Webbit 2004 - Milano 4 giugno

Adempimenti tecnici del nuovo codice privacy

ing. Andrea Gelpi
security@gelpi.it
www.gelpi.it

Adempimenti tecnici del nuovo codice privacy

- Che cosa è la sicurezza informatica?
  - Insieme di norme, regole e comportamenti per l'uso di sistemi informatici e di comunicazione
  - Norme -> Leggi e regolamenti
  - Regole -> Politiche di sicurezza aziendale
  - Comportamenti -> Formazione agli utenti

Adempimenti tecnici del nuovo codice privacy

- Internet assomiglia ad un enorme centro commerciale virtuale
  - Conosciamo i comportamenti rischiosi di un centro commerciale
  - E quelli presenti su Internet?
  - In un centro commerciale adottiamo dei comportamenti ben noti
  - E quando navighiamo su Internet?
- Quindi esiste per prima cosa un problema culturale
  - L'utente va sensibilizzato al problema
  - L'utente va guidato

Adempimenti tecnici del nuovo codice privacy

- Le regole tecniche del D.Lgs. 196/03 (Codice privacy) sono parte della sicurezza informatica e fanno la parte del leone
- Esistono altri aspetti di sicurezza informatica da considerare
  - Diritto d'autore (L. 633/41)
  - Reati informatici (L. 547/93)
  - ecc...

Adempimenti tecnici del nuovo codice privacy

- Codice Privacy - Misure di sicurezza
  - art. 31 Misure idonee
  - art. 32 Chiarisce l'art. 2 D.L. 171/98 (telecomunicazioni)
  - art. 33 Misure minime obbligatorie
  - art. 34 Regole tecniche per trattamenti con strumenti elettronici
  - art. 35 Regole tecniche per trattamenti senza strumenti elettronici
  - art. 36 Allegato B verrà aggiornato periodicamente
  - Allegato B Regole tecniche

Adempimenti tecnici del nuovo codice privacy

- Codice Privacy - Allegato B (trattamenti elettronici)
  - Sistema di autenticazione - non identifica l'utente, ma autentica dei codici
    - Codici d'accesso
      - Dispositivo di autenticazione (token, smart-card, biometria, ...)
      - Identificativo (UserID)
      - Parola chiave (password) [minimo 8 caratteri] riservata e conosciuta solamente dall'incaricato
      - Obbligo di cambio password al primo utilizzo e ogni 6 mesi o ogni 3 mesi in caso di trattamenti di dati sensibili o giudiziari
      - Parola chiave non deve contenere riferimenti agevolmente riconducibili all'incaricato
      - Codici non possono essere riutilizzati
      - Disattivazione dei codici d'accesso se non utilizzati da 6 mesi o cambio mansione dell'incaricato
      - Postazione di lavoro non può rimanere incustodita durante la sessione di lavoro

Adempimenti tecnici del nuovo codice privacy

- Codice Privacy - Allegato B (trattamenti elettronici)
  - Sistema di autorizzazione
    - Esiste in tutti i sistemi moderni
    - Va usato e controllato periodicamente (almeno una volta l'anno)
    - Va fatta pulizia dei profili vecchi e non più utilizzati (almeno una volta l'anno)

    - Windows autorizzazioni massime all'inizio - devo chiudere
    - Unix/Linux autorizzazioni minime all'inizio - devo aprire

Adempimenti tecnici del nuovo codice privacy

- Codice Privacy - Allegato B (trattamenti elettronici)
  - Altre misure di sicurezza
    - Obbligo di uso di antivirus aggiornato ogni 6 mesi
      - Va aggiornato tutti i giorni non ogni 6 mesi
    - Obbligo di eseguire il backup almeno una volta la settimana
      - Vanno fatte verifiche che il backup funzioni
      - Attenzione a dove conservo i backup
      - Le cassette ignifughe non sono dei frigoriferi - servono a poco
    - Obbligo di tenere aggiornati i sistemi (installazione dei correttivi)
    - Stesura documento programmatico sulla sicurezza
      - se si trattano dati sensibili o giudiziari
      - C'è chi sostiene vada fatto anche negli altri casi (la legge non è chiarissima)

Adempimenti tecnici del nuovo codice privacy

- Codice Privacy - Allegato B (trattamenti elettronici)
  - Altre misure di sicurezza solo per trattamenti di dati sensibili o giudiziari
    - I supporti rimovibili (FD, CD, USB, ecc.) alla fine del trattamento vanno distrutti o resi illeggibili
    - Obbligo di protezione contro l'accesso abusivo mediante utilizzo di idonei strumenti elettronici.
    - Obbligo di ripristino dei dati in caso di danni entro 7 giorni (disaster recovery)
    - Gli organismi sanitari effettuano il trattamento di dati inerenti lo stato di salute e la vita sessuale separandoli dagli altri dati personali o cifrando i dati.
    - I dati genetici sono trattati in locali chiusi ad accesso controllato e il loro trasferimento avviene in contenitori chiusi a chiave o cifrato se il trasferimento è in formato elettronico.

Adempimenti tecnici del nuovo codice privacy

- Codice Privacy - Allegato B (trattamenti elettronici)
  - Documento programmatico sulla sicurezza
  - Deve contenere:
    - L'elenco dei trattamenti
    - La distribuzione dei compiti e delle responsabilità
    - l'analisi dei rischi
    - Le misure di sicurezza adottate sia per la protezione dei dati, che dei locali
    - Un piano di disaster recovery con ripristino entro 7 giorni
    - Il piano di formazione degli incaricati
    - Le regole per i trattamenti affidati all'esterno

Adempimenti tecnici del nuovo codice privacy

- Codice Privacy - Allegato B (trattamenti non elettronici)
  - Istruzioni scritte agli incaricati per il controllo e la custodia di atti e documenti loro affidati durante il trattamento
  - Lista degli incaricati con i relativi profili di autorizzazione deve essere rivista annualmente
  - Gli atti e documenti contenenti dati sensibili o giudiziari affidati agli incaricati non devono essere visibili da terzi
  - L'accesso a dati sensibili o giudiziari è controllato e fuori dall'orario di lavoro va tenuto apposito registro per identificare e registrare chi accede.
  - Le persone che accedono a dati sensibili o giudiziari vanno preventivamente autorizzate.

Adempimenti tecnici del nuovo codice privacy

- Codice Privacy - Art. 31
  - 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 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.