La rete TACS non è abbastanza protetta

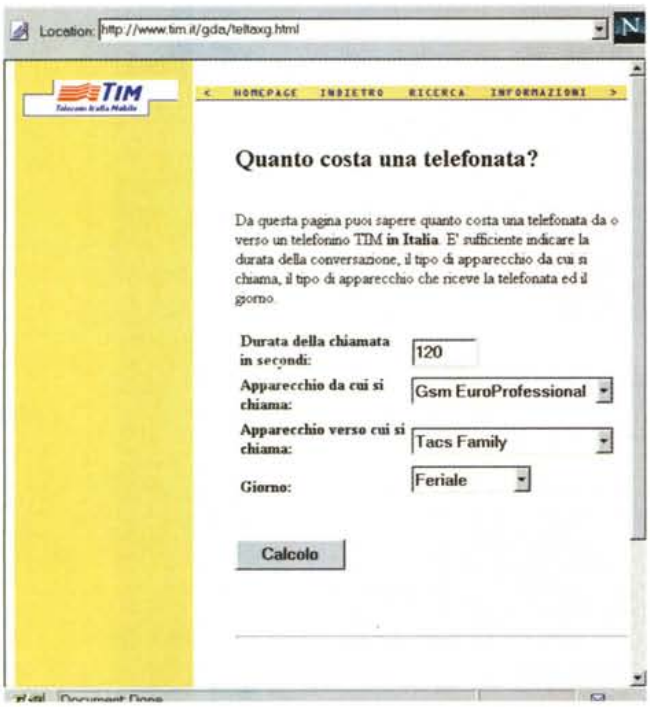
Cellulari clonati un rischio inevitabile?

Chi ha un cellulare TACS è sempre esposto al rischio che qualcuno duplichi i numeri del suo telefonino e se ne serva per chiamate internazionali. Una bella seccatura, anche se non c'è un danno economico diretto. Che cosa si dovrebbe fare per diminuire l'incidenza di un fenomeno troppo diffuso?

di Manlio Cammarata

Provate a dire a qualcuno a cui è stato clonato il telefono cellulare che il "phone phreaking" è bello, socialmente utile e che aiuta a migliorare la tecnologia. Molto probabilmente riceverete una risposta irriferibile. Ma se andate a vedere su Internet nei numerosi siti che trattano questa materia resterete perplessi e sarete tentati a dare ragione a chi afferma che la Rete è un covo di delinquenti. Naturalmente i cultori di questa diffusa attività si offendono se qualcuno li tratta da criminali e cercano di distinguere chi si inserisce abusivamente nelle reti telefoniche per il puro gusto della sfida tecnologica da chi lo fa a scopo di lucro. La realtà è una sola: l'utilizzo illegittimo delle risorse di una rete di telecomunicazioni è ovunque un reato e provoca comunque danni ingenti alle società telefoniche. Che queste trovino poi uno stimolo a migliorare i sistemi di sicurezza è tutto da dimostrare, come vedremo tra poco.

Sul sito di Telecom Italia Mobile c'è un servizio per il calcolo delle tariffe a seconda dei tipi e degli orari di collegamento: http://www.tim.it/gda/teltaxg/html.



Un sistema insicuro all'origine

I telefoni cellulari attualmente diffusi in Italia appartengono a due diverse categorie: quelli che funzionano sulla "vecchia" rete analogica, secondo lo standard TACS (o più esattamente ETACS, *Extended Total Access Communication System*), e i più recenti GSM (*Global System for Mobile communication*), completamente digitali. Degli oltre quattro milioni di telefonini in funzione in Italia la maggior parte è ancora TACS e fa capo all'unica rete disponibile, gestita da TIM (Telecom Italia Mobile); per i GSM ci sono invece due gestori in concorrenza: la stessa TIM e Omnitel, che ha Olivetti come azionista di riferimento.

