VERBALE DI ACCORDO

In data 19 luglio 2011 si sono incontrate

RCS Quotidiani S.p.A. –settore Quotidiani Italia e

le **RSU RCS Quotidiani spa**

Premesso che:

- i sistemi informativi sono impiegati in tutti i processi operativi aziendali ed è opportuno adottare misure di protezione tecnico - organizzative a livello di Gruppo;
- l'azienda riconosce l'importanza dei sistemi informativi quale strumento di comunicazione e informazione e ne mette a disposizione l'accesso compatibilmente con la necessità di garantire la sicurezza e l'operatività della rete aziendale. Il loro utilizzo è consentito per scopi leciti e coerenti con il Codice Etico adottato dal Gruppo;
- in data 1° marzo 2010 è stata istituita tra le Parti una Commissione tecnica in materia di ICT;
- a tale Commissione è stato affidato il compito di approfondire le tematiche relative a un corretto utilizzo delle risorse informatiche aziendali anche per i riferimenti connessi all'art. 4 legge 300/70 Statuto dei Lavoratori e all'applicazione in sede aziendale del D.Lgs 196/03 e D.Lgs. 231/01 e successive modifiche;
- la Commissione si è più volte riunita e ha approfondito i temi oggetto dell'analisi all'interno del Gruppo RCS;
- la Commissione ha condiviso l'opportunità di introdurre delle policy aziendali al fine di tutelare al meglio il patrimonio informatico aziendale, garantire i livelli di sicurezza previsti dalla legge, l'efficienza e continuità dei servizi e dei sistemi informativi nonché l'integrità e la disponibilità delle informazioni trattate, contenere e ridurre il rischio di commissione di reati perseguibili ai sensi del D.Lgs. 231/01 e sue successive modifiche (e in particolare i delitti informatici introdotti dalla legge 48/2008 quali ad esempio: Accesso abusivo ad un sistema informatico o telematico; Diffusione di programmi diretti a danneggiare o interrompere un sistema informatico; Danneggiamento di sistemi informatici o telematici) e in genere assicurare la conformità alle normative vigenti in materia;
- la Commissione ha esaminato le policy in materia predisposte dalla Direzione ICT di cui ne viene consegnata copia;
- tra queste misure, descritte anche nei Documenti Programmatici per la Sicurezza dei dati (DPS) redatti nell'ambito del sistema di gestione della Privacy di Gruppo, si riscontra la

conduzione di attività di verifica del corretto funzionamento ed utilizzo dei sistemi informatici aziendali;

- tali attività sono necessarie a garantire la sicurezza nonché l'efficienza e continuità degli strumenti e dei servizi informatici a disposizione dei dipendenti quali strumenti atti allo svolgimento della propria attività lavorativa e sono previste allo scopo di contenere e ridurre il rischio di commissione di reati perseguibili ai sensi del D.Lgs. 231/01 e sue modifiche;
- il presente accordo si pone quindi l'obiettivo di descrivere la natura delle informazioni raccolte dai sistemi di protezione, gestione, monitoraggio ed erogazione dei servizi informatici aziendali, laddove queste possano essere rilevanti per la privacy degli utenti e soprattutto chiarirne le modalità e finalità di trattamento;
- per qualsiasi necessità di supporto e/o necessità di informazioni in ambito ICT, sia operative che tecnico-amministrative, i dipendenti continueranno a rivolgersi all'HelpDesk.

Sulla base di queste premesse,

le Parti si confermano che l'utilizzo degli strumenti e servizi informatici aziendali in quanto strumenti di lavoro è diretto allo svolgimento dell'attività lavorativa svolta a favore dell'azienda. I criteri di utilizzo degli stessi sono esplicitati in apposite policy visibili e pubblicate sul sito di Gruppo.
Le ordinarie attività tecniche di gestione volte a garantire la continuità dei servizi forniti, uniti alla necessità di assicurare la sicurezza della rete informatica aziendale, implicano per loro natura che gli utilizzatori degli strumenti informatici aziendali siano consapevoli che il personale ICT addetto (Amministratori di Sistema/Servizio) possa avere accesso controllato alle informazioni in esso contenute.

Tipologia di dati raccolti

- I sistemi che erogano il servizio di posta elettronica registrano dati in continuo sul proprio funzionamento. Tali dati contengono informazioni relative ad orario d'invio, mittente, destinatario e oggetto di ogni mail inviata o ricevuta.
  Si precisa che la suddetta attività di monitoraggio non prevede né controllo né tanto meno registrazione dei contenuti del messaggio.

- I sistemi (ad es. Firewall, Intrusion Prevention System, Content Filtering) utilizzati per proteggere la rete aziendale e monitorare la qualità del servizio erogato, rilevano l'instaurarsi e la natura delle sessioni di comunicazione tra dispositivi o utenze appartenenti alla rete stessa e risorse che risiedono al di fuori di essa. Tali sistemi registrano quindi, per esempio, il fatto che una postazione di lavoro informatica aziendale o un'utenza abbia acceduto ad un certo sito o servizio web,

quando questo è avvenuto e la quantità di dati scambiata. Inoltre tracciano, ove verificatosi, il tentativo di accedere illecitamente alla rete aziendale o ad un computer in essa contenuto.
Si precisa che non vengono effettuati registrazioni od esami dei contenuti scambiati in una sessione di comunicazione.

