
Sicurezza ed etica nella tutela dei dati personali

maggio 2004

Gigi Tagliapietra
Amministratore Delegato Siosistemi SpA
Comitato Direttivo CLUSIT

I temi di oggi

- Il valore della sicurezza
- Le minacce
- Il codice sulla privacy
- La posta in gioco

La sicurezza è un bisogno

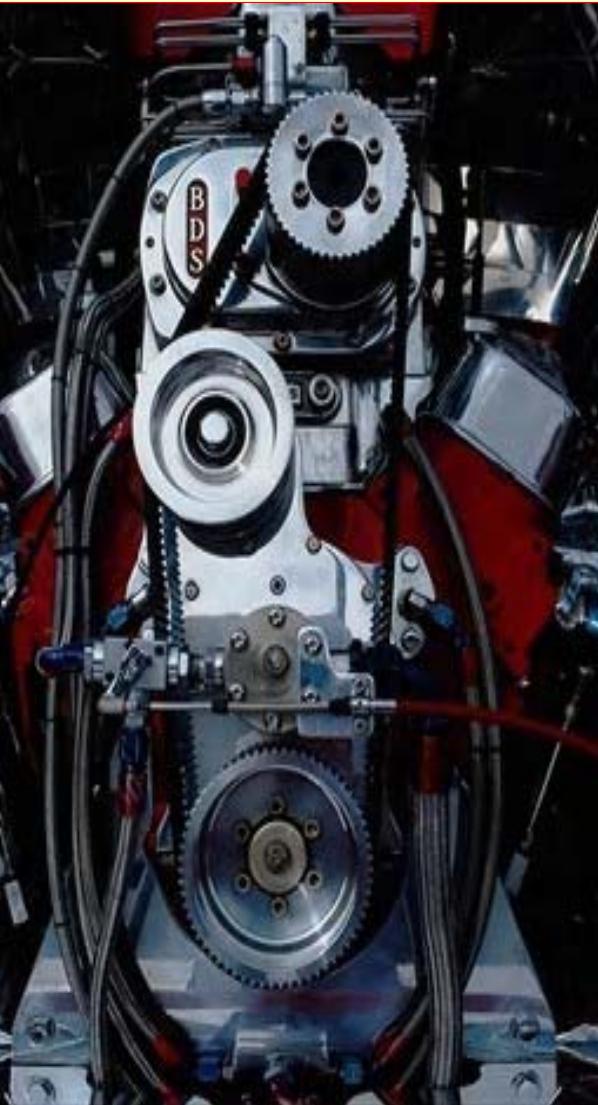


Il valore



- Sempre più le aziende vivono di informazioni
- Proteggere le informazioni vuol dire proteggere l'impresa
- Se l'informazione è seria va trattata seriamente
- La sicurezza della comunicazione digitale
 - ◆ il centro gravitazionale dell'intero sistema.
 - ◆ la condizione **affinché la comunicazione possa** non semplicemente agire, ma **essere.**

La tecnologia



- La tecnologia serve a ridurre i costi
- La tecnologia serve a fare meglio
- La tecnologia serve all'impossibile
- La tecnologia serve alla direzione

PRIMO PUNTO

**Un ambiente
sicuro
sarà sempre più
un valore primario**



Uno sguardo avanti

- HIPERMOBILE

- ◆ GSM GPRS
- ◆ UMTS
- ◆ Wi-Fi

- BROADBAND

- ◆ Canone, senza canone, gratis?

Alice

ALICE FREE ALICE MEGA ALICE FLASH SAT ALICE RICARICABILE

VANTAGGI DI ALICE
LE OFFERTE DI ALICE
VERIFICA LA COPERTURA

AREA CLIENTI

FASTWEB

Adsl SENZA CANONE

Tiscali libera anche Internet veloce

Adsl SEMPRE

On line quando e quanto vuoi

Tutto il giorno ad alta velocità

Adsl Ora Adsl Mega Adsl

CHI SIAMO

ABBONATI ONLINE

INTERNET SENZA LIMITI	TV DI FASTWEB	TUTTO SENZA LIMITI
INTERNET SUPER VELOCE 24 ORE SU 24 ORE A	LA VERA TV INTERATTIVA (CON IL CALCIO GRATIS) A SOLI	INTERNET E TELEFONO ALL INCLUSIVE!
67 EURO	30 EURO	85 EURO

Malware

- **Dai virus agli Exploit alla combinazione dei due**
 - ◆ Dialer
 - ◆ Spyware
 - ◆ Adware
 - ◆ Popups
 - ◆ Modifiche dei files di registro
 - ◆ WORM
 - ◆ NETWORK WORM

Affrontare i worm



- **Rispetto ai virus ha fattori di propagazione più alti**
- **Colpisce strutture delicate (server / apparati)**
- **Vanifica l'aumento di banda**
- **Genera crisi da infarto: passaggio repentino da funzionamento a blocco totale**