Lo schema generale di funzionamento è identico per TACS e GSM: il territorio servito è diviso in piccole zone, dette "celle", ciascuna servita da una stazione ricetrasmittente (una descrizione dettagliata è su MCmicrocomputer n. 131, luglio-agosto 1993). Le stazioni base (BTS, *Base Transceiver Station*) sono raggruppate da centri di controllo distribuiti sul territorio (BSC, *Base Station Controller*) e tutti fanno capo ai sistemi di smistamento (MSC, *Mobile Service switching Centre*). Ci sono poi alcuni registri centrali che contengono l'elenco degli apparati abilitati, la loro posizione momentanea e così via. La principale differenza tra i due sistemi, oltre al funzionamento analogico o digitale, è nella capacità: a parità di numero di canali, il sistema GSM consente di servire un numero di apparati mobili otto volte più grande.

L'elemento più delicato del sistema è l'identificazione del radiomobile, che serve non solo a consentire l'accesso alla rete, ma anche per le complesse procedure di *roaming* e *handover*, che consistono nel passaggio da una cella all'altra e da un canale all'altro quando il radiomobile si sposta. La

rete identifica l'apparato sulla base di due numeri: uno è il "seriale" del singolo apparecchio, e dovrebbe essere segreto, l'altro è il numero di utente assegnato dal gestore del servizio. Si tratta, in sostanza, di un codice di autenticazione a doppia chiave. E' chiaro che se si conosce la coppia seriale-abbonato appartenente a qualcuno e si ha la possibilità di cambiare il seriale di un telefonino, magari rubato, si può telefonare a spese del legittimo titolare dell'abbonamento.
Questo è enormemente più facile nel sistema analogico. Infatti nel TACS il numero seriale è scritto in una memoria interna del telefonino, mentre nel GSM risiede nella "card" che viene consegnata dal gestore all'abbonato. Inoltre, per attivare un apparecchio GSM è necessario inserire, ogni volta che si accende l'apparecchio un codice segreto (PIN, *Personal Identification*

Era venerdì 17 (diario di un utente clonato)

