

CLUSIT- Associazione Italiana per la Sicurezza Informatica

Focus sulla fornitura MSSP e Servizi SOC
Il caso I.NET, gruppo British Telecommunications Plc

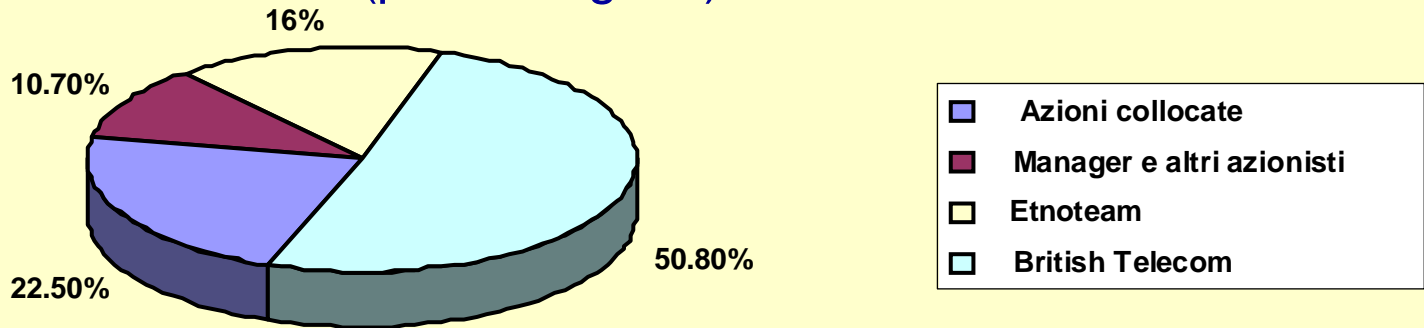
Stefano Quintarelli
16 giugno, 2003



Associazione Italiana per la
Sicurezza Informatica

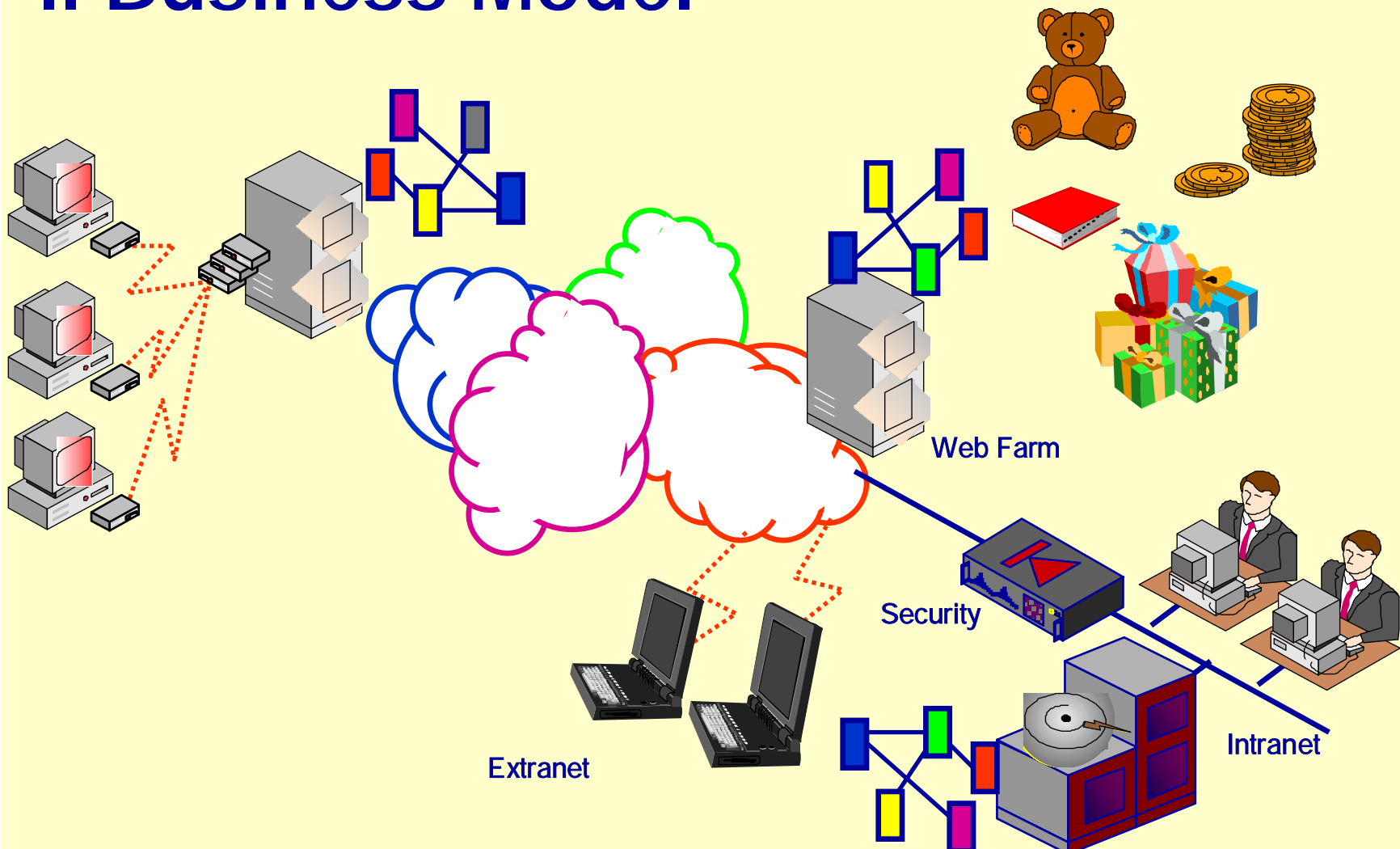
I.NET

- Nata nel giugno 1994, quotata al Nuovo Mercato (IPO: 4/00)
 - ◆ 58 M€ di ricavi
 - ◆ 240 Persone, elevata scolarizzazione
 - ◆ Controllata da BT (parte di Ignite)