SECONDO PUNTO

**Le infezioni saranno
sempre più gravi
nessuno potrà dirsi
immune**

Nuovi obblighi



- Il codice **IMPONE** cifratura dei dati sensibili
- Il codice **IMPONE** sistemi antivirus
- Il codice **IMPONE** autenticazione
- Il codice **IMPONE** controlli perimetrali
- Il codice **IMPONE** backup e restore
- Il codice **IMPONE** un documento (DPS) con l'analisi dei rischi
- Il codice **IMPONE** misure minime e organizzative

La specificità della sanità



■ TRATTAMENTO DI DATI SENSIBILI

- ◆ Identificazione certa dei soggetti
- ◆ Crittografia dei dati
- ◆ Rendicontazione delle misure

■ NECESSITA' DI APERTURA

- ◆ Rapporto con le istituzioni
- ◆ Rapporto con il territorio
- ◆ Rapporto con i singoli utenti

Sicurezza Attiva



- **Non reagisco: mi attrezzo**
 - ◆ Miglioro le mie difese
 - ◆ per essere meno attaccabile
 - ◆ per portare il nemico sul mio terreno
 - ◆ gestisco attivamente il processo
- **Sicurezza = vantaggio competitivo**
 - ◆ abilita il mio business
 - ◆ da adempimento a disciplina
- **Devo → Voglio**

TERZO PUNTO

**Devo tutelare le
informazioni perché
me lo impone la legge**

**oppure perché ritengo
sia un mio dovere
primario**

La posta in gioco



- **Non sono in gioco i bit e i bytes**
- **E' in gioco il sistema nervoso dell'impresa**
- **E' in gioco la difesa della nostra privacy**
- **Non basta la tecnica**
- **Occorre organizzazione**
- **Non basta la buona volontà**
- **Occorre la disciplina**

Un punto di vista



- La sicurezza non esiste
- La sicurezza è un'emozione
- E' un ossimoro
- Richiede coerenza
- E' la gestione di un rischio

Innanzitutto sicurezza perimetrale



- Proteggere dall' "esterno"
 - ◆ "il lupo è spesso in mezzo al gregge"
- Proteggere zone sensibili all'interno
- Le VPN: il "perimetro" non finisce al firewall, l'azienda si estende ai clienti e ai partner
- Il problema della "sorveglianza delle mura": monitoraggio e allarmi

AAA



- **Verifica dell'Identità presentata**
(Chi Sei ?)
Authentication
- **Cosa può fare sulla/della risorsa**
(Che permessi hai ?)
Autorizzazione
- **Registro "il fatto"**
(data, ora, login, IP ..)
Accounting

Autenticazione: Chi sei?



- Non si tratta solo di permettere l'accesso ai sistemi
- Si tratta di identificare ruoli/funzioni
- Trovando i modi più efficaci per
 - ◆ Utenti interni
 - ◆ Partner esterni
 - ◆ Pazienti
- Non dimenticando le applicazioni

Niguarda



- **AUTENTICAZIONE PER ACCESSO ALLE CARTELLE CLINICHE E RADIOGRAFIE**
 - ◆ Accesso web per i medici
 - ◆ Il sistema paziente/medico
 - ◆ L'interazione con il sistema sanitario
 - ◆ La protezione degli investimenti applicativi

Auditing



■ QUANTO SONO
DEBOLE?

Rafforzamento

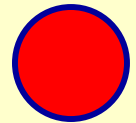
■ **COME POSSO
ESSERE PIU'
FORTE?**



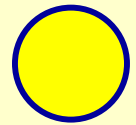
Cosa dare in esterno



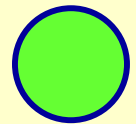
1. Responsabilità



2. Rischio



3. Gestione



Il fattore tempo



- Il codice sulla privacy impone tempi stretti e scadenze precise
- Ci sono ritardi “storici” da recuperare
- Soluzioni affrettate possono essere altamente insicure

Il fattore costo



- Dovendo affrontare in simultanea tanti temi, i costi iniziali possono essere alti
 - ◆ **COSTI**
 - ◆ La gestione dei sistemi
COSTA
 - ◆ Spiegare modelli diversi
COSTA
 - ◆ La sicurezza “insicura”
COSTA MOLTO
 - ◆ **ORGANIZZAZIONE**
 - ◆ Numero di utenti vs. investimento
 - ◆ Tempi di attivazione
 - ◆ Budget
- Dovendo garantire la sicurezza nel tempo, occorre una visione progettuale per evitare alti costi di gestione

Competenza



- L'ombrello che ripara dalle scottature
- La necessità di usare al meglio le funzioni dei prodotti migliori
- La garanzia di efficacia nei progetti in outsourcing
- La sicurezza nella traduzione delle policies aziendali nelle implementazioni sul campo

Sicurezza e etica



- Sicurezza non per paura
- Sicurezza non per chiudere

- **SICUREZZA PER
DARE SICUREZZA**



**La sicurezza
è fondamentale
una questione di
persone**

Grazie per l'attenzione

gigi@siosistemi.it