Federazione Regionale USB Lombardia

L' AGENTE SEGRETO DELL'INPS

Milano, 28/12/2012

Con la circ. 135 del 3/12/2012, l'Istituto ha dettato un "disciplinare per l'utilizzo degli strumenti informatici", a cui sono tenuti ad attenersi tutti i soggetti in attività presso l'INPS, siano essi dipendenti o collaboratori temporanei.

Il dichiarato intento è quello di proteggere le infrastrutture informatiche, che possono essere messe a rischio da un uso improprio della posta elettronica e della navigazione Internet, da parte dei Lavoratori abilitati.

Per questa protezione l'Istituto ha messo già in atto strumenti tecnici specifici, come l'installazione di firewalls, antivirus e controlli sui server di rete, che sono tanto efficaci da rendere superflue gran parte delle raccomandazioni dettate, nessun PC, già adesso, può incappare neanche per errore in qualcuno dei siti WEB considerati "non di interesse aziendale". Non si può navigare collegandosi con una chiavetta Internet, perché l'antivirus in agguato ne rileva la presenza e disabilita subito la porta USB su cui è collegata.

Tutte le attività in rete sono monitorate e registrate in “log” che, come prescrive la normativa sulla privacy, dovrebbero essere anonimi, finalizzati al solo utilizzo di protezione e cancellati dopo un certo periodo di conservazione.

Tutto appare chiaro e regolare, anche se leggendo questa circolare alcune domande vengono spontanee, per esempio:

- in considerazione di tutte le precauzioni e di tutti i controlli effettuati, come mai l’accesso ad Internet rimane un “privilegio” a vantaggio solo di alcuni dipendenti?
- perchè non si è colta l’occasione di chiarire la posizione dell’Amministrazione per l’utilizzo della posta elettronica da parte del Lavoratore in riferimento a contenuti di carattere sindacale?
- Cosa significa che, in caso d’assenza del dipendente, un responsabile “può accedere alle comunicazioni nella mailbox dell’utente”? Vuol dire che non solo i tecnici preposti, ma anche i dirigenti possono leggere il contenuto della e-mail dei Lavoratori?
- come si concilia il divieto di installare software non autorizzato con le innumerevoli applicazioni sviluppate ufficiosamente in sedi periferiche, che divengono strumenti di lavoro quotidiani promossi dalle direzioni locali per aumentare la produttività?

A fronte di tutte le rivelazioni offerte dalla circolare, con dovizia di spiegazioni terminologiche, l’Amministrazione sembra tuttavia nascondercene una importante:

Sembra che, in ogni PC della nostra rete, sia stato installato un software spia.

Il suo nome sarebbe Agent Digital Guardian.

Questo è caricato sulla macchina prima della partenza dello stesso sistema operativo, come se fosse un driver, quindi non è rilevabile dall’utente.

Tutti abbiamo sperimentato che, alcune volte, i nostri PC di lavoro non completano l’avvio al mattino e continuano, inutilmente, a mostrare il logo di Windows che gira all’infinito: sarebbe l’Agent che, non essendosi caricato correttamente, impedisce al Sistema Operativo di partire senza di lui!

Il compito di questo programma è di registrare, in modo dettagliato e completo, tutte le attività effettuate sulla macchina: ciò che si vede sullo schermo, ciò che si digita, i programmi usati, le chiavette o i CD che vengono introdotti, persino i documenti inviati alla stampante! Tutti i dati verrebbero raccolti e trasmessi ad un indirizzo che li archivia, in gran segreto, per scopi non dichiarati.

Tutta questa attività nascosta, naturalmente, rallenta fortemente le prestazioni della macchina, per il controllo dei propri dipendenti, tuttavia, l'Amministrazione non sembra badare a spese e sarebbe disposta non solo a tollerare un calo produttivo, ma anche a sostenere il peso economico della licenza di questo sofisticato software, che sarebbe il più caro tra quello acquistato finora per la "sicurezza informatica".

L'USB non è nuovo ad occuparsi di questioni del genere: Già nel novembre 2009, con il comunicato n.23/09, il nostro Coordinamento regionale del Lazio aveva lanciato l'allarme sull'installazione di questo software, in via sperimentale, su alcune postazioni di lavoro a Roma.

L'anno scorso l'USB ha portato in tribunale l'Agenzia delle Entrate che, basandosi sui dati raccolti con un analogo software spia, aveva cominciato ad avviare richiami disciplinari sulla produzione ai propri dipendenti.

In quell'occasione il tribunale di Cagliari ha dato pienamente ragione al nostro Sindacato per la palese violazione dell'art.4 dello Statuto dei Lavoratori, che vieta il controllo a distanza da parte del datore di lavoro. Una sentenza importante che riafferma come i diritti dei Lavoratori non possano essere prevaricati dalle necessità organizzative.

Con la complicità di alcuni presunti "sindacati", presto le garanzie normative potrebbero cambiare: il recentissimo "Accordo sulla Produttività", firmato da CISL, UIL e UGL, non a caso prevede, tra le altre scellerate deroghe: *"…l'affidamento alla contrattazione collettiva delle modalità attraverso cui rendere compatibile l'utilizzo di nuove tecnologie con la tutela dei diritti fondamentali dei lavoratori…"!*

Come sempre, l'INPS funge da sperimentatore di tutte queste belle "novità" e si è attrezzato per tempo ad applicarle, se la Legge glielo consentirà, a danno dei suoi dipendenti o, meglio, di alcuni di loro!

Ciliegina sulla torta: sembra che l'*"Agent segreto"* sui PC della Direzione Generale non sia in attività, mentre lavorerebbe a pieno regime sulle Sedi periferiche di produzione…

In attesa di avere riscontro dalla nostra Amministrazione, su queste notizie ufficiose, riteniamo doveroso informare i Lavoratori, perché siano consapevoli del rischio che, ormai, corrono quotidianamente semplicemente lavorando!

Coordinamento Regionale

USB Inps Lombardia