



POLIZIA DI STATO

COMPARTIMENTO POLIZIA POSTALE E DELLE COMUNICAZIONI PER L'UMBRIA

Via Mario Angeloni 72 - Perugia

Tel. 075/5001703 - 5011967 Fax.075/5000655

poltel.pg@poliziadistato.it

Settore Operativo

OGGETTO:verbale di sommarie informazioni rese da: -----

Dr. RIZZO Luca, nato a Savona il 05.12.1970, residente a Finale Ligure (SV), identificato a mezzo di C.I. nr. AG 8855343 ril. dal Comune di Finale Ligure (SV) il 05.09.2003, domiciliato per l'incarico di Direttore della Sicurezza, presso la sede legale di Fastweb S.p.A., sita in Milano, via F. Caracciolo, nr. 51 tel. 02/45454270. -----

L'anno 2007 addì 16 del mese di novembre, alle ore 11.51 in Milano, Via nr., negli uffici di Fastweb S.p.A.-----

Innanzitutto ai sottoscritti Ufficiali e Agenti di P.G. Commissario Capo Filippo Bartolozzi, Sost. Comm. Giorgio Magna, Assistente Marco Capolungo ed Assistente Mirko Gregori, appartenenti all'Ufficio in epigrafe indicato, sono presenti il nominato in oggetto, il quale, in qualità di Direttore della Sicurezza Fastweb S.p.A., viene escusso per acquisire informazioni tecniche in ordine ai dati forniti dal predetto gestore telefonico, nell'ambito del p.p. nr. 9066/2007 R.G.N.R. mod. 21 iscritto presso la Procura della Repubblica presso il Tribunale di Perugia. Il signor Luca RIZZO viene reso edotto degli obblighi inerenti l'esame del testimone e, in particolare, quello di riferire secondo verità e di non nascondere nulla di ciò che è a sua conoscenza.-----

L'Ufficio, preliminarmente chiede di fornire una descrizione del funzionamento della rete clienti Fastweb, in particolare riguardo i clienti residenziali con tecnologia ADSL, e dei relativi sistemi di supporto.-----

Risposta: "Volendo semplificare, possiamo dire che il cliente, ad un primo livello, è collegato tramite un "doppino" telefonico, su tecnologia ADSL, alla centrale Telecom di appartenenza. All'interno di tale centrale, sono dislocati gli apparati di proprietà Fastweb che raccolgono il traffico generato dai clienti e lo inoltrano all'interno della rete dei clienti Fastweb. Il cliente, nella propria abitazione ha un dispositivo hardware HAG o MODEM (dipende dal servizio da lui acquistato) che gli permette di fruire dei servizi da noi erogati (VOCE, DATI, VIDEO). Una peculiarità riguarda la parte internet. Il sistema di tracciamento storico dei clienti, per motivi di natura tecnico-infrastrutturale, è dislocato presso i punti d'interconnessione della rete Fastweb verso il "mondo esterno", ovvero verso internet. Ne consegue che il traffico dati di un cliente Fastweb verso un altro cliente Fastweb non viene tracciato dal sistema di tracciamento storico, ma sarebbe rilevabile soltanto attraverso un'intercettazione telematica. Nei punti d'interconnessione, su appositi firewall, viene registrato il traffico delle singole connessioni effettuate dal cliente. Questi

AS

Luca Rizzo
Settore Sicurezza

dati sono poi raccolti in un sistema di tracciamento storico (dei dati). Nel caso di un'utente flat, non è richiesto alcun tipo di autenticazione ed il collegamento dati è sempre disponibile. Per specificare meglio, possiamo dire che non esistono log di autenticazione, in quanto il collegamento fino alla sua macchina è sempre disponibile; la sessione è aperta e Fastweb può vedere, solo se il collegamento genera traffico, quali eventi lo abbiano riguardato. Diversamente, in caso di un utente con servizio "a consumo" è necessaria un'autenticazione specifica, ogni volta che egli decide di collegarsi,."

Domanda: "Può specificare come il Vs. sistema organizza i dati e come li rende fruibili in caso di richieste dell'Autorità Giudiziaria?"

Risposta: "Il sistema si avvale di una batteria di server che ricevono i log della sessione relativa alla comunicazione che avviene tra il cliente Fastweb ed il sistema remoto. Un secondo livello di macchine si occupa della normalizzazione ed indicizzazione dei dati prima indicati. Gli stessi vengono archiviati ed è così possibile fruirne, per fornirli all'A.G., con delle apposite ricerche. "

Domanda: "Tecnicamente, come erogate il servizio ai Vs clienti ADSL?"