Venerdì 17 gennaio. Il telefonino squilla e una voce femminile dice: "Qui è Telecom Italia Mobile, il suo telefonino è stato clonato. Riceverà un telegramma che le spiegherà che cosa deve fare".
Martedì 21 gennaio. Siccome non è arrivato nessun telegramma, chiamo il 119: "Sì, il suo telefonino risulta clonato, strano che non le sia arrivato il telegramma. Provvediamo subito".
Giovedì 23 gennaio. Nessun telegramma. Vado al Commissariato di Polizia e presento un esposto.
Venerdì 24 gennaio. Mattina. Nessun telegramma. Chiamo allora l'ufficio stampa di TIM: "Strano che non ti sia arrivato il telegramma. Comunque devi andare a via di Tor Pagnotta per vedere il tabulato e devi fare una denuncia". Poi l'addetto stampa mi spiega come sono bravi a scoprire le clonazioni.
Pomeriggio. Arriva una telefonata da TIM: "Se ci dà l'indirizzo le mandiamo il telegramma e anche il tabulato".
Sabato 25 gennaio. Arriva il telegramma. Spiega che "a seguito anomalie traffico telefonico relativo all'utenza..." devo cambiare numero di abbonato o il seriale del telefonino. Devo rivolgermi a uno dei centri di assistenza, poi definiti "negozi", dove provvederanno gratuitamente alla variazione. Nessun tabulato.
Martedì 28 gennaio. Opto per il cambio del seriale, perché dovrei informare troppe persone del cambio del numero. Porto il telefonino a un centro di assistenza autorizzato dal fabbricante.
Giovedì 30 gennaio. Ritiro l'apparecchio: 90.000 lire per il cambio del numero seriale, la sostituzione dell'antenna e l'aggiornamento del software. Poi vado nel più vicino negozio TIM per chiedere la variazione: "Spiacenti, non siamo abilitati". Provo con altri negozi, e al terzo tentativo ne trovo uno "abilitato". Riempio un modulo, presento un documento di riconoscimento, il telegramma e il foglio dell'assistenza con il nuovo numero seriale. Intanto decido di stipulare un abbonamento al GSM, visto che fino al 31 gennaio TIM lo offre completamente gratis a chi sceglie di pagare con la carta di credito. Dopo una lunga attesa arriva la conferma del cambio del seriale e il modulo per l'abbonamento al GSM. "Il sottoscritto dichiara di conoscere e accettare incondizionatamente e senza riserve tutte le Condizioni di Abbonamento al Servizio GSM, che gli sono state consegnate e che ha sottoscritto contestualmente al presente modulo". Quali condizioni? Mistero, il negoziante non ha nessun contratto da consegnarmi. Guardo meglio e scopro che c'è una voce "Ant. Conv. Int. 500.000" - TOTALE 500.000. Ma non dovrebbe essere tutto gratis? "Non si preoccupi, è un errore del computer, l'abbonamento è tutto gratis". Invece mi preoccupo e rifiuto il contratto, restituendo la card e la busta ancora sigillata con il PIN. "Ormai è tardi, torni domani mattina".
Venerdì 31 gennaio. Mattina. Il telefonino non funziona ancora. Torno al negozio, dove mi dicono che il contratto è stato annullato. "Ne facciamo un altro". Ecco un altro modulo come il primo, ma qualcosa non va, pare che TIM non dia conferma. "Venga nel pomeriggio, proveremo di nuovo". Chiedo perché il telefonino TACS non funziona ancora: ci vuole un po' di tempo, è come una nuova attivazione. Comunque, verifichiamo". Aspetto una buona mezz'ora, poi mi passano un *cordless*: "TIM vuole parlare con lei". Una gentile signorina, che dice di essere "Milano 388", si informa del mio caso e cerca di parlare con Roma, ma da Roma nessuno risponde (nota: tutto questo si svolge a Roma...). Mi assicura che farà il possibile e mi chiede un numero di telefono per darmi informazioni appena possibile.
Intanto è arrivato un telegramma da TIM. E' il primo, risulta spedito da Roma il 18 gennaio alle 9.30, ma sulla busta c'è scritto che alle 16.53 il fattorino non ha trovato nessuno. Oltre sette ore per recapitare un telegramma sono molte, due settimane non sono un po' troppe?
Pomeriggio. Torno al negozio TIM dove compero un GSM (intanto il TACS è sempre muto), e riparte la procedura di abbonamento. Dopo un'ora di attesa non c'è ancora il numero. Torno a casa e trovo nella segreteria telefonica un messaggio della simpatica "Milano 388", che mi informa che è tutto a posto. Poi arriva il fax del negozio, con il cosiddetto "contratto" del GSM e il nuovo numero.
Sabato 1 febbraio. Mattina. Il TACS è sempre fuori servizio (quinto giorno), il GSM non è ancora attivo. Chiamo il 119 (sempre da Roma), e questa volta risponde il centro di Palermo. La signorina indaga e scopre che non mi hanno cambiato il seriale, ma il numero di abbonato. Per forza non funziona! Torno al negozio (dove da giovedì ho trascorso parecchie ore) dove mi spiegano che ormai il vecchio numero è disattivato e devo tenermi il nuovo (quale? nessuno me lo ha comunicato). Faccio il diavolo a quattro. Mi fanno riempire di nuovo il modulo per la variazione del seriale, chiamano di nuovo TIM: dopo una mezz'ora il TACS è finalmente on-line con il vecchio numero e le internazionali disattivate, perché non mi hanno comunicato un nuovo PIN.
Pomeriggio. Il GSM è ancora muto. Chiamo ancora il 119, per sentirmi dire che ormai dovrò aspettare fino a lunedì. Ma alle 23.15 il telefonino emette tre gioiosi "beep" ed entra in servizio.
Giovedì 6 febbraio. E il tabulato? Seguo il consiglio dell'ufficio stampa e vado alla sede TIM di via di Tor Pagnotta, cioè in capo al mondo, sessanta chilometri tra andata e ritorno. Dove un cartello informa che gli uffici non sono aperti al pubblico. Un usciere mi dice di "compilare un modulo, sarà richiamato entro 24 ore".
Venerdì 7 febbraio. Nella buca delle lettere trovo due "Postel" provenienti da TIM. Identici. Mi ringraziano per aver scelto i servizi di Telecom Italia Mobile e mi spiegano che nella prima bolletta troverò gli addebiti per il contributo attivazione e il minimo anticipo interurbano (alla faccia del GRA-tis dell'irritante pubblicità). Le due missive differiscono per un piccolo dettaglio: una riporta il numero del mio GSM, l'altra quello della prima richiesta di abbonamento, quella che avevo rifiutato perché prevedeva l'anticipo di 500.000 lire!
Giovedì 13 febbraio. Invio a TIM una raccomandata con avviso di ricevimento, con le opportune proteste e diffide, e la riserva di richiesta di risarcimento dei danni.
Venerdì 14 febbraio. San Valentino. E il tabulato?

