Misure minime di sicurezza informatica del nuovo codice della privacy (D.Lgs. 196/2003)

di Enrico Zimuel (enrico@zimuel.it)

7 Maggio 2004 Padova

Note sul copyright (copyfree):

Questa presentazione può essere utilizzata liberamente
a patto di citare la fonte e non stravolgerne il contenuto.

Questa presentazione è stata realizzata con OpenOffice 1.1,
il software open source per l'automazione d'ufficio disponibile
sui sistemi Gnu/Linux e Ms Windows.
www.openoffice.org

Sommario

- Il nuovo Codice della privacy (D.Lgs. 196/2003)
- Principi generali e definizioni di base (Art. 1 - 6)
- Misure minime e misure idonee di sicurezza (Art. 31 – 36)
- Disciplinare tecnico in materia di misure minime di sicurezza (Allegato B)
- Il documento programmatico sulla sicurezza
- La “sicurezza” delle password ed i sistemi a doppia autenticazione
- Il ruolo della crittografia nella difesa della privacy

Il nuovo Codice della privacy (D.Lgs. 196/2003)

- Il nuovo Codice della privacy, approvato alla fine di giugno 2003, rappresenta una vera e propria rivoluzione in questo settore.

- E' un Codice “voluminoso” con i suoi 186 articoli e 3 allegati; è entrato in vigore nel primo gennaio 2004 ed è un aggiornamento sostanziale del precedente D.P.R. 318/99.

- L'obiettivo fondamentale del nuovo Codice è quello di accorpare e semplificare i numerosi provvedimenti legislativi che hanno integrato la legge 675/96 in materia di protezione dei dati personali.

- Introduzione di uno specifico disciplinare tecnico, allegato B, in materia di misure minime di sicurezza.

Principi generali e definizioni di base

- “La protezione dei dati personali e' un diritto fondamentale delle persone” Stefano Rodotà (Garante per la protezione dei dati personali).

- Art. 1 (Diritto alla protezione dei dati personali)
Chiunque ha diritto alla protezione dei dati personali che lo riguardano.

- Art.2 (Finalità)
1. Il presente testo unico, di seguito denominato “codice”, garantisce che il trattamento dei dati personali si svolga nel rispetto dei diritti e delle libertà fondamentali, nonché della dignità dell’interessato, con particolare riferimento alla riservatezza, all'identità personale e al diritto alla protezione dei dati personali.

2. Il trattamento dei dati personali è disciplinato assicurando un elevato livello di tutela dei diritti e delle libertà di cui al comma 1...

Principi generali e definizioni di base

- Art.3 (Principio di necessità nel trattamento dei dati)

I sistemi informativi e i programmi informatici sono configurati riducendo al minimo l'utilizzazione di dati personali e di dati identificativi, in modo da escluderne il trattamento quando le finalità perseguite nei singoli casi possono essere realizzate mediante, rispettivamente, dati anonimi od opportune modalità che permettano di identificare l'interessato solo in caso di necessità.

- Art. 4 (Definizioni)

b) "dato personale", 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;

Principi generali e definizioni di base

- Art. 4 (Definizioni)

c) "dati identificativi", i dati personali che permettono l'identificazione diretta dell'interessato;

d) "dati sensibili", 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;

e) "dati giudiziari", i dati personali idonei a rivelare provvedimenti di cui all'articolo 3, comma 1, lettere da a) a o) e da r) a u), del d.P.R. 14 novembre 2002, n. 313, in materia di casellario giudiziale, di anagrafe delle sanzioni amministrative dipendenti da reato e dei relativi carichi pendenti, o la qualità di imputato o di indagato ai sensi degli articoli 60 e 61 del codice di procedura penale;

Principi generali e misure minime di sicurezza

- Art.5 (Oggetto ed ambito di applicazione)

1. Il presente codice disciplina il trattamento di dati personali, anche detenuti all'estero, effettuato da chiunque è stabilito nel territorio dello Stato o in un luogo comunque soggetto alla sovranità dello Stato.

