GUIDA ALLA GESTIONE DELLE LICENZE SOFTWARE IN UFFICIO

SOFTWARE PIRATA IN AZIENDA

Come un sistemista di rete può tutelare l'azienda e il suo posto di lavoro contro l'utilizzo di software illegale da parte dei dipendenti.

Questo articolo nasce da una lettera spedita da Fievel82, che chiedeva appunto come potersi tutelare contro i colleghi che installano software pirata sui computer aziendali. Noi abbiamo a nostra volta girato a Enzo Borri, consulente antipirateria per aziende e per le Forze dell'Ordine.

Il problema dell'utilizzo di software illegale in un'azienda va affrontato su due fronti: uno quello tecnico e uno quello legale.

Parlando dell'aspetto tecnico, vi sono diverse tipologie d'approccio.

Una soluzione macchinosa ma utile nei casi in cui è necessario lasciare ampio spazio agli utenti, consiste nel creare un programmino usando uno degli strumenti di base del sistema operativo – un .bat in DOS da usarsi su Windows piuttosto che un AppleScript su Mac per fare degli esempi – che **a ogni avvio o spegnimento della macchina invii a un server in rete un elenco di tutti i programmi, i font e quant'altro interessi tenere sotto controllo.** Vi sarà poi un ulteriore programma sul server che analizzerà questi file al fine di rilevare discrepanze con quanto installato dall'amministratore di rete.

Sebbene possa funzionare, è uno scenario confuso in cui l'amministratore di sistema dovrebbe sempre esaminare giorno per giorno se sono state rilevate irregolarità. Inoltre, **basterebbe decisamente una conoscenza minima del sistema per disabilitare questo tipo di controllo.**

Una soluzione più efficace, consiste nel limitare le possibilità dell'utente. Se il sistema operativo ha capacità di affidare il controllo totale della macchina a un amministratore, si può autorizzare solo questo a installare software e si possono autorizzare invece tutti gli utenti al semplice utilizzo.

Questa strada è valida per diversi sistemi operativi Windows, per Mac OS e per i sistemi multiutente come Windows XP, Mac OS X e Linux.

Se la rete e le macchine sono molte, nascono però dei problemi: nell'arco di pochi giorni tutti conoscerebbero la password dell'amministratore. Chi opera in grosse aziende sa benissimo che per comodità vi è una unica password usata dall'amministratore di sistema per accedere a qualsiasi macchina. È proprio l'amministratore che a volte, stanco di correre da un ufficio all'altro per installare una volta un aggiornamento, una volta WinZip o qualcos'altro, **prima o poi rivela la password a uno degli utenti per fare sì che questi si arrangi da solo** togliendogli una scocciatura. Quest'utente, è tipicamente lo **smanettone dell'azienda che comincerà a dare la password di amministratore a desra e a manca.**

>> Un sistema centrale

La soluzione che ora sta iniziando a prendere piede – e che appare la migliore e la

più semplice da gestire – consiste nell'usare uno o più server su cui sarà installato sia il sistema operativo che i programmi che verranno usati dai vari utenti. Questo metodo – sebbene richieda delle reti dimensionate e ben studiate in funzione del traffico – si rivela essere anche più economico di altri in quanto consente l'acquisto di licenze "a utente" piuttosto che "a postazione". Queste consentono infatti l'uso di un programma a un certo massimo di utenti. Raggiunto tale numero di utenti, chi vorrà usare quel programma dovrà attendere che uno degli utilizzatori lo chiuda. Se ci si pensa bene, non tutti gli utenti usano contemporaneamente tutti i programmi che hanno installato o cui hanno accesso. Va comunque prestata attenzione alla licenza d'uso: molti prodotti software infatti hanno clausole che dicono che occorre una licenza per ogni utente che può utilizzare quel programma e non per il numero massimo di utenti contemporanei!
Tra i limiti di questa soluzione, vi può anche essere il fatto della difficoltà nel personalizzare il sistema operativo con driver specifici in funzione di particolari Hardware diversi tra le varie macchine in rete.
Una delle soluzioni più belle del "Net-Boot" è quella di Apple. Quando varie macchine – anche di modello diverso – sono collegate a un server con il sistema operativo – Mac OS – usato dai client, ciascuno di questi può accedere a un suo set di driver (estensioni, pannelli di controllo, librerie tipo DLL eccetera) specifico per il suo hardware e per i programmi cui ha accesso. Da un unico pannello di controllo è possibile – in un paio di minuti al massimo – stabilire quali elementi attivare e creare dei set già pronti da utilizzare per più utenti.

