omogenee di incarico e dei relativi profili di autorizzazione.
28. Quando gli atti e i documenti contenenti dati personali sensibili o giudiziari sono affidati agli incaricati del trattamento per lo svolgimento dei relativi compiti, i medesimi atti e documenti sono controllati e custoditi dagli incaricati fino alla restituzione in maniera che ad essi non accedano persone prive di autorizzazione, e sono restituiti al termine delle operazioni affidate.
29. L'accesso agli archivi contenenti dati sensibili o giudiziari è controllato. Le persone ammesse, a qualunque titolo, dopo l'orario di chiusura, sono identificate e registrate.
Quando gli archivi non sono dotati di strumenti elettronici per il controllo degli accessi o di incaricati della vigilanza, le persone che vi accedono sono preventivamente autorizzate.

GLOSSARIO

3DES (Triple DES)
tripla applicazione del DES. L'algoritmo alla base di 3DES è lo stesso di DES, l'algoritmo più studiato e collaudato di tutti i tempi. 3DES è molto robusto e affidabile, ma è stato progettato circa 30 anni fa ed è stato concepito per l'implementazione in hardware.

Accountability
Vedi rendicontabilità.

Accuratezza
tutte le funzioni intese a garantire l'accuratezza delle informazioni.

AES
pubblicato dal NIST nel 2001, è l'algoritmo richiesto per proteggere le informazioni riservate, ma non classificate, del governo statunitense. Nel 2003 il governo USA ha autorizzato l'uso di AES per la cifratura di documenti classificati fino al livello di secret con chiave di 128 bit e di top secret con chiave di 192 o 256 bit. E' previsto che risulti sicuro per decenni a venire ed è utilizzabile senza il pagamento di royalty.

Affidabilità del servizio
una vasta categoria di contromisure, perché sono diverse le aree che potrebbero compromettere l'affidabilità dei servizi informatici.

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

AH (Authentication Header)
uno dei protocolli della famiglia IPSec. Fornisce la prova di origine dei pacchetti ricevuti, l'integrità dei dati e la protezione da replay.

Algoritmo (o cifrario)
un insieme di regole logiche e matematiche usate nella cifratura e nella decifratura.

Analisi dei protocolli
uno dei tre metodi usati dagli IDS per riconoscere segni d'intrusione. Meno specifico del pattern matching, esamina il pattern (la struttura) del traffico, anziché il campo dati dei pacchetti. Sono verificati gli header e la loro coerenza con la struttura dei pacchetti.

Analisi del rischio
si classificano le informazioni e le risorse soggette a minacce e vulnerabilità e si identifica il livello di rischio associato a ogni minaccia.

Autenticità
garantisce che eventi, documenti e messaggi vengano attribuiti con certezza al legittimo autore e a nessun altro.

Bene
un bene è qualsiasi cosa, materiale o immateriale, che abbia un valore e debba quindi essere protetta.

Blowfish
Blowfish è un cifrario simmetrico a blocchi di 64 bit con chiavi di lunghezza fino a 448 bit. Durante la cifratura i dati sono sottoposti a 16 fasi di funzioni crittografiche. Blowfish è un algoritmo molto robusto ed è stato scritto da Bruce Schneier, uno degli autori più citati nel campo della crittografia.

BS 7799
Le linee guida BS 7799, oggi ISO/IEC 17799 e BS 7799-2, hanno una storia che risale agli inizi degli anni '90, quando il Dipartment of Trade and Industry britannico istituì un gruppo di lavoro con l'intento di fornire alle aziende linee guida per la gestione della sicurezza delle informazioni. Nel 1993 questo gruppo pubblicò il Code of practice for information security management, un insieme di buone regole di comportamento per la sicurezza delle informazioni.

Business Continuity
(talvolta chiamata business continuance) descrive i processi e le procedure che un'organizzazione mette in atto per assicurare che le funzioni essenziali rimangano operative durante e dopo un disastro.

Busta elettronica
una busta elettronica (digital envelope) consiste di un messaggio che usa la cifratura simmetrica a chiave segreta e una chiave segreta cifrata in modo asimmetrico. Qualunque messaggio formattato con CMS può essere incapsulato dentro un altro messaggio CMS, applicando ricorsivamente la busta elettronica. Ciò permette agli utenti di firmare una busta digitale, di cifrare una firma digitale o di eseguire varie altre funzioni.

CBC (Cipher Block Chaining)
uno dei principali cifrari a blocchi. Utilizza il blocco di testo cifrato precedente e lo combina in XOR (OR esclusivo, un'operazione tra due bit che produce come risultato 1 se i bit sono diversi o 0 se sono uguali) con il blocco successivo di testo in chiaro prima della cifratura. Il primo blocco è combinato in XOR con un Vettore di Inizializzazione (IV, Initialization Vector), scelto con forti proprietà di pseudocasualità in modo che testi diversi producano lo stesso testo cifrato.
La decifratura funziona nel modo opposto: ogni blocco è decifrato e combinato in XOR con il blocco precedente. Il primo blocco è decifrato e combinato in XOR con il vettore d'inizializzazione.

CEN (Comitato Europeo di Normalizzazione, www.cenorm.org)
un organismo europeo composto dagli enti di standardizzazione dei paesi membri dell'Unione Europea e dell'EFTA (European Fair Trade Association - tra cui l'UNI per l'Italia).