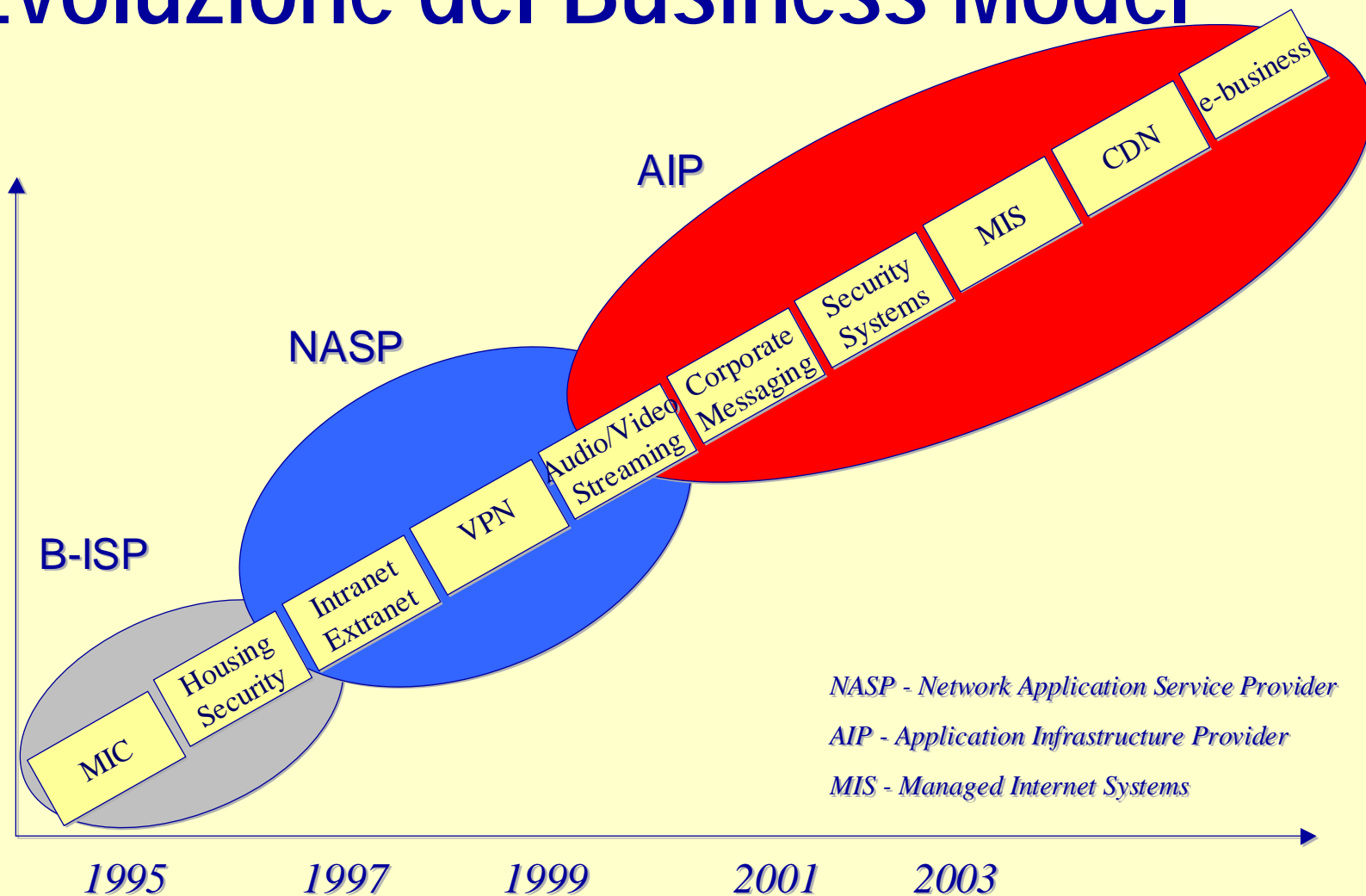


- Focalizzata sul segmento LOMO (Large Office Medium Office)
- Primo AIP (Application Infrastructure Provider) italiano

Il Business Model



Evoluzione del Business Model

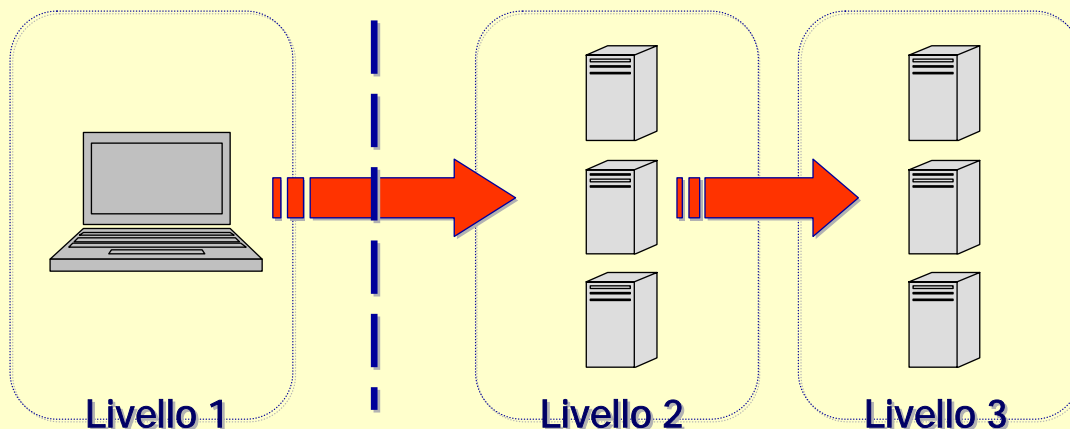


Le dimensioni

- >1800 Clienti di cui >200 per outsourcing security
 - ◆ >2200 server in WF
 - ◆ >570 rack
 - ◆ Customer Retention Rate > 80%
- Dependability:
 - ◆ >200 fault di rete al mese gestiti verso i fornitori
 - ◆ >2800 trouble ticket chiusi al mese
 - ◆ >3000 punti di rete privata virtuale (fix o mobile)
 - ◆ >350 firewall
 - ◆ >3500 router