- Art. 31 (Obblighi di sicurezza)

1. I dati personali oggetto di trattamento sono custoditi e controllati, anche in relazione alle conoscenze acquisite in base al progresso tecnico, alla natura dei dati e alle specifiche caratteristiche del trattamento, in modo da ridurre al minimo, mediante l'adozione di idonee e preventive misure di sicurezza, i rischi di distruzione o perdita, anche accidentale, dei dati stessi, di accesso non autorizzato o di trattamento non consentito o non conforme alle finalità della raccolta;

Misure minime di sicurezza

- Art. 33 (Misure minime)

1. Nel quadro dei più generali obblighi di sicurezza di cui all'articolo 31, o previsti da speciali disposizioni, i titolari del trattamento sono comunque tenuti ad adottare le misure minime individuate nel presente capo o ai sensi dell'articolo 58, comma 3, volte ad assicurare un livello minimo di protezione dei dati personali.

- Art. 34 (Trattamenti con strumenti elettronici)

1. Il trattamento di dati personali effettuato con strumenti elettronici è consentito solo se sono adottate, nei modi previsti dal disciplinare tecnico contenuto nell'allegato B), le seguenti misure minime:
a) autenticazione informatica;
b) adozione di procedure di gestione delle credenziali di autenticazione;
c) utilizzazione di un sistema di autorizzazione;

Misure minime di sicurezza

- Art. 34 (Trattamenti con strumenti elettronici)

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

Misure minime di sicurezza

- Art. 36 (Adeguamento)

1. Il disciplinare tecnico di cui all'allegato B), relativo alle misure minime di cui al presente capo, è aggiornato periodicamente con decreto del Ministro della giustizia di concerto con il Ministro per le innovazioni e le tecnologie, in relazione all'evoluzione tecnica e all'esperienza maturata nel settore.

Disciplinare tecnico in materia di misure minime di sicurezza (Allegato B)

- Modalità tecniche da adottare a cura del titolare, del responsabile ove designato e dell'incaricato, in caso di trattamento di strumenti elettronici.

- Sistema di autenticazione informatica

- Credenziali di autenticazione: codice per l'identificazione (username) + parola chiave; dispositivo di autenticazione (smart card, token usb, etc) + parola chiave (PIN) opzionale; dispositivo biometrico (impronte digitali, retina, volto, etc) + parola chiave opzionale.

- Le credenziali di autenticazione sono strettamente personali e devono essere disattivate nel caso di inutilizzo prolungato (6 mesi).

- La parola chiave deve essere di almeno 8 caratteri oppure della dimensione massima disponibile dal sistema informatico.

Disciplinare tecnico in materia di misure minime di sicurezza (Allegato B)

- La parola chiave non deve contenere riferimenti agevolmente riconducibili all'incaricato e deve essere modificata da quest'ultimo al primo utilizzo.

- La parola chiave ha una validità temporale massima di 6 mesi e nel caso di dati sensibili e dati giudiziari di 3 mesi.

- Gli incaricati devono essere istruiti sulle modalità di gestione della sicurezza del sistema informativo soprattutto con i sistemi da loro utilizzati quotidianamente. Non devono lasciare incustoditi i loro terminali informatici! (log-out o screen saver con password nel caso di assenza dalla postazione di lavoro)

- Backup dei dati legati alla privacy con frequenza almeno settimanale.

Disciplinare tecnico in materia di misure minime di sicurezza (Allegato B)

- Aggiornamento, almeno semestrale, dei sistemi informatici di sicurezza e dei relativi programmi (software) per la protezione dei dati.

- Aggiornamento, almeno annuale, dell'individuazione dell'ambito del trattamento consentito ai singoli incaricati e addetti alla gestione o alla manutenzione degli strumenti elettronici e conseguente aggiornamento dei profili di autorizzazione.

- Copia delle credenziali di autorizzazione e/o di un sistema alternativo di accesso ai dati in caso di assenza dei responsabili o degli incaricati.

- Cifratura dei dati personali idonei a rivelare lo stato di salute e la vita sessuale.