CERT (Computer Emergency Response Team)
(squadra di intervento per le emergenze informatiche) ha la missione di operare con la comunità di Internet per facilitare la risposta agli eventi riguardanti la sicurezza degli host (i computer collegati a Internet), prendere iniziative per sensibilizzare la comunità sugli aspetti della sicurezza e condurre ricerche rivolte a incrementare la sicurezza dei sistemi esistenti.

CERT-CC
il primo CERT (www.cert.org) è diventato il CERT Coordination Center (CERT-CC) ed è situato presso il Software Engineering Institute, finanziato dal governo USA e gestito dalla Carnegie Mellon University di Pittsburg. Si focalizza sulle violazioni alla sicurezza, allerta sulle nuove minacce, reagisce agli attacchi (i cosiddetti incidents) e fornisce assistenza, informazioni sulla vulnerabilità dei prodotti e istruzione con documenti e tutorial.

certificate repository
è il database dove la CA pubblica i certificati che genera, che può essere utilizzato come fonte centrale dei certificati e delle chiavi pubbliche dagli utenti della PKI. Esso può inoltre essere usato come ubicazione centrale delle CRL.

Certification Authority (CA)
la CA garantisce le chiavi pubbliche delle entità del proprio dominio mediante l'emissione dei "certificati digitali" in formato standard, contenenti: 1) una serie d'informazioni, tra cui il nome del titolare del certificato, la sua chiave pubblica, il periodo di validità del certificato e altre informazioni che concorrono a identificare il titolare e l'autorità che emette il certificato; 2) la firma digitale, apposta alle suddette informazioni utilizzando la chiave privata della CA.

certificato
è una struttura di dati che associa l'identità del titolare alla coppia di chiavi (la chiave pubblica è inclusa nel certificato), certificata tramite una firma digitale prodotta

per mezzo della chiave privata della CA. Detto anche certificato digitale e certificato a chiave pubblica.

Chiave
la sequenza segreta di bit che governa l'atto della cifratura o della decifratura.

Chiave privata
una delle due chiavi usate nella crittografia asimmetrica. E' segreta e viene mantenuta in possesso del solo proprietario.

Chiave pubblica
una delle due chiavi usate nella crittografia asimmetrica. E' pubblicamente disponibile a chiunque voglia comunicare con il suo proprietario.

Chiave segreta
la chiave usata nella crittografia simmetrica e comune sia al mittente sia al destinatario. Deve essere mantenuta segreta perché la sua conoscenza consente di decifrare qualsiasi messaggio cifrato alla fonte.

Cifrare o cifratura
l'azione di trasformare i dati in formato illeggibile.

Cifrario a blocchi
opera sui dati un blocco alla volta (le dimensioni tipiche dei blocchi sono di 64 o 128 bit) e ogni operazione su un blocco è un'azione elementare.

Cifrario a flusso
opera invece un bit o un byte alla volta; una volta inizializzati con una chiave, producono un flusso di bit e si prestano alla cifratura di grandi quantità di dati.

CMS (Cryptographic Message Syntax)
il formato con cui sono codificati i messaggi creati con la cifratura asimmetrica è definito dallo standard PKCS #7

Cryptographic Message Syntax (CMS).
Altre proprietà del formato CMS sono: 1) gestisce la firma congiunta di più firmatari, 2) gestisce la firma per un numero arbitrario di destinatari, 3) consente di aggiungere attributi firmati al messaggio, come la data e l'ora della firma, 4) consente di allegare al messaggio i certificati dei firmatari, agevolando la verifica della firma, 5) include gli identificatori degli algoritmi crittografici utilizzati e gli elementi che facilitano la decifratura e la verifica della firma.

Common Criteria
criteri standard di valutazione di applicabilità globale che allinea i criteri di valutazione esistenti ed emergenti: TCSEC, ITSEC, il canadese CTCPEC (Canadian Trusted Computer Product Evaluation Criteria) e i criteri federali USA. Il progetto è stato sviluppato attraverso la collaborazione degli enti nazionali di standardizzazione di Stati Uniti, Canada, Francia, Germania, Regno Unito e Olanda. I benefici di questo sforzo comune comprendono la riduzione della complessità del sistema di valutazione, la disponibilità di un unico linguaggio per le definizioni e per i livelli di sicurezza e, a beneficio dei produttori, l'uso di un unico insieme di requisiti per vendere i prodotti sul mercato internazionale.

Controllo degli accessi
le funzioni di sicurezza che verificano se il processo o l'utente, di cui è stata autenticata l'identità, ha il diritto di accedere alla risorsa richiesta.

Controllo del rischio
vengono individuate le modalità che l'azienda intende adottare per ridurre i rischi associati alla perdita della disponibilità di informazioni e risorse informatiche e della integrità e riservatezza di dati e informazioni.

Contromisure
le contromisure di sicurezza sono le realizzazioni e le azioni volte ad annullare o limitare le vulnerabilità e a contrastare le minacce.

Contromisure di carattere fisico
Queste contromisure sono generalmente legate alla prevenzione e al controllo dell'accesso a installazioni, locali, attrezzature, mezzi di comunicazione.

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

Contromisure di tipo tecnico informatico
sono le contromisure realizzate attraverso mezzi hardware, firmware e software e prendono anche il nome di funzioni di sicurezza.