- I sistemi di autenticazione (inserimento di nome utente e password), che consentono l'accesso alla rete ed alle applicazioni aziendali registrano: ora, nome utente ed esito di tutti i tentativi di accesso.
  Se l'accesso avviene dall'esterno alla rete (webmail, vpn, numero verde) viene registrato anche l'indirizzo IP o il numero di telefono dal quale è avvenuto l'accesso stesso.

- E' importante notare che le informazioni suddette:

  - sono a disposizione solo di chi riveste il ruolo di Amministratore di Sistema/Servizio, individuati da un Responsabile di Settore della Funzione ICT, anche come richiesto dal provvedimento del Garante (G.U. n. 300 del 24 dicembre 2008) "Misure e accorgimenti prescritti ai titolari dei trattamenti effettuati con strumenti elettronici relativamente alle attribuzioni delle funzioni di amministratore di sistema - 27 novembre 2008" e successive modifiche;

  - sono conservate per un periodo limitato;

  - sono trattate unicamente per motivi di garanzia del buon funzionamento dei servizi;

  - sono funzionali alla tutela della sicurezza aziendale, in ottemperanza a specifiche richieste dell'Autorità Giudiziaria.

<u>Modalità e finalità di trattamento</u>

Vengono giornalmente rilasciati report diagnostici al fine di rilevare anomalie sullo stato di funzionamento della rete aziendale e dei servizi da questa erogati.
I report contengono:

- dati aggregati, che riguardano cioè la rete o uno specifico servizio nel suo complesso come, ad esempio, il numero totale di mail in ingresso e in uscita o il numero di Byte scambiati in sessioni di trasferimento file (FTP) in un giorno;
- dati statistici che evidenziano anomalie di traffico rispetto ad una situazione normale;
- dati statistici riguardanti i tentativi di intrusione effettuati, suddivisi per pericolosità;

- dati statistici riguardanti il numero di tentativi di autenticazione falliti, ovvero tentati digitando una password sbagliata.

Nel caso in cui i report dei sistemi di autenticazione evidenzino, da parte di uno specifico account utente, un notevole numero di tentativi falliti di accesso alla rete aziendale, l'utente stesso può essere contattato dal servizio di Helpdesk allo scopo di stabilire se quei tentativi siano frutto di un errore effettuato dall'assegnatario dell'account o siano invece indice di un tentativo di utilizzo fraudolento da parte di Terzi.

Quando si verifichi un'anomalia statistica, come nel caso di un'utenza che invia migliaia di mail o di una postazione di lavoro informatica che trasferisca su Internet una notevole mole di dati in un breve tempo, vengono svolte analisi tecniche di dettaglio (che possono comportare una verifica dell'elenco di mail relative a quella determinata utenza o delle sessioni di comunicazione stabilite da quella postazione in quel tempo) allo scopo di stabilire se l'anomalia rilevata sia da attribuire ad un malware/virus presente nella rete aziendale.

Il sospetto della presenza di un malware/virus o di un tentativo di intrusione nella rete aziendale e la conseguente finalità di verificare l'eventuale esistenza di un fenomeno illecito possono comportare la temporanea analisi/deviazione/blocco del traffico da e verso il computer/server infetto o obiettivo dell'accesso illecito con la connessa informazione all'utente eventualmente coinvolto.

Quando l'utente segnala l'anomalia in un servizio (non riesce a ricevere posta elettronica o a navigare su un certo sito, per esempio) il problema verrà preso in carico dall'Helpdesk che, aperta la chiamata, anche insieme all'utente, cercherà di diagnosticarne le cause e ripristinare il normale livello di servizio. Se il lavoro dell'Helpdesk non dovesse avere successo, ovvero si rendesse necessario un esame più approfondito dell'anomalia, possono essere eseguite fino alla soluzione del problema con conseguente chiusura dell'intervento, sul traffico generato dalla specifica utenza, ed a scopo puramente diagnostico, analisi simili a quelle descritte nel caso di anomalie statistiche, per verificare eventuali tentativi di intrusione nella rete aziendale.

Nel caso vengano rilevate attività illecite in danno al patrimonio tecnologico e di dati gestito dal Gruppo, ovvero in danno a Terzi, o perseguibili penalmente, la Società stessa si riserva il diritto di tutelarsi nelle opportune sedi utilizzando allo scopo tutti i dati in suo possesso.

Si specifica infine che, qualora l'Autorità Giudiziaria dovesse farne ufficiale richiesta, la Società è tenuta a fornire tutti i dati in suo possesso o a sua disposizione.

Infine, le Parti, stante quanto sopra concordato anche ai sensi dell'art. 4 della L.300/1970, nello spirito e nei contenuti della presente intesa, convengono sull'istituzione di un Osservatorio tecnico paritetico con il compito di monitorare gli sviluppi/aggiornamenti dei software introdotti, le eventuali ripercussioni verificatesi in ambito lavorativo e le conseguenti tutele nei confronti dei lavoratori utilizzatori di tali strumenti anche nel rispetto del citato art.4 della L. 300/1970.

L'Azienda, riconoscendo l'importanza dei temi trattati, provvederà a svolgere attività di informazione e sensibilizzazione dei lavoratori che fruiscono dei sistemi e dei servizi informatici per un utilizzo degli stessi in modo coerente con lo spirito e i contenuti della presente intesa e delle relative disposizioni.

Milano, 19 luglio 2011

RCS Quotidiani spa

RSU