Manlio Cammarata (continua)

Number), che in sostanza funziona come quello del Bancomat. E c'è una differenza fondamentale: nel TACS le comunicazioni funzionano in chiaro, mentre nel GSM tutto è cifrato con algoritmi quasi inviolabili. Questo significa che per impadronirsi della coppia seriale-abbonato di un TACS basta intercettare una chiamata con uno *scanner* sintonizzato sul canale di scambio dei dati, mentre col GSM si ottiene solo un'inutile sequenza di bit in codice. Inoltre, mentre cambiare il seriale su un telefonino TACS è relativamente semplice, per falsificare un SIM occorre un'apparecchiatura molto costosa e praticamente introvabile anche per i delinquenti. Questo spiega anche perché i non rari casi di clonazioni in serie, originati dalla diffusione delle coppie da parte di dipendenti infedeli della società concessionaria, riguarda solo la rete TACS.
C'è da aggiungere, per completezza di cronaca, che anche il GSM è soggetto a una forma di truffa, che peraltro danneggia solo il gestore: la sottoscrizione di un abbonamento con la presentazione di un documento di identità falso, resa a volte possibile dalla disinvoltura con la quale operano le strutture commerciali, che si preoccupano solo di aumentare il numero dei clienti.

Corasaniti: il "phone phreaking" all'italiana

Il dottor Giuseppe Corasaniti, sostituto procuratore presso la Pretura circondariale di Roma, è una figura nota ai lettori più affezionati di MCmicrocomputer. Infatti, per la sua conoscenza della materia, è il magistrato più attivo sul fronte del crimine telematico. Ora l'argomento dell'intervista è il "phone phreaking", sul quale Corasaniti rivela aspetti preoccupanti.

Dottor Corasaniti, come lavorano i clonatori italiani?

Più o meno come quelli di tutto il mondo. Basta fare una semplice ricerca su Internet, sull'espressione "phone phreaking" per avere tutte le indicazioni al riguardo.
Sostanzialmente ci sono diversi metodi di clonazione. Il primo è quello dello hacking classico: uno si introduce nel sistema informativo del gestore e scarica a blocchi le coppie numero seriale - numero di abbonato, poi le rivende. Sul "mercato" un numero costa in media 100.000 lire. Con questa cifra ci si assicura un discreto periodo di uso abusivo, perché in molti casi la vittima non si accorge della clonazione fino a quando non riceve una bolletta stratosferica. C'è da aggiungere che si verifica anche qualche caso di clonazione passiva, perché il telefono "clone" viene usato anche per ricevere, con una complicata procedura che disabilita il telefonino clonato. Basta leggere il "manuale del phreaker", liberamente disponibile in rete...
Poi c'è il metodo diretto, l'acquisizione dei numeri alla fonte. E' stato accertato più volte a Roma e recentemente anche a Napoli, dove un signore, dipendente di TIM, è stato arrestato con un suo bravo CD-ROM, sul quale aveva scaricato la bellezza di 500.000 numeri. I phreaker italiani sono molto scrupolosi, perché dividono in numeri per zone, per tipo di utenza e così via. Il primo caso di acquisizione diretta, accertato tempo fa a Bologna, avvenne per colpa degli uffici del gestore, dove periodicamente si buttavano via i tabulati di back-up, e i soliti ignoti si presentavano regolarmente a... ritirare la spazzatura. Naturalmente la procedura è stata cambiata. I primi clonatori organizzati lavoravano proprio con questi metodi, poi le procedure sono state rese molto più sicure e anche i pirati si sono dovuti adeguare.

E sono passati all'intercettazione...