Correttezza
è un attributo intrinseco di un prodotto (o componente o procedura), che riflette il grado di corrispondenza tra le effettive funzioni svolte dal prodotto e le sue specifiche.

Criteri di valutazione della garanzia
sono i metodi con cui viene valutata la fiducia che può essere accordata ai sistemi e ai prodotti informatici di sicurezza. Tra le pubblicazioni disponibili, le tre più significative sono i criteri americani TCSEC (Trusted Computing Security Evaluation Criteria, 1985), i criteri europei ITSEC (Information Security Evaluation Criteria, 1991) e i criteri internazionali ISO/IEC 15408, noti come Common Criteria e pubblicati nel 1999.

Crittoanalisi
la pratica di ottenere il messaggio in chiaro dal messaggio cifrato senza disporre della chiave o senza scoprire il sistema di cifratura.

Crittografia
la scienza della scrittura nascosta (o segreta) che permette di memorizzare e trasmettere dati in una forma utilizzabile solo dagli individui a cui essi sono destinati.

crittografia a curve ellittiche (ECC)
tecnologia di cifratura asimmetrica con chiavi molto più corte rispetto a RSA. Una chiave ECC di 163 bit equivale a una chiave RSA di 1024 bit. Le curve ellittiche sono una branca della teoria dei numeri e sono definite da certe equazioni cubiche (di terzo grado); le loro proprietà permettono di creare algoritmi crittografici asimmetrici, vista l'estrema difficoltà di eseguire i calcoli a ritroso per ricostruire la chiave privata dalla chiave pubblica e dalle condizioni iniziali.

Crittografia asimmetrica
la chiave di cifratura è diversa da quella di decifratura. Detta anche crittografia a chiave pubblica.

Crittografia simmetrica
la chiave di cifratura è la stessa usata per la decifratura, o possono essere derivate facilmente una dall'altra. Detta anche crittografia a chiave segreta.

Crittologia
lo studio della crittografia e della crittoanalisi.

Crittosistema
l'implementazione hardware o software della crittografia, che trasforma un messaggio in chiaro (plaintext) in un messaggio cifrato (ciphertext) e poi di nuovo nel messaggio in chiaro originario.

CRL (Certificate Revocation List)
contiene l'elenco dei certificati sospesi e revocati. E' una struttura firmata (poiché occorre garantire l'attendibilità delle informazioni che vi sono contenute) ed è composta di due parti: una generale con informazioni sulla CRL stessa e la lista dei certificati revocati dall'ente emettitore.
CSIRT (Computer Security Incident ResponseTeam) squadre di intervento per gli incidenti di sicurezza informatica coordinate dal CERT-Coordination Center.

Custode dei dati
ha la responsabilità della manutenzione e della protezione dei dati.

Decifrare o decifratura
l'azione di trasformare i dati in formato leggibile.

DES (Data Encryption Standard)
è l'algoritmo di cifratura più conosciuto ed è stato il primo di cui sono stati forniti tutti i dettagli di implementazione. E' stato incluso nella maggioranza dei prodotti commerciali

dotati di funzionalità crittografiche ed è stato usato dagli enti governativi. Per oltre un decennio, DES è stato considerato uno degli algoritmi più efficaci ed efficienti, finché la NSA smise di supportarlo nel 1988, prevedendo la sua vulnerabilità a fronte della crescita della potenza di calcolo dei computer.

Diffie-Hellmann
algoritmo di crittografia asimmetrica, è utilizzato per lo scambio delle chiavi, dove i due interlocutori si scambiano le chiavi pubbliche e, con le proprie chiavi private, costruiscono una chiave segreta condivisa.

Digest
vedi hash.

Disaster Recovery
nel contesto informatico, è la capacità di un'infrastruttura di riprendere le operazioni dopo un disastro.

Disponibilità
è il grado in cui le informazioni e le risorse informatiche sono accessibili agli utenti che ne hanno diritto, nel momento in cui servono.

Distributed IDS (DIDS)
è una combinazione di sensori NIDS e sensori HIDS, distribuiti attraverso la rete aziendale, che riportano le informazioni a un sistema centrale di coordinamento.

DMZ (Demilitarized Zone)
il termine di origine militare indica un'area tampone tra una zona fidata e una non fidata all'interno della quale non sono consentite le armi. Applicata al networking, una DMZ è una sottorete alla quale sono connessi sistemi accessibili da reti con diversi livelli di fiducia e criticità.

DSA (Digital Signature Algorithm)
una variante dell'algoritmo di cifratura asimmetrica ElGamal è il DSA, o Digital Signature Algorithm, sviluppato dalla NSA e pubblicato dal NIST (National Institute of Standards and Technology) e diventato uno standard del governo USA.

DSS (Digital Signature Standard)
Lo standard federale americano per la firma elettronica di cui DSA è l'algoritmo di firma e SHA è l'algoritmo di hash.

Dynamic packet filtering
Vedi Stateful inspection.

ECB (Electronic Code Book)
un dei principali cifrari a blocchi. Ogni blocco di testo in chiaro viene trasformato in un blocco di testo cifrato. Lo stesso blocco di testo, con la stessa chiave, produce sempre lo stesso blocco di testo cifrato, il che consente ai malintenzionati di compilare un codice (code book) di tutti i possibili testi cifrati corrispondenti a un dato testo in chiaro.

ECDSA
una variante più efficiente del DSA basata sulle curve ellittiche.