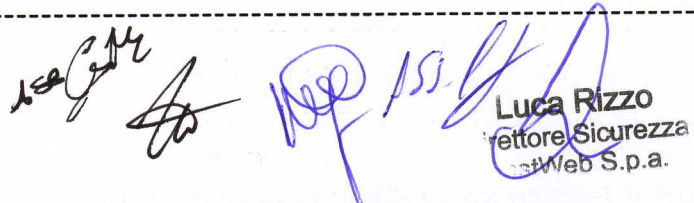
Risposta: "Il nostro cliente ADSL flat ha a disposizione tre indirizzi I.P. interni/privati. L'estrazione dei dati relativi al traffico eventualmente richiesti dall'A.G. viene effettuata utilizzando come criterio di ricerca l'indirizzo I.P. che il cliente ha utilizzato in base alle sue esigenze (esempio utilizzo di più p.c. o altri dispositivi quali video - station). E' bene specificare che nel caso in cui il nostro cliente utilizzasse uno solo dei predetti tre I.P. interni / privati noi possiamo fornire i dati relativi soltanto a quello e relativamente agli altri due avremmo delle risposte negative (visualizzabili attraverso dei tabulati dove non compaiono stringhe)."

Domanda: "Quali protocolli il Vs. sistema è in grado di tracciare?"

Risposta: "I protocolli attualmente tracciati sono il TCP e UDP, pertanto il sistema restituirà, relativamente all' indirizzo I.P. sorgente, l'indirizzo I.P. "nattato" (che è un indirizzo I.P. pubblico temporaneamente assegnato all'utente per quella singola connessione finalizzata alla navigazione all'interno del mondo internet) e relativa porta di nat, I.P. di destinazione, e porta di destinazione. Nella riga del tracciato è disponibile l'indicazione del giorno, ora d'inizio e fine della connessione (in formato ora "local", ovvero quella di Roma), quantità del traffico scambiato all'interno della connessione espressa in byte".

Domanda: "Può indicarci quali sono i servizi fruibili in internet, registrati dai Vs. sistemi, in relazione ai quali è imprescindibile la presenza di un operatore sul terminale connesso?"

Risposta: "In premessa mi preme specificare che posso rispondere solo relativamente ai servizi fruibili in rete erogati da Fastweb ai proprio clienti. Ovviamente nel fornire questa risposta bisogna tener conto che potrebbero esistere dei software i quali effettuano una sequenza automatica di operazione in tutto simile a quella posta in essere da un operatore. E' chiaro che i servizi che richiedono un'autenticazione dell'utente sono quelli in cui è imprescindibile la presenza dell'operatore. A titolo di esempio posso citare i seguenti: l'accesso alla casella di posta elettronica fastwebnet.it (ovvero quella normalmente fornita, quale servizio accessorio, a tutti i titolari di un contratto con Fastweb), accesso alla sezioni riservate del portale Fastweb (esempio conto on-line, consultazione del traffico telefonico ecct.), trasferimento di chiamata che può anch'esso essere effettuato via web, cambio di profilo tariffario".


Luca Rizzo
Direttore Sicurezza
FastWeb S.p.a.

Domanda: “in relazione ai files di log da Voi fornitici in data 10.11.2007, in parziale ottemperanza ad un apposito provvedimento dell’A.G. precedente, è stato rilevato un elevato traffico su porte riconducibili a software *peer to peer*. Può specificarci, richiamandoci a quanto già chiestoLe precedentemente, se, per quanto a sua conoscenza, tale attività possa o meno richiedere la presenza di un operatore al terminale?-----

Risposta:”per quanto a mia conoscenza, posso affermare che la presenza fisica di un operatore al terminale è ipoteticamente necessaria in una fase di ricerca e selezione del file da scaricare”. Ovviamente è possibile pianificare lo scarico di più files in periodi antecedenti. Quindi può avvenire che una persona abbia effettuato una ricerca per poi selezionare uno o più files, avviando così la fase di scarico in una determinata data, possa comportare un’attività tecnica di scarico del file che con durata indefinita. Tale attività, inoltre, può essere arrestata dallo spegnimento del p.c. e riprendere, automaticamente, al momento del suo riavvio.”-----

Domanda: “in relazione alla presenza di tipologie di traffico denominate T.C.P. ed U.D.P. è possibile associare l’utilizzo di uno in particolare di questi due protocolli alla fruizione di un determinato tipo di servizio?”-----

Risposta: “posso dire, fornendo così un’indicazione di massima, che il protocollo U.D.P. viene utilizzato nell’erogazione di servizi tipo video, voce, broadcast. Il protocollo T.C.P. invece nella maggior parte degli altri casi”.-----

Il Dr. Luca RIZZO viene reso edotto dell’obbligo di mantenere la massima riservatezza sui fatti contenuti nel presente verbale e su tutto ciò di cui è venuto a conoscenza sulle indagini in corso. -----

Il presente verbale, previa rilettura e conferma, viene chiuso alle ore 14.45 in luogo e data di cui sopra e sottoscritto dai verbalizzanti e dal signor Dr. Luca RIZZO. -----

Dr. Luca RIZZO


Luca Rizzo
Direttore Sicurezza
Web S.p.a.



Ass. M. GREGORI

Ass. M. CAPOLUNGO

Sost. C. G. MAGNA

Comm. C. F. BARTOLOZZI