Sono passati dal sistema "fisico" ai sistemi di tipo intercettativo. Che è molto comune negli Stati Uniti, dove non c'è ancora un sistema diffuso di telefonia mobile digitale, e quindi sufficientemente sicuro. Gli USA sono la patria della clonazione, al punto che, come si vede anche nei telefilm, gli agenti di polizia e i magistrati non usano il cellulare, ma i cercapersone, perché i telefonini sono troppo insicuri. Il sistema importato dagli Stati Uniti è basato su scanner sofisticatissimi che lavorano sul canale dei dati invece che su quello della voce, e spesso sono collegati a un PC portatile. Il signore si piazza in un punto qualsiasi, preferibilmente nei pressi di una cella e "fotografa" tutto il traffico. E' chiaro che ci sono numeri più appetibili di altri: quelli dei professionisti che usano molto il telefono, o delle società, soprattutto se fanno traffico internazionale e quindi è difficile accorgersi subito di un aumento delle chiamate.
Ma la pirateria telefonica non riguarda solo il traffico internazionale. Ci sono anche le truffe con il vecchio sistema inaugurato anni fa con il Videotel da società fantasma che usano telefonini clonati per chiamare i propri numeri "166" e riscuotere i proventi delle chiamate fittizie.

Però ora anche l'abilitazione al 166 deve essere richiesta espressamente dall'abbonato.

In conclusione, il sistema TACS è intrinsecamente insicuro contro le clonazioni, dal momento che non esiste nessuna forma di protezione della chiave di identificazione dell'apparato mobile.

Una password troppo semplice

C'è ancora un aspetto importante: le clonazioni non sono opera di individui isolati, phreaker più o meno in buona fede, extracomunitari disperati perché costa troppo restare in contatto con le famiglie lontane. La clonazione dei telefonini è un'attività su scala industriale, condotta da organizzazioni criminali ben dotate di mezzi, che ne ricavano utili ingenti a causa del costo elevato delle chiamate internazionali. Ma, dirà qualcuno, c'è il blocco affidato alla password di quattro cifre, che l'abbonato deve inserire per abilitare le telefonate all'estero. E qui, come si suol dire, casca l'asino.
Infatti una password di quattro numeri permette solo 9.999 combinazioni: uno scherzo per un PC collegato a un telefono cellulare e un apposito

Per arrivare a questo punto è stata necessaria una lunga battaglia, perché i servizi col prefisso 166 sono quelli di utilità sociale. C'è anche da discutere sulla classificazione dei servizi, perché ho qualche dubbio sull'utilità sociale di servizi tipo "la dottoressa dell'amore"... Alla fine gli unici servizi fruibili dal cellulare senza richiederne espressamente l'attivazione saranno quelli di emergenza. E' inevitabile.

Ci sono altri sistemi di pirateria diffusa?

C'è un altro aspetto pericoloso del phone phreaking: il trasferimento di chiamata. Non dobbiamo pensare che i telefonini vengano clonati da extracomunitari qualsiasi. Tra di loro ci sono tecnici qualificatissimi, ingegneri, gente di alto livello. Una volta gli apparecchi col numero clonato venivano sistemati in batterie, come centralini, e questi signori andavano a telefonare disciplinatamente, in fila, con ordinatissime sale d'attesa. Adesso è in voga il sistema del trasferimento di chiamata, che a volte per noi è un rebus, qualcosa di estremamente complicato da accertare. Succede che il cellulare clonato si trova chissà dove, e viene raggiunto con un trasferimento di chiamata, con un sofisticato sistema informatico che identifica il primo cellulare libero a disposizione. Più di qualche volta siamo riusciti ad intervenire in flagranza, ma non è facile. In un'operazione dell'anno scorso abbiamo accertato che le telefonate partivano da Roma, dalla zona della stazione Termini, però i cloni erano un gruppo in Olanda e un gruppo in Austria. Lì sono stati arrestati in flagranza di reato, in Italia sarebbero stati denunciati a piede libero e avrebbero ripreso l'attività dal giorno stesso.

Resta il fatto che le chiamate internazionali dovrebbero essere protette dal codice di quattro cifre, il PIN, che la società assegna ad ogni utente e che deve essere inserito per abilitare i prefissi che iniziano con due zeri.

In effetti in un primo momento Telecom aveva abbattuto il numero delle clonazioni ricorrendo al PIN. Ma il problema è che per il PIN si scelgono spesso sequenze numeriche ovvie, cioè di quattro cifre uguali o in sequenza, come 1234, che sono facili da ricordare e che sono anche le prime tentate dai programmi di ricostruzione delle password. Un noto phreaker mi ha detto durante un interrogatorio: "Noi andiamo su base statistica, su diecimila tentativi otteniamo quei cento numeri che ci servono per un pezzo". E questo statisticamente è vero.