Efficacia
una proprietà che mette in relazione la contromisura (prodotto, procedura o altro) con il contesto in cui è utilizzata, in particolare le vulnerabilità, la gravità e la probabilità di attuazione delle minacce.

ElGamal
algoritmo di cifratura asimmetrica. Può essere usato sia per la cifratura sia per l'autenticazione con firma digitale. E' un algoritmo sicuro e ha la caratteristica di generare un testo cifrato lungo il doppio del testo in chiaro.

ESP (Encapsulation Security Payload)
uno dei protocolli della famiglia IPSec. Fornisce la prova di origine dei pacchetti ricevuti, l'integrità dei dati, la protezione da replay (invio ripetuto degli stessi dati) e la riservatezza, ottenuta attraverso la cifratura del traffico.

ETSI (European Telecommunications Standards Institute)
un'organizzazione europea indipendente, riconosciuta dalla Commissione Europea e dall'EFTA. Ha sede a Sophia Antipolis (Francia) ed è responsabile per la standardizzazione delle tecnologie informatiche e di comunicazioni (ICT) in Europa.

Firma digitale
una firma dev'essere difficile da falsificare, non ripudiabile (non può essere cancellata o disconosciuta), inalterabile (dopo l'apposizione della firma, non deve essere possibile modificare il documento) e non trasferibile (da un documento a un altro). La firma digitale si basa sulla cifratura asimmetrica di un hash o digest calcolato sul contenuto del documento o messaggio.

FIRST (Forum for Incident Response and Security Teams)
I CERT o CSIRT delle varie nazioni sono collegati in una struttura internazionale, il FIRST, che permette la rapida condivisione delle informazioni utili a fronteggiare minacce e attacchi.

FTP bounce
un attacco (rimbalzo FTP) che sfrutta una vulnerabilità del protocollo FTP per cui un attaccante è in grado di usare il comando PORT per chiedere accesso alle porte indirettamente, attraverso l'uso del server FTP come intermediario nella richiesta.

Funzionalità
applicato alla sicurezza, conserva il significato generale che ha in altri settori; è l'insieme di ciò che un prodotto o un sistema informatico fornisce in relazione alla protezione delle informazioni e, di riflesso, delle risorse e dei servizi informatici.

Funzioni di sicurezza
Vedi contromisure di tipo tecnico informatico.

Garanzia
concetto introdotto da chi si occupa di sicurezza per esprimere il grado in cui l'implementazione di una funzionalità riduce una vulnerabilità o la possibilità di attuazione di una minaccia.

Gestione del rischio
nella gestione del rischio si possono individuare due fasi distinte.1) Analisi del rischio. 2) Controllo del rischio.
Hash un numero binario di lunghezza fissa, ricavato da un input (file, messaggio, blocco di dati eccetera) di lunghezza variabile, che funge da "impronta" del dato di partenza.

HMAC
Un tipo speciale di MAC specificato nella RFC 2104. HMAC è anch'essa una funzione keyed hash, ma in realtà costituisce un keyed hash
all'interno di un keyed hash.

honeynet
una rete composta da honeypot, ossia sistemi vulnerabili verso cui attirare un attaccante per distrarlo dai sistemi critici e trattenerlo abbastanza a lungo da individuarlo.

Honeypot
un sistema esca, distinto e complementare rispetto a un IDS, progettato per attirare gli attaccanti lontano dai sistemi critici.

Host-Based IDS (HIDS)
un IDS basato su host (HIDS) differisce da un NIDS in due modi: protegge solo il sistema su cui è installato (anziché la sottorete) e la scheda di rete del sistema su cui è installato funziona in modo non promiscuo (non ascolta i pacchetti destinati agli altri nodi della sottorete).

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

IANA (Internet Assigned Numbers Authority)
mantiene le funzioni di coordinamento centrale dell'Internet globale nel pubblico interesse. La IANA custodisce i numerosi parametri e valori di protocollo unici necessari per il funzionamento di Internet e per il suo sviluppo futuro.

ICANN (Internet Corporation for Assigned Names and

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

IDEA
IDEA è un cifrario simmetrico a blocchi di 64 bit, suddivisi in 16 sotto-blocchi sottoposti a otto serie di manipolazioni matematiche. IDEA presenta similitudini con DES, ma è molto più robusto. La chiave è lunga 128 bit. IDEA è brevettato ed è concesso in licenza dalla società svizzera Mediacrypt.

Identificazione e autenticazione
Le funzioni di questa categoria servono a identificare un individuo o un processo e ad autenticarne l'identità.

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

IETF (Internet Engineering Task Force)
una vasta comunità internazionale di progettisti, operatori, produttori e ricercatori nel campo del networking, interessati all'evoluzione dell'architettura di Internet e all'affidabilità del suo funzionamento.

IKE (Internet Key Exchange)
uno dei protocolli della famiglia IPSec. Fornisce un modo dinamico automatico per autenticare gli interlocutori, negoziare i servizi di sicurezza e generare chiavi condivise.

Impatto
è la conseguenza dell'attuazione di una minaccia.
Integrità è la fedele conservazione del contenuto originario di un documento archiviato o trasmesso in rete, attestata da strumenti che segnalano se il documento ha subito alterazioni. L'integrità è il grado di correttezza, coerenza e affidabilità delle informazioni e anche il grado di completezza, coerenza e condizioni di funzionamento delle risorse informatiche.