Il documento programmatico sulla sicurezza (DPS)

- 19. Entro il 31 marzo di ogni anno (entro il 30 giugno per il 2004, parere del Garante 22/3/2004), 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;

Il documento programmatico sulla sicurezza (DPS)

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...

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.

Misure minime e misure idonee

- Le misure minime di sicurezza individuate nel Codice della privacy (allegato B) sono necessari ma non sufficienti per garantire una sicurezza adeguata dei dati personali, sensibili e giudiziari.

- A queste misure minime è necessario affiancare delle misure idonee così come indicato anche nell'Art. 31 dove si parla di "adozione di idonee e preventive misure di sicurezza" in base al progesso tecnico.

- Ad esempio i tempi di aggiornamento dei sistemi di sicurezza indicati in almeno 6 mesi nell'allegato B non sono certamente sufficienti. Nella sicurezza informatica gli aggiornamenti sono a volte giornalieri (vedi ad esempio i sistemi antivirus o antispam).

- Lo stesso per i tempi di backup almeno settimanali che possono essere ridotti facilmente a tempi quotidiani grazie all'adozione di sistemi di backup automatizzati.

Alcune considerazioni sulle misure idonee

- Oltre alle misure minime di sicurezza introdotte nel Codice della privacy può essere opportuno far riferimento ad altri standard di sicurezza informatici come la normativa britannica BS 7799, codice di pratica per la gestione della sicurezza delle informazioni.

- Utilizzare metodi di analisi del rischio per la realizzazione del sistema di sicurezza dei dati e del documento programmatico di sicurezza. Ad esempio il metodo inglese CRAMM.

- I principi fondamentali del Codice della privacy impongono di adottare appropriate misure tecniche ed organizzative, che prevengono la rivelazione non autorizzata, ma, anche se la rivelazione potrebbe costituire una prova della violazione di questo obbligo, non può costituire una prova automatica di responsabilità.

Lunghezza della parola chiave e sicurezza

- Chiavi più lunghe = chiavi più sicure? In teoria si, in pratica no.
- Le chiavi vengono generate quasi sempre attraverso delle password di autenticazione scelte dall'utente (ad esempio la *pass phrase* del Pgp/GnuPg).
- Quasi sempre le password di autenticazione sono frasi di senso compiuto o frasi casuali di piccole dimensioni, ad esempio di 8 caratteri, è difficile ricordare a memoria più di 8 caratteri casuali.
- Questo limite umano fa diminuire notevolmente lo spazio delle chiavi ossia l'insieme di tutte le possibili permutazioni di una chiave di n bit.
- Tramite dei semplici programmi di cracking è possibile effettuare con successo un attacco di forza bruta (brute-forcing) basato su di un dizionario.

Lunghezza della parola chiave e sicurezza

- Alcuni test effettuati nel 2000 con un famoso programma di cracking, L0phtcrack, hanno dimostrato che il 90% delle password possono essere determinate in meno di un giorno e circa il 20% nell'arco di pochi minuti.
- Se in un sistema che contiene 1.000 account 999 utilizzano password incredibilmente complicate, L0phtcrack riesce a entrare nel sistema scoprendo l'unica password debole.
- Le password di autenticazione sono dunque insicure proprio perchè subentra nel sistema di sicurezza il fattore umano, le password devono essere ricordate dagli utenti.
- Il concetto stesso di password si basa su di un ossimoro: la password deve infatti essere una stringa di caratteri casuali, facile da ricordare.

I sistemi a doppia autenticazione

- Per evitare di affidare la sicurezza ad un semplice password scelta "casualmente" da un utente si possono utilizzare delle smart card e/o dei token hardware (smart card, usb keys, etc).
- Una smart card/token è un dispositivo di sicurezza in grado di memorizzare una chiave, ed in alcuni casi un algoritmo, in maniera sicura. Utilizzando tale dispositivo possiamo accedere in maniera sicura ad un sistema informatico.
- Oltre al possesso del dispositivo per poterlo utilizzare è necessario ricordare una password, un PIN, di accesso al dispositivo, ecco perchè si parla di doppia autenticazione.