Ma non c'è un sistema che dopo un certo numero di tentativi abbatte il collegamento e segnala il fatto?

Dovrebbe essere in fase di attivazione un sistema più sicuro di controllo degli accessi alla rete, ma il problema è che nel settore manca un organismo indipendente di verifica dei livelli di sicurezza, come l'Istinform per le banche, e manca anche la concorrenza, che potrebbe essere fondata anche sull'offerta di maggiori livelli di sicurezza. Non dimentichiamo che c'è anche il sistema, sempre buono, del furto o della falsificazione delle carte di credito telefoniche. Un'altra variazione che ci preoccupa riguarda il GSM, si cerca di rubare fisicamente la card o di falsificarla. Per fortuna i duplicatori di SIM card sono rarissimi e molto costosi, ma fino a qualche tempo fa era impensabile che si potesse duplicare perfettamente un CD audio o un CD ROM e oggi chiunque lo può fare con una macchina che costa meno di un milione. E nel prossimo futuro sorgeranno anche i problemi delle frodi sulla televisione a pagamento e su ogni altro servizio a tecnologia avanzata. Il fatturato di queste attività è di centinaia di migliaia di dollari e i danni ricadono su tutte le compagnie telefoniche.

Quali sono le possibilità di difesa?

Il problema è che l'organizzazione pubblica per l'accertamento e la repressione dei reati informatici deve essere sempre all'altezza della situazione, bisognerebbe aggiornare continuamente le norme e le procedure. Non dimentichiamo che in Italia tra poco questo tipo di reati riguarderà anche le norme sulla protezione dei dati personali. La cattura, con qualsiasi sistema, dei numeri seriali e dei PIN sarà una violazione della riservatezza delle persone e bisognerebbe chiedersi se gli attuali sistemi di protezione impiegati dalle varie società danno le garanzie di sicurezza previste dalla legge 675/96. Qualcosa dovrà cambiare.

programma che le prova una per una. Tanto più facile se è vero che in realtà le combinazioni effettivamente usate sono molte di meno, perché vengono scelte solo sequenze facili da ricordare, come 1234 o 9991. Resta una curiosità: perché TIM non adotta un programma che blocca l'accesso dopo un certo numero di tentativi con codici errati? Questa soluzione è presente in qualsiasi sistema di controllo basato sull'inserimento di una password ed è molto efficace.
Secondo il gestore della rete TACS c'è una procedura automatica di verifica, che ogni quindici minuti controlla tutte le utenze e segnala, su base statistica, le anomalie del traffico. Quando c'è un'impennata improvvisa rispetto all'uso abituale che un singolo utente fa del telefonino, scatta l'allarme. L'interessato viene avvertito e deve cambiare numero di telefono, o il seriale dell'apparecchio, sporgere una denuncia e quindi esaminare i tabulati per disconoscere le telefonate che non ha fatto. Il danno economico ricade interamente sulle spalle dell'azienda, che deve comunque pagare ai gestori esteri le tratte internazionali, ma per l'utente è un fastidio e una perdita di tempo non indifferente.
Resta da considerare un fatto: tra qualche mese, quando sarà completamente in vigore la legge 675/96 sulla protezione dei dati personali, la mancata adozione di adeguate misure di sicurezza, determinate in funzione degli sviluppi della tecnologia, sarà un reato. Che il numero seriale e il PIN siano dati personali è indiscutibile. E non c'è dubbio che il controllo statistico a posteriori è irrilevante, perché i dati vanno protetti all'origine, con i mezzi, già disponibili, che oggi non vengono impiegati anche se sono universalmente diffusi.

Internet per tutti urbana e notturna?

Ultim'ora

Il sottosegretario alle Poste annuncia un progetto: Internet per tutti a tariffa urbana e sempre con gli scatti alla cadenza più lenta, quella notturna.