Internet Society – ISOC
un'organizzazione privata senza fini di lucro che riunisce professionisti nel mondo del networking e che ha la missione di garantire il continuo funzionamento di Internet e il suo potenziamento.

Intrusion Detection Systems (IDS)
sistemi hardware o software che automatizzano il processo di monitoraggio degli eventi che avvengono in un sistema o in una rete, analizzandoli alla ricerca d'indicatori riconducibili a problemi di sicurezza. Hanno il compito di riscontrare attività sospette e intrusioni, sia di tipo classificato e riconoscibile tramite pattern matching, sia di tipo sconosciuto in virtù di qualche anomalia di comportamento o di uso scorretto dei protocolli.

Intrusion Prevention Systems (IPS)
sistemi che cercano d'inviduare tentativi d'intrusione e rispondere immediatamente. Anziché limitarsi a monitorare il traffico come fanno gli IDS, gli IPS vengono installati in linea, di fronte alla rete o al servizio da proteggere, in modo da bloccare il traffico ostile.

IPSec (Internet Protocol Security)
La principale suite di protocolli usata per creare VPN (Virtual Private Network). Fornisce funzioni di autenticazione e di cifratura a livello del protocollo IP. Il modo in cui IPSec protegge i pacchetti IP è attraverso l'uso di uno dei suoi due protocolli, ESP (Encapsulation Security Payload) o AH (Authentication Header). AH fornisce la prova di origine dei pacchetti ricevuti, l'integrità dei dati e la protezione da replay. ESP offre tutto ciò che fornisce AH con in più la riservatezza, ottenuta attraverso la cifratura del traffico.

IRTF (Internet Research Task Force)
ha la missione di promuovere attività di ricerca che possano contribuire in modo significativo al futuro sviluppo di Internet. Opera creando gruppi di ricerca focalizzati sui seguenti temi: protocolli, applicazioni, architettura e tecnologia.

ISO (International Organization for Standardization)
la maggiore organizzazione internazionale di standardizzazione e comprende gli enti di standardizzazione nazionali di 146 paesi (l'UNI è il membro italiano).

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

ITSEC (Information Security Evaluation Criteria)
il primo tentativo di stabilire un unico standard di valutazione degli attributi di sicurezza da parte di molti paesi europei.

ITU (International Telecommunication Union)
un'organizzazione internazionale, nell'ambito dell'ONU, dove governi e settore privato coordinano le reti e i servizi globali di telecomunicazioni. Ha sede a Ginevra e comprende i settori ITU-T (standardizzazione), ITU-R (radiocomunicazioni) e ITU-D (sviluppo).

Keyed hashing
Far dipendere l'hash del messaggio da una chiave segreta. Il keyed hashing viene usato nella crittografia simmetrica per produrre i codici MAC utilizzati per autenticare i messaggi e garantirne l'integrità.

Keyspace
(spazio delle chiavi) l'insieme di tutti i possibili valori che una chiave può assumere.

Layer 2 Forwarding (L2F)
protocollo di tunneling di strato 2. A differenza di PPTP e L2TP, L2F è destinato all'uso tra dispositivi di rete, come il server di accesso alla rete di un ISP (Internet Service Provider), e il gateway VPN di un'azienda. Gli utenti stabiliscono una connessione non protetta dal loro computer all'ISP. Quest'ultimo riconosce che il traffico degli utenti deve essere incapsulato in un tunnel verso l'azienda, perciò autentica ogni utente e il gateway dell'azienda, quindi fornisce la protezione del traffico tra il proprio server e l'azienda.

Layer 2 Tunneling Protocol (L2TP)
alla pari di PPTP, protegge le comunicazioni tra un client e un server entrambi abilitati a L2TP. Utilizza un proprio protocollo di tunneling che fa uso della porta UDP 1701. Inoltre, L2TP supporta sessioni multiple nello stesso tunnel.

Link Mode Port
vedi Port Mirroring.

MAC (Message Authentication Code)
un hash calcolato su un messaggio con l'aggiunta di una chiave segreta condivisa, usato per verificare all'altro capo della comunicazione l'integrità del messaggio.

man-in-the-middle
tipo di attacco dove il nemico finge rispettivamente di essere l'altro interlocutore nei confronti di due sistemi tra i quali si è interposto. Intercetta il traffico dell'uno prima di ritrasmetterlo all'altro e viceversa, fingendo ogni volta di essere il mittente e il destinatario corretto per ciascuna

comunicazione.

MD5
algoritmo di hash evoluzione di MD4, è stato sviluppato da Ron Rivest all'MIT nel 1991 ed è descritto nella RFC 1321 (www.ietf.org/rfc). MD5 è molto popolare, ma la crescita della potenza di calcolo e i primi successi degli attacchi sia basati su forza bruta sia di tipo crittoanalitico (basati sull'analisi dell'algoritmo) inducono a considerare MD5 vulnerabile

Microsoft Point-to-Point Encryption (MPPE)
un meccanismo di cifratura per PPTP sviluppato da Microsoft, che usa una chiave da 40 o 128 bit con l'algoritmo RC4 di RSA.

MIME (Multipurpose Internet Mail Extensions)
è lo standard che specifica come devono essere trasferiti i dati multimediali e gli allegati di e-mail.

Minaccia
è un'azione potenziale, accidentale o deliberata, che può portare alla violazione di uno o più obiettivi di sicurezza.