I sistemi di autenticazione biometrica

- E' possibile ottenere un sistema di autenticazione a due fattori senza dover possedere una chiave su di un dispositivo hardware? La chiave può essere costituita da noi stessi!
- Tutti gli esseri umani presentano delle differenze fisiche caratteristiche ed univoche. Ad esempio le impronte digitali, la retina dell'occhio, la voce,etc.
- I sistemi biometrici sfruttano queste diversità fisiche per garantire l'univocità dell'accesso ad un sistema informatico.
- Anche in questo caso è consigliabile implementare sempre il sistema con una doppia autenticazione: una caratteristica fisica + una password/PIN per l'accesso.

Il ruolo della crittografia nella difesa della privacy

- Anche se nelle misure minime di sicurezza del Codice della privacy la cifratura dei dati è richiesta esclusivamente per alcune tipologie di dati sensibili è buona norma utilizzare sempre la crittografia quando ciò è possibile.
- Nei sistemi di autenticazione i dati relativi agli utenti (operatori) devono essere cifrati e le password memorizzate con i loro valori hash (SHA-1).
- Le comunicazioni tra sedi periferiche di una società devono essere protette tramite VPN (Virtual Private Network).
- La posta elettronica degli utenti può essere cifrata ed autenticata grazie ad un sistema PKI (Public Key Infrastructure).
- Quali algoritmi crittografici scegliere? Andare sul "sicuro" utilizzando gli Standard (AES, Blowfish, 3-DES, RSA, ElGamal, DSA, SHA-1, etc).

Concludendo

- Le misure minime di sicurezza non sono sufficienti per garantire realmente la privacy dei dati.
- La sicurezza non si ottiene semplicemente acquistando prodotti hardware o software.
- E' necessario adottare una cultura della sicurezza che non si limiti agli ambiti tecnici ma anche a quelli gestionali ed operativi in qualsiasi settore.
- Il nuovo Codice della privacy è solo un punto di partenza e non un punto di arrivo.
- Il DPS non deve essere considerato solo un adempimento ma uno strumento per identificare le problematiche legate alla gestione globale dei dati sensibili.
- "La sicurezza in un sistema informatico non è un prodotto ma un processo" Bruce Schneier

Bibliografia

- *Codice della privacy e misure minime di sicurezza. Con CD-ROM*
di Biasiotti Adalberto; EPC Libri

- *Codice della privacy. Commento alla normativa sulla protezione dei dati personali*
di Imperiali Riccardo; Imperiali Rosario ; Il Sole 24 Ore Pirola

- *Il nuovo codice della privacy. (Commento al d.lgs. 30 giugno 2003, n.196).*
di Elli Gianmario; Zallone Raffaele ; Linea Professionale

- *Guida al codice della privacy.*
di De Giorgi Maurizio; Lisi Andrea ; Edizioni Giuridiche Simone

- *Guida pratica alle nuove misure di sicurezza per la privacy*
di Berghella Fulvio ; Maggioli Editore

- *Le nuove norme in materia di privacy*
di Acciai Riccardo; Orlandi Stefano ; Maggioli Editore

- *Privacy. Il sogno americano: che cosa ne è stato?*
di Faulkner William - Adelphi Edizioni

Alcuni siti Internet italiani sulla privacy e sulla security

- Interlex, diritto tecnologia informazione - Protezione dei dati personali
http://www.interlex.it/675/indice.htm

- Sito ufficiale del Garante per la protezione dei dati personali
http://www.garanteprivacy.it/

- E-privacy 2004 - Data retention e diritto all'oblio
http://e-privacy.firenze.linux.it/

xs2law - portaile di accesso al "diritto" in rete
http://www.ecn.org/crypto/law/

- Clusit – Associazione italiana per la sicurezza informatica
http://www.clusit.it/

- Ministro per l'innovazione e le tecnologie
http://www.innovazione.gov.it/ita/index.shtml

- Punto informatico – Canale Privacy
http://punto-informatico.it/archivio/canali.asp?i=Privacy