Normativa sulla Sicurezza e sulla Privacy

Classe 5ASI
ITCG Fermi

Definizioni

- **Riservatezza** (o **confidenzialità**, o **segretezza**) **dei dati**: dati leggibili e comprensibili solo dalle persone autorizzate
- **Integrità dei dati**: dati letti e/o modificati solo da persone autorizzate
- **Disponibilità dei dati**: dati devono essere disponibili in qualunque momento per le persone autorizzate per cui occorre garantire la continuità del servizio
- **Paternità** (o **non ripudiabilità**) **dei dati**: ogni dato deve essere associato ad un utente che non può ripudiare i dati da lui spediti e/o firmati.
- **Autenticazione** ("o" **autenticità**): processo di riconoscimento delle credenziali dell'utente per assicurarsi dell'identità di chi invia e/o esegue operazioni.
  Metodi di verifica dell'identità di un utente: (1) informazioni riservate (es. password), (2) oggetti elettronici (es. smart card), (3) strumenti di riconoscimento biometrici (es. impronta digitale, fondo retina ecc.)
- **Autorizzazione**: per l'utente autenticato occorre stabilire l'insieme delle autorizzazioni (azioni permesse, risorse accessibili, dati consultabili e/o modificabili)

Azioni per la Sicurezza Informatica di un'Azienda

1. Definizione e attuazione di politiche che garantiscano le sei proprietà della sicurezza elencate nella slide precedente
2. Identificazione delle informazioni critiche e strategiche
3. Individuazione delle possibili minacce e delle strategie operative da attuare per prevenirle
4. Analisi della normativa vigente e conseguente adeguamento dei SIA
5. Analisi economica dei costi per la messa in opera degli interventi di adeguamento individuati e scelta delle alternative più convenienti

Prof. Montemurro

Giurisprudenza Informatica

1. Leggi sui crimini informatici e relative sanzioni per i malintenzionati e per coloro che eseguono azioni illecite
2. Leggi su **misure minime di sicurezza** che coloro che trattano i dati devono adottare (i) per ridurre al minimo i rischi di distruzione o perdita anche parziale dei dati, e (ii) per tutelare la privacy di tutti coloro che hanno fornito dati personali. Ciò viene fatto tramite l'utilizzo:
   i. di sistemi di autenticazione;
   ii. di sistemi di autorizzazione;
   iii. di soluzioni antivirus;
   iv. di sistemi di protezione da intrusioni maligne;
   v. di soluzioni di sicurezza per prevenire/evitare la commissione di reati da parte dei dipendenti (azienda può controllare il PC di un dipendente per prevenire gli abusi, ma non per monitorare la prestazione lavorativa).

Prof. Montemurro

Giurisprudenza Informatica

3. **Legge n. 675/1996**:
   i. istituisce il **garante della privacy** il quale è un organo composto da 4 membri eletti dal Parlamento, che rimangono in carica per un mandato di 4 anni rinnovabile. Il garante è un'autorità indipendente il cui obiettivo è assicurare (a) la tutela dei diritti e delle libertà fondamentali, (b) il rispetto della dignità nel trattamento dei dati personali, e (c) diffondere la cultura della tutela dei dati personali;
   ii. definisce il **titolare del trattamento dei dati** (cioè colui che usa i dati) come la persona fisica/giuridica, la Pubblica Amministrazione, un qualsiasi ente, organismo cui competono le scelte di fondo sulle finalità e sulle modalità di trattamento dei dati.

Giurisprudenza Informatica

4. **Legge sulla privacy** (o **D.lgs. n. 196/2003**):
   i. introduce il diritto alla protezione dei dati personali; il proprietario dei dati non è chi li usa, ma le persone a cui i dati si riferiscono;
   ii. sancisce, per chi tratta dati personali, (a) il dovere di proteggerli e conservarli, (b) l'obbligo della compilazione annuale del **Documento Programmatico sulla Sicurezza** (**DPS**) per attestare la corretta esecuzione e adempimento delle misure atte a proteggere e conservare i dati personali.

Giurisprudenza Informatica

5. **Regolamento europeo sulla privacy** (**General Data Protection Regulation GDPR**): regolamento UE, riguardante la protezione dei dati personali, rivolto a enti e organizzazioni che raccolgono dati personali online, di cittadini europei, e li archiviano su server residenti sia all'interno che all'esterno dell'Unione Europea. Le novità introdotte da tale regolamento riguardano:
   i. le condizioni che regolano la diffusione dei dati personali; il trattamento dei dati dell'utente deve essere richiesto in modo esplicito, tracciabile, e non deve condizionare l'accesso ad un servizio;
   ii. il diritto alla cancellazione dei dati personali (**diritto all'oblio**), cioè il proprietario dei dati personali può chiedere al titolare del trattamento degli stessi di cancellarli.

Giurisprudenza Informatica

5. **Regolamento europeo sulla privacy** (**General Data Protection Regulation GDPR**): istituisce il **registro del trattamento dei dati personali** il quale prevede che il titolare del trattamento dei dati personali:
   i. conservi la documentazione di tutti i trattamenti effettuati sotto la propria responsabilità;
   ii. indichi obbligatoriamente, per ogni trattamento eseguito, tutte le informazioni che comprovano la conformità di ciascuna operazione alle disposizioni del regolamento GDPR.


thank you
danke
謝謝
ngiyabonga
teşekkür ederim
gracias
спасибо
dziękuję
obrigado
bedankt
sukriya
kop khun krap
go raibh maith agat
mochchakkeram
arigatō
dakujem
merci
мерси
terima kasih
grazie
감사합니다
dank je
tapadh leat
sagolun
hvala
takk