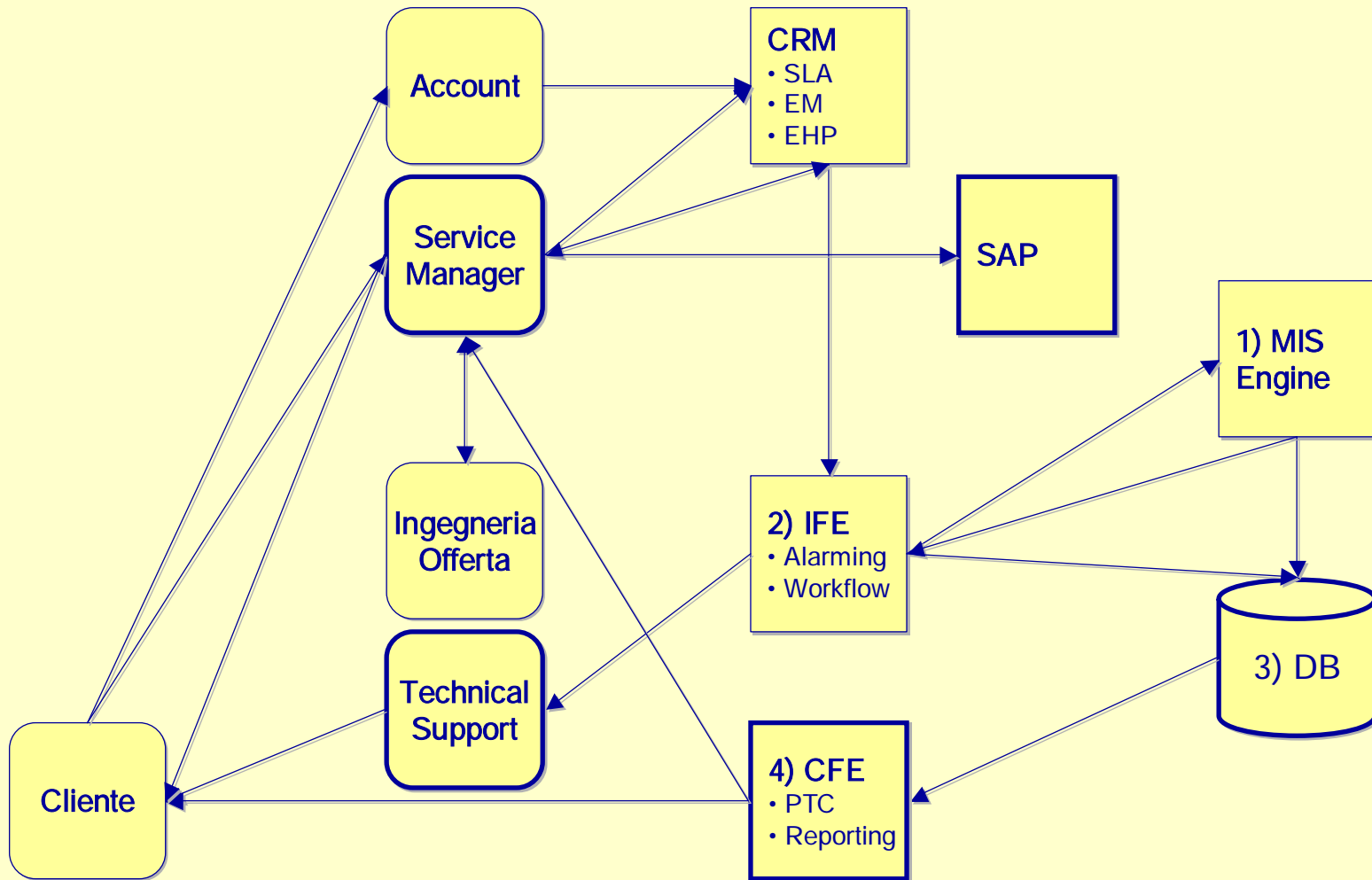
I.NET Security Operations Center

- Il modello architetturale del SOC I.NET è costituito da tre distinti livelli:



- Completa ridondanza, grazie alla struttura client-server in High Availability esistente tra il livello 2 e il livello 3
- Sicurezza, garantita dall'accesso via SBC integrato con strong-authentication

Organizzazione e Processi



Proposta I.NET per la Security

- I Security Operation Center
 - ◆ Servizi I.NET in Outsourcing
 - ◆ Realizzazione SOC per Clienti
- I servizi Managed Security del portafoglio I.NET prevedono:
 - ◆ Managed Firewall
 - ◆ Managed VPN
 - ◆ Managed Strong-Authentication
 - ◆ Managed Intrusion Detection System
 - ◆ Managed Antivirus
 - ◆ Managed URL Filtering
 - ◆ Progetti Speciali
- I.NET, con dei partner, fornisce servizi non tecnologici, quali consulenza tecnologica e legale, copertura assicurativa.