Monitoring Port
vedi Port Mirroring.

Network-Based IDS (NIDS)
sotto controllo un intero segmento di rete (o sottorete). La scheda passa agli strati di rete superiori non solo i pacchetti diretti all'indirizzo MAC (Media Access Control) della scheda, ma tutti i pacchetti che transitano in quel punto della rete, qualunque sia il destinatario. L'IDS si comporta quindi da sniffer di tutto il traffico in transito, che viene quindi analizzato con metodi diversi.

Non ripudio
impedisce che un evento o documento possa essere disconosciuto dal suo autore.

Norme e linee guida
segnaliamo le linee guida ISO/IEC 13335 e le norme BS (British Standard) 7799.

Norme funzionali
sono relative ai prodotti e hanno lo scopo principale di ricercare l'interoperabilità dei prodotti informatici. Coprono argomenti quali i protocolli di comunicazione, il formato dei dati (per esempio in un certificato digitale o in una smartcard) e così via.

Obiettivi
gli obiettivi di sicurezza sono il grado di protezione che si intende predisporre per i beni, in termini di disponibilità, integrità e riservatezza.

OCSP (Online Certificate Status Protocol)
è un protocollo relativamente semplice di domanda-risposta, che offre uno strumento per ottenere online informazioni aggiornate sulla revoca dei certificati, fornite da un'entità fidata.

one-way hash function
produce una trasformazione a senso unico, dove a N possibili input corrisponde un output, da cui non è possibile risalire all'input. L'hashing one-way viene usato nella crittografia asimmetrica per produrre le firme digitali (ad esempio con gli algoritmi RSA o DSA), anche in questo caso per assicurare l'autenticità e l'integrità dei dati trasmessi o archiviati.

Packet filter
il tipo più semplice di firewall che consiste di un router che include una funzione di controllo d'accesso per i singoli pacchetti governata da una serie di regole (ruleset) eseguite in sequenza.

Padded Cell
una padded cell (cella imbottita) opera in coppia con un IDS, Quando l'IDS riconosce un attaccante, lo trasferisce in modo trasparente a uno speciale host con funzione di padded cell, che contiene un ambiente simulato dove l'attaccante non può fare danno.

Pattern matching
uno dei tre metodi usati dagli IDS per riconoscere segni d'intrusione. Consiste nel riconoscimento dei pacchetti a fronte di un database di "firme" che identificano i vari tipi di attacco.

PGP (Pretty Good Privacy)
un programma di sicurezza per la posta elettronica realizzato da Phil Zimmermann e pubblicato inizialmente nel 1991 come freeware. Le funzioni di PGP sono: firma digitale, cifratura dei messaggi, compressione, conversione in ASCII (in base 64) e segmentazione dei messaggi; di queste, le prime due rientrano nel contesto delle applicazioni crittografiche.

PKCS (Public Key Cryptographic Standard)
comprende un'intera serie di standard che hanno l'obiettivo di agevolare l'implementazione delle tecnologie PKI (per esempio, PKCS #1 descrive lo standard di cifratura RSA). PKCS #7 specifica i formati binari usati per la firma digitale e per la "busta elettronica". Lo standard PKCS #7 è stato adottato dall'IETF nella RFC 2315, aggiornata dalla RFC 2630.

PKI (Public Key Infrastructure)
L'infrastruttura a chiave pubblica nasce con lo scopo di distribuire e gestire in modo sicuro le chiavi pubbliche per tutto il periodo della loro validità, garantendo la corrispondenza tra ogni chiave pubblica e il proprietario della coppia di chiavi. La garanzia di autenticità delle chiavi pubbliche (e quindi delle corrispondenti chiavi private) è fornita dalle Autorità di Certificazione (Certification Authority o CA) tramite l'emissione di certificati digitali.

Point-to-Point Tunneling Protocol (PPTP)
fornisce un tunnel protetto tra un client (per esempio un personal computer) e un server entrambi abilitati a PPTP. La versione 2 ha risolto molti problemi di sicurezza, ma se ne consiglia l'utilizzo solo per connessioni occasionali senza alti requisiti di sicurezza.

Politica di sicurezza
è un documento sintetico in cui il management superiore, o un comitato delegato allo scopo, delinea il ruolo della sicurezza nell'organizzazione o in un suo aspetto particolare.

Port Mirroring
per consentire l'analisi del traffico a scopo di prevenzione delle intrusioni, gli switch vengono riconfigurati in modo da replicare i dati di tutte le porte o VLAN (Virtual LAN) su una singola porta di mirroring. Spesso Port Mirroring indica più precisamente la capacità di copiare il traffico da una singola porta a una porta di mirroring, disattivandone il traffico bidirezionale. Vedi anche Spanning Port.

Privacy
consiste nella salvaguardia dei dati privati degli utenti, anche in conformità alla legge 196/2003 sulla protezione dei dati personali.

Proprietario dei dati
un membro del management superiore, il massimo responsabile della protezione delle informazioni e della sicurezza in generale.

Proxy
(procuratore) un server che si frappone fra un'applicazione client (come un browser) e un reale server (come un web server). Al server il proxy appare come se fosse il client, mentre al client esso appare come se fosse il vero server.

Proxy firewall
un firewall basato su proxy (detto anche application gateway, proxy gateway e proxy server) che richiede un'applicazione specifica per ogni protocollo. Vengono usate applicazioni che accettano connessioni dai client, esaminano il traffico e aprono corrispondenti connessioni verso i server.

