

La Sicurezza nei Contratti ICT

“Che cosa il Committente può *ragionevolmente*
pretendere

Che cosa il Fornitore deve *ragionevolmente*
garantire”

L. Vann.

In quali Contratti ?

tutti quelli in cui siano previste le seguenti facoltà

- Accesso (fisico o virtuale / remoto)
- Permanenza / intromissione in applicazioni
- Sviluppo / personalizzazioni, ecc.
- Interventi in aree protette (fisiche o virtuali)

- Durata del rapporto contrattuale

“consuetudine di compresenza...”

L. Vann.

Sicurezza nel contratto: quale è il problema ?

Rilevanza della previsione / prevenzione

Una violazione di sicurezza può provenire da:

- agenti / cause esterne *o interne*

...qualcosa non ha funzionato nelle misure protettive
esiste nel ctr una chiara definizione delle responsabilità ?

- inadempimento di una parte contraente

disattenzione / errori

"culpa in vigilando" – omissione di azioni protettive

uso improprio di info riservate (*colpa grave – dolo?*)

L. Vann.

Sicurezza nel Contratto: quale è il problema ?

A) Ctr di Servizi di implementazione e gestione di

Sistemi di Sicurezza: = definire l'oggetto e responsabilità / compiti delle parti

Domanda: è un contratto di obbligazione di MEZZI o di RISULTATO ?

B) Altri contratti di Servizi:

regolare l'intromissione di un terzo (Fornitore)

nelle "mie" aree critiche

chiarire responsabilità

prevenire contenziosi

L. Vann.

...praticamente, tutti i contratti di:

- Manutenzione (HW, SW o impianti)
- Assistenza, consulenza
- Sviluppo, personalizzazione applicazioni
- Gestione continuativa di applicazioni
- System Integration
- Outsourcing di processi (di qualunque genere)

Sicurezza FISICA : *cosa vuol dire ?*

- accesso aree
 - protezione supporti
 - prevenzione incidenti (incendio, ecc.)
 - separazione fisica aree / supporti / data base
 - archivi fisici separati e protetti
 - back-up / recovery
- ... eccetera ...

Sicurezza LOGICA: cosa vuol dire ?

- barriere SW di protezione
 - chiavi accesso per livelli / log / identificativi
 - encryption / firme digitali, ecc.
 - antivirus (e simili...)
 - monitoring saltuari e periodici
 - "intrusion detection"
- ... eccetera ...

... per i CONTRATTI ...

Due Definizioni: *(al solo scopo di questa presentazione)*

❖ DATI: sequenze alfanumeriche suscettibili di elaborazione

❖ INFORMAZIONI: insieme aggregato di dati che dà a chi ne accede una notizia aggiuntiva

ESEMPI

L. Vann.

I DATI , in quanto tali, devono essere:

- memorizzabili, reperibili, gestibili
- protetti da perdite – fortuite o dolose
- accessibili solo dagli autorizzati
- recuperabili, in caso di “crash”
- protetti “in itinere” = in fase di trasmissione
- gestibili, modificabili solo dagli autorizzati (diversi livelli di autorizzazioni)

In sede di definizione contrattuale, ne consegue che:

- II COMMITTENTE deve
fissare le sue policy e specs di sicurezza (sia fisica che logica)
fissare i perimetri di azione del Fornitore – sia fisici che logici – e controllarne l'osservanza
comunicare tutte le info pertinenti
- II FORNITORE deve
adempiere a tutto quanto sopra
ruolo diverso se Fornitore di Sicurezza

Riservatezza delle INFORMAZIONI

Presupposto: le info da proteggere sono già in possesso o comunque accessibili / conoscibili

Obiettivo del COMMITTENTE:

- impedirne l'uso improprio / divulgazione

Obiettivo del FORNITORE:

- definire "quali", "come" e per quanto tempo
- assumere l'impegno e trasferirlo al personale
- mantenere il controllo

Considerazioni

A) - Sicurezza e protezione dei DATI:

in PREVALENZA problema “tecnico” di pertinenza dello “owner” del sistema

il Committente può *pretendere* solo ciò che ha definito come specs – sia fisiche che logiche, organizzative e procedurali

il Fornitore può/deve *garantire* solo le obbligazioni definite e accettate a contratto

... importanza della fase di negoziazione

Considerazioni

A) - Sicurezza e protezione dei DATI: *(segue)*

➤ contratti di sviluppo / adeguamento SW:

adeguamento a specs *fisiche e logiche* esistenti

➤ contratti di Outs. / Gestione Security

accordo su nuove implementazioni

Responsabilità: *accurata definizione contrattuale -
normalmente il fornitore dell'antifurto non può
essere responsabile se il ladro è stato più "bravo"
salvo colpa grave*

Considerazioni

B) – Riservatezza delle INFORMAZIONI:

Regolamentazione contrattuale di
comportamenti umani

definire *“quali”* info sono riservate
“tutto è riservato” equivale a “nulla...”
stabilire almeno le “tematiche” – definire le
esclusioni (es. info di dominio pubblico)

definire *“come”*: Es. *“...usando lo stesso grado*
di cura e discrezione impiegato per le proprie
info riservate” – valido se certif. Qualità

L. Vann.

Considerazioni

B) – Riservatezza delle INFORMAZIONI:
Regolamentazione contrattuale di
comportamenti umani (...segue)

Il dilemma delle “definizioni”:

RISERVATEZZA = *accesso solo agli autorizzati*

CONFIDENZIALITA' = *non divulgazione a non aut.*

... ma, chi sono gli “autorizzati” e a che cosa ?

quale il comportamento degli “autorizzati” ?

“Comportamenti Umani” = anello debole della catena...

Classificazione dei livelli di riservatezza

Procedure / norme di gestione delle informazioni

... e dei comportamenti !

L. Vann.

Considerazioni

B) – Riservatezza delle INFORMAZIONI:

Regolamentazione contrattuale di
comportamenti umani (...segue)

Trasferire validamente le obbligazioni al
personale *proprio e dei subcontractors*

In casi particolari, procedure ad hoc per il
trasferimento, detenzione e restituzione della
documentazione

Stabilire un limite temporale (es.: 2 anni dopo
il termine del contratto)

Considerazioni

B) – Riservatezza delle INFORMAZIONI: *(segue)*

Frequente sovrapposizione con “Proprietà del SW” –
due tematiche diverse e distinte
è opportuno differenziarle in contratto ...

Il problema dei “Residuals”:

*“... le idee, concetti, know-how o tecniche relativi alla
elaborazione e trasmissione dei dati potranno essere usati da
entrambe le parti, senza limitazione alcuna”*

principio riconosciuto anche dalla legge

(art. 2 Dlgs 518 / 92 “tutela del SW”)

“...non si può lobotomizzare il sistemista...”

L. Vann.

Impatto L. 675/96 – tutela privacy *(solo un esempio)*

Gestione dati personali = attività pericolosa

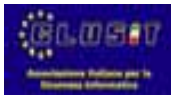
applicazione art 2050 c.c.

= inversione onere prova

= “colpa grave” estesa – impatto su limitazione di responsabilità

... a chi tocca dei due contraenti ???

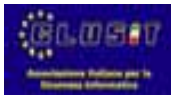
L. Vann.



Luigi Vannutelli

19

L. Vann.



Luigi Vannutelli

20