Roma, 14 febbraio. L'articolo che apre queste pagine di Informatica e società è già pronto per la stampa, troppo tardi per modificarlo. Ma la novità è importante e merita un'aggiunta (un grazie alla redazione per questo spazio in più), perché quello che solo "sei pagine fa" sembrava un sogno potrebbe già essere realtà mentre leggete questa nota: Internet a tariffa urbana agevolata da qualsiasi località italiana.
Lo ha detto il sottosegretario alle Poste, Vincenzo Vita, nel suo intervento alla conferenza dell'Associazione italiana Internet providers (AIIP). Il progetto, ancora non definito in tutti i particolari al momento dell'annuncio, prevederebbe l'istituzione di un "numero verde" a livello provinciale, che consentirebbe l'accesso a Internet, da qualsiasi località e a qualsiasi ora, alla tariffa della fascia più bassa della TUT, quella notturna.
Meglio tardi che mai, è il caso di dire, perché viene finalmente rimosso uno degli ostacoli più importanti alla diffusione di Internet nel nostro paese, quello del costo della chiamata, con tutte le conseguenze che si possono immaginare.
Ma non è tutto oro quello che luccica: se l'operazione partisse realmente il 1. marzo, se ne avvantaggerebbe in un primo momento solo Telecom Italia, che ha avuto tutto il tempo per preparare sia gli aspetti tecnici, sia le relative proposte commerciali. Gli Internet provider privati ne subirebbero un danno rilevante, perché per un certo periodo tutti i nuovi utenti troverebbero più conveniente l'abbonamento ai servizi Internet offerti dal monopolista. Poi, per far ricadere anche sull'Italia i vantaggi della società dell'informazione, non basta rendere più conveniente il collegamento. Occorre una politica chiara e lungimirante, che superi i ristretti limiti del dibattito attuale sulle reti di Berlusconi e della Rai, e imposti progetti di vasto respiro, che possono essere molto efficaci per creare nuova occupazione. Lo ha detto anche il commissario europeo Emma Bonino, nel suo lucido e documentato intervento alla conferenza della AIIP, del quale parleremo sul prossimo numero.
Ma il Ministero delle poste è su un'altra lunghezza d'onda: Vita è arrivato a dire che "Stati Uniti e Gran Bretagna hanno perseguito una politica protezionistica, non realizzando una vera e propria liberalizzazione, ma costituendo monopoli e rigide barriere" (testuale dalla sintesi dell'intervento). Affermazione falsa, perché in Gran Bretagna è stato favorito con regolamentazioni asimmetriche l'ingresso di nuovi operatori (mentre da noi si continua a favorire la posizione dominante di Telecom Italia) e negli USA i monopoli sono ferocemente combattuti da sempre. Insomma, scende il prezzo del collegamento a Internet e salgono l'arroganza e la cattiva informazione. Non c'è da stare allegri.

Manlio Cammarata

START™
DOING
EXTRAORDINARY
THINGS

EXTENSA 900
IL NUOVO PESO SPECIFICO DELLA POTENZA.

2,2 Kg batteria inclusa. Leggerezza, caratteristica essenziale per un mondo in cui gli spostamenti sono una componente essenziale del business e la pronta disponibilità d'informazioni è essenziale per determinare il successo.

EXTENSA 900. Lo strumento ideale. Una famiglia di prodotti dal rapporto prezzo prestazioni sorprendentemente vantaggioso che, in più, offre una carratteristica essenziale per il moderno mobile computing. La performance è eccezionale grazie al **Processore Pentium® 133 MHz** per garantire velocità di elaborazione. Memoria **RAM EDO** standard da **16 MB** espandibile a 48 per utilizzare facilmente i più sofisticati software. **HDD** da **1,35 GB standard** per gestire e archiviare i dati più complessi. Display da **12,1" DSTN** o **11,3" TFT*** per garantire ottima leggibilità. E grazie alla Mobile Productivity Base** potrete usufruire del CD ROM 8x, uno slot per APCI card, uno slot per la batteria aggiuntiva rimanendo nello standard di peso dei comuni notebook. **EXTENSA 900** eccezionale combinazione di leggerezza e potenza.

intel inside pentium

TEXAS INSTRUMENTS

* Escluso modello EXTENSA 900
** Standard sul modello EXTENSA 900 CDT

Tutti i marchi citati sono registrati dai legittimi proprietari.