RC4
RC4 è il più noto dei cifrari a flusso. E' stato creato nel 1987 da Ron Rivest per RSA Security. Utilizza un keystream di dimensioni variabili (ma solitamente di 128 bit) e opera su un byte alla volta. In origine il cifrario era segreto, ma fu fatto filtrare su Internet. L'algoritmo è molto

robusto se utilizzato con chiavi di lunghezza adeguata (tipicamente 128 bit) casuali e non riutilizzate.

RC5
RC5 è un cifrario simmetrico a blocchi dotato di parecchi parametri per assegnare le dimensioni del blocco, la lunghezza della chiave e il numero di passaggi di trasformazione da eseguire. E' stato creato da Ron Rivest (la R di RSA). Di solito si utilizzano blocchi di 32, 64 o 128 bit e la chiave può raggiungere i 2.048 bit. RC5 è stato brevettato da RSA Security nel 1997. Il basso consumo di memoria lo rendono adatto per smartcard e altri dispositivi simili.

Recovery Point Objective (RPO)
il momento nel tempo a cui il sistema è riportato.

Recovery Time Objective (RTO)
il lasso di tempo che intercorre prima di ripristinare l'infrastruttura.

Registration Authority
un componente dell'infrastruttura che viene talvolta utilizzato per sollevare la CA da certe funzioni, aumentando la scalabilità e riducendo i costi. I servizi della RA sono di autenticazione e validazione delle richieste provenienti dalle entità utenti.

Rendicontabilità (accountability)
le funzioni che permettono di attribuire la responsabilità degli eventi agli individui che li hanno causati.

Replay
tecnica d'attacco che prevede l'invio ripetuto degli stessi dati oppure con forte alterazione della sequenza. L'attaccante usa un vecchio messaggio o parte del traffico che ha intercettato e registrato e che ora ripropone per indurre un server a ripetere una determinata operazione. Un impiego tipico è richiedere l'autenticazione riciclando informazioni di autenticazione utilizzate da qualcun altro in precedenza.

Reverse proxy
indica un proxy utilizzato per la protezione di un server, tipicamente un web server (HTTP/HTTPS) su Internet. Gli usi più comuni dei reverse proxy riguardano il bilanciamento del carico e la continuità del servizio, che costituiscono anche un aspetto di disponibilità.

Rilevamento delle anomalie
uno dei tre metodi usati dagli IDS per riconoscere segni d'intrusione. Suddivisibili in anomalie basate sul comportamento e in anomalie basate sul protocollo. Il rilevamento delle anomalie si basa sull'esame del traffico a livello superiore rispetto al pattern matching e all'analisi dei protocolli. Anziché i singoli pacchetti, si osserva il traffico nel suo complesso

RIPEMD-160
algoritmo di hash sviluppato nell'ambito del progetto European RACE Integrity Primitives Evaluation (RIPE) da un gruppo di ricercatori che avevano conseguito parziali successi nell'attaccare MD4 e MD5.

Rischio
Concettualmente, il rischio è la possibilità che si verifichi un evento dannoso ed è tanto maggiore quanto è forte l'impatto causato dall'evento e quanto è alta la probabilità che esso si verifichi.

Riservatezza
consiste nel limitare l'accesso alle informazioni e alle risorse informatiche alle sole persone autorizzate e si applica sia all'archiviazione sia alla comunicazione delle informazioni.

Riutilizzo degli oggetti
le funzioni che permettono di riutilizzare oggetti contenenti informazioni riservate: supporti magnetici, supporti ottici riscrivibili, aree di memoria RAM, zone di memoria dei processori (registri, cache, ecc.), buffer di periferiche e simili.

RSA
dell'omonima azienda, è il cifrario asimmetrico più utilizzato. Può essere usato sia per la cifratura (per ottenere la riservatezza), sia per la firma digitale (per ottenere l'autenticazione), sia per lo scambio delle chiavi (come nell'esempio di cui sopra).

S/MIME (Secure/Multipurpose Internet Mail Extensions)
è un protocollo che aggiunge la cifratura e la firma elettronica ai messaggi MIME descritti nella RFC 1521 (Mechanisms for Specifying and Describing the Format of Internet Message Bodies).

Scambio dati sicuro
le funzioni destinate a garantire la sicurezza delle trasmissioni. Il modello OSI Security Architecture (ISO 7498-2) le classifica nelle seguenti sottoclassi: autenticazione, controllo dell'accesso, riservatezza, integrità (dell'hardware, dei dati e dei flussi di pacchetti trasmessi sia in modo connectionless, come UDP, sia connection-oriented, come TCP, anche ai fini della corretta sequenza dei pacchetti) e non ripudio.

Screened subnet
a differenza di una DMZ che è una piccola sottorete collocata tra il router Internet e l'interfaccia esterna del firewall, una screened subnet è una rete isolata accessibile solo attraverso una delle interfacce del firewall e non connessa direttamente alla rete interna.

Secure Shell (SSH)
un protocollo per realizzare un collegamento remoto sicuro da un computer a un altro attraverso una rete insicura. Supporta il login remoto sicuro, il trasferimento sicuro di file e l'inoltro sicuro del traffico di tipo TCP/IP e X Window. SSH è in grado di autenticare, cifrare e comprimere i dati trasmessi.