Proposta I.NET di eSourcing

- Focalizzazione su
 - ◆ Sistemi basati su open standard
 - ◆ Reti IP
- Attività
 - ◆ **Analisi** dell'infrastruttura
 - ◆ **Monitoraggio** dei sistemi per ottimizzarne il funzionamento
 - ◆ **Notifica al Cliente** dei disservizi per permettergli di intervenire tempestivamente
 - ◆ **Event handling** per ripristinarne il regolare funzionamento
 - ◆ **Reporting** dello stato dell'infrastruttura e degli interventi compiuti da I.NET
- SLA e SLG

Esempi di SLA

■ dependability dell'infrastruttura

Elemento di servizio	Dependability
I.NET Managed Infrastructure	
• Internet Connectivity	99,8%
• Web Farm Network	99,99%
• Systems	99%

■ tempi di intervento

Livello	Severity	Target Risposta	Target Chiusura
1	Elevata	30 minuti	4 ore
2	Intermedia	1 ora	8 ore
3	Bassa	1 ora	1 giorno

Esempi di SLG

- ◆ dependability dell'infrastruttura
 - ★ 4% per ogni decimo di punto % di scostamento dalla soglia
 - ★ ammontare complessivo massimo pari al 20% del canone annuo
- ◆ tempi di intervento

Livello	Severity	% risposta	Tempo risposta	Penale
1	Elevata	99%	30 minuti	1000 Euro per ogni punto % di scostamento dalla soglia
		100%	1 ora	2000 Euro per ogni punto % di scostamento dalla soglia
2	Intermedia	95%	1 ora	500 Euro per ogni punto % di scostamento dalla soglia
		100%	2 ore	1000 Euro per ogni punto % di scostamento dalla soglia
3	Bassa	95%	1 ora	250 Euro per ogni punto % di scostamento dalla soglia
		100%	2 ore	500 Euro per ogni punto % di scostamento dalla soglia

Esempio di Calcolo

■ Formula:

$OreDependabilitySLG = OreDempendabilitySLA - OreFermiconcordati - OreFermiforzamaggiore$

$$ValorePenale = ValoreContratto * \% Penale \left[\frac{(OreDependabilitySLG - OreDependabilityreali)}{Oreannue} \right]^{-1}$$

■ Esempio numerico:

- ◆ SLA del 99,7% sulla disponibilità dell'intera infrastruttura
- ◆ Penale del 4% per ogni decimo di punto di scostamento dalla soglia
- ◆ Dependability reale del 99,5%
- ◆ Fermi concordati per 0,1% annuo
- ◆ Contratto a canone annuo di 100.000 Euro

■ Valore penale = 4.000 Euro

Un esempio di Progetto Speciale

- Un Cliente I.NET (multinazionale leader nel proprio settore) ha subito un tentativo di Netstrike. I.NET in questo caso:
 - ◆ ha rilevato l'intenzione del Netstrike
 - ◆ ha approntato una struttura custom di Intrusion Detection:
 - ★ attivo
 - ★ con software ad-hoc
 - ◆ ha effettuato una difesa H24 nei giorni dell'attacco:
 - ★ segnalazione H24 di allarmi alla polizia di stato
 - ★ gestione specialistica H24 dell'IDS
 - ◆ dopo l'attacco ha effettuato una revisione complessiva dell'infrastruttura di security del Cliente

Conclusioni

- Flessibilità: accesso all'innovazione e adozione granulare
- Efficienza: economie di scala date dalla gestione svolta da un gruppo di specialisti I.NET per molte aziende differenti
 - ◆ lato conoscenze
 - ◆ lato costi (H24)
- Efficacia: aumento della funzionalità complessiva dell'infrastruttura determinato
 - ◆ dalla qualità della piattaforma di monitoraggio e gestione
 - ◆ dalla professionalità costantemente aggiornata degli specialisti I.NET
- Governance: con le adeguate garanzie contrattuali
 - ◆ Focus del Cliente su requisiti e verifica
 - ◆ Focus di I.NET sulla esecuzione

stefano@inet.it