Secure Sockets Layer (SSL)
è un protocollo per la protezione di un canale di comunicazione attraverso una rete e funziona allo strato di trasporto, tra i protocolli di trasporto e di applicazione. Come altri protocolli di sicurezza di rete, SSL utilizza la crittografia simmetrica e asimmetrica e le funzioni di hash per fornire l'autenticazione del server (e in opzione anche del client), la cifratura dei messaggi e l'integrità dei dati.

SHA (Secure Hash Algorithm)
uno standard FIPS (Federal Information Processing Standard) statunitense. SHA genera un digest di 160 bit che viene passato a DSA o a un altro degli algoritmi di firma digitale ammessi dal governo USA (RSA ed ECDSA, Elliptic Curve Digital Signature Algorithm).

SHA-1
è stato sviluppato dal NIST ed è stato pubblicato come standard federale USA nel 1993 con il nome di Secure Hash Algorithm (SHA, FIPS 180) e riveduto nel 1995 come SHA-1 (FIPS180-1). SHA-1 riceve in input un messaggio di lunghezza massima inferiore a 264 bit (una dimensione equivalente a 2.147 Gbyte e perciò praticamente illimitata), suddiviso in blocchi di 512 bit, e produce un hash di 160 bit.

Sicurezza attiva
le misure di sicurezza che proteggono le informazioni in modo proattivo, in modo cioè da anticipare e neutralizzare i problemi futuri. Questo viene ottenuto non solo impedendo agli estranei di accedere alle informazioni (sicurezza passiva o difensiva), ma rendendo le informazioni intrinsecamente sicure a livello applicativo, proteggendone la riservatezza (confidentiality, chiamata anche confidenzialità), l'integrità e l'autenticità.

Sicurezza passiva
un approccio fondamentalmente difensivo o passivo, che valuta quali rischi accettare, quali delegare a terzi e quali controllare, riducendoli o azzerandoli.

Skipjack
Skipjack è un cifrario a blocchi sviluppato dalla NSA nel 1987, messo in servizio nel 1993 e declassificato nel 1998.

Social engineering

è la pratica di manipolare ad arte le persone per indurle a compiere azioni (come l'esecuzione di software maligno) oppure a rivelare informazioni (come le password) utili a ottenere accesso a dati e risorse.

SPAN port
vedi Spanning Port.

Spanning Port
in parte sinonimo di Port Mirroring. Per consentire l'analisi del traffico a scopo di prevenzione delle intrusioni, gli switch vengono riconfigurati in modo da replicare i dati di tutte le porte o VLAN (Virtual LAN) su una singola porta di mirroring. Spanning Port indica in particolare la possibilità di copiare il traffico da tutte le porte a una singola porta, disattivandone il traffico bidirezionale.

Stateful inspection
tutti i filtri di pacchetti che implementano qualche forma di stateful inspection mantengono in memoria lo stato di tutte le comunicazioni che attraversano il firewall e determinano se bloccare i singoli pacchetti in base a interi flussi di comunicazione, non semplicemente sulla base dei singoli pacchetti. Perciò, i firewall del tipo stateful inspection (o stateful packet inspection, SPI) permettono o bloccano il passaggio di un pacchetto non solo in base a indirizzi IP e porte, ma anche utilizzando SYN, ACK, numeri di sequenza e altri dati contenuti nell'header TCP (strato 4).

Static packet filtering
Vedi Packet filtering

TCSEC (Trusted Computing Security Evaluation Criteria)
un sistema per valutare la funzionalità e garanzia di un prodotto, usato soprattutto negli USA e descritto nel cosiddetto Orange Book, un volume dalla copertina arancione. Serve per valutare sistemi operativi, applicazioni e prodotti di vario genere.

Testo cifrato (ciphertext)
dati in forma cifrata o illeggibile.

Testo in chiaro (plaintext o cleartext)
dati in forma leggibile o intelligibile.

Time Stamp Authority (TSA)
una terza parte fidata che attesta il tempo di produzione o d'invio di un documento tramite una "marca temporale", che è di fatto una controfirma del documento contenente un hash del documento, il riferimento temporale e altre informazioni.

TLS (Transport Layer Security)
un protocollo definito dall'IETF nella RFC 2246, simile a SSL, ma con differenze soprattutto negli algoritmi crittografici utilizzati.

UNINFO
una libera associazione a carattere tecnico, con lo scopo di promuovere e di partecipare allo sviluppo della normativa nel settore delle tecniche informatiche. L'UNINFO è associato all'UNI, l'ente nazionale italiano di unificazione (www.uni.com/it) e rappresenta l'Italia presso CEN e ISO. Verifica (audit) le funzioni che registrano gli eventi in un file di logging, con informazioni riguardo a errori e a violazioni di sicurezza.

Virtual Private Network (VPN)
una VPN è una rete virtuale, costruita sulla base di reti fisiche esistenti, in grado di fornire un meccanismo di comunicazione sicura dei dati e delle informazioni IP trasmessi in rete.

Vulnerabilità
una vulnerabilità è un punto debole del sistema informatico (hardware, software e procedure) che, se colpito o sfruttato da una minaccia, porta alla violazione di qualche obiettivo di sicurezza.

Work factor (fattore di lavoro)
il tempo, lo sforzo e le risorse che si stimano necessari per violare un crittosistema.