>> Non solo software

Tutte le soluzioni esaminate finora, **non impediscono la presenza di crack, di raccolte di numeri di serie o di programmi sotto forma di installer** che qualcuno potrebbe prelevare da Internet. Va infatti detto che anche i programmi sotto forma di installer necessitano di licenza e che i crack e le raccolte di numeri di serie sono da considerarsi illeciti in quanto rientrano tra i "mezzi intesi unicamente a consentire o facilitare la rimozione arbitraria o l'elusione funzionale di dispositivi applicati a protezione di un programma per elaboratori". Le sanzioni, sono le medesime che per il software illecitamente duplicato.
Si rende quindi necessario **limitare l'accesso a Internet lasciando aperte solo le porte necessarie alle attività utili all'azienda** (es consultare siti, prelevare posta elettronica, accedere a database su server di altre sedi eccetera) chiudendo le porte tipicamente usate per FTP o da programmi tipo HotLine, Carracho e simili. Questa, può anche essere un'occasione per chiudere anche le porte usate da programmi tipo Napster per lo scambio di MP3. Sebbene infatti questa attività potrebbe non essere illecita, sicuramente il tempo perso e il traffico generato sulla rete sono sempre un danno — o almeno un fastidio — per l'azienda.

>> L'aspetto legale

Esaminando poi l'aspetto legale del problema, occorre dire che i reati di cui si è parlato, sono reati penali! Ciò significa che **per questi non può essere impuatata una figura giuridica quale un'azienda bensì una persona fisica.** Trattandosi di persona fisica, se come responsabile viene identificato un dipendente, sarà questo a essere denunciato oppure – nel caso venisse denunciato il responsabile legale dell'azienda – quest'ultimo potrà rivalersi in sede civile nei confronti del dipendente chiedendo un risarcimento per il danno subìto. Va anche detto che, secondo le norme del contratto collettivo di lavoro **il dipendente potrebbe anche essere licenziato a causa di questo suo comportamento illecito.**
Una buona educazione in ambito aziendale sui rischi nel caso si installi illecitamente del software è innanzitutto doverosa, ed è un ottimo deterrente per evitare gran parte dei possibili comportamenti scorretti.
Ma anche gli amministratori devono sottostare a certe regole, **e non possono mettersi a sorvegliare indiscriminatamente le attività dei colleghi.** Lo statuto dei lavoratori vieta espressamente l'installazione sul posto di lavoro di strumenti di controllo remoto (art. 4), quali telecamere e microfoni e –per estensione– anche strumenti di logging delle attività Internet o di monitoraggio del lavoro svolto al computer (keylogger, strumenti per la cattura remota dello schermo). A volte, **qualche amministratore colto dalla sindrome di onnipotenza che spesso affligge i sysadmin, dimentica queste regole e si mette a "spiare" i propri colleghi** (qualche volta persino per espressa indicazione della direzione). È bene che si sappia che queste attività non possono essere praticate senza aver fatto prima un accordo con le rappresentanze sindacali e informato tutto il personale sottoposto ai controlli.

>> Conclusioni

Viste le varie soluzioni possibili, la super-soluzione può essere quella di fornire a tutti i dipendenti informazioni sulle leggi e sulle politiche aziendali attuate in propria tutela e informare i dipendenti sull'esistenza di file di log che consentono l'identificazione del nome utente utilizzato all'atto dell'installazione di componenti software o dell'indirizzo IP utilizzato per attività su Internet. Fornendo poi a ciascun utente una propria login e password personali per accedere al proprio elaboratore il quale avrà un suo indirizzo IP assegnato dall'amministratore. Oltre a tutelare l'azienda evitando comportamenti scorretti o potendo identificare eventuali responsabili, si tutelerà anche il dipendente evitando che qualcun'altro compia operazioni "strane" a sua insaputa. Di solito infatti… è sempre colpa di qualcun'altro! In ultimo, secondo la Legge in tutela della Privacy, va detto che l'utilizzo di una password onde consentire l'accesso agli elaboratori solo da parte del personale autorizzato, rientra tra i requisiti minimi da attuarsi qualora sugli elaboratori vengano effettuati dei trattamenti di dati personali.

ENZO BORRI
enzo@borri.org

Link utili

`www.privacy.it`
Informazioni varie legate al tema della privacy

`www.garanteprivacy.it`
Sito del Garante per la protezione dei dati personali

`www.lomb.cgil.it/leggi/legge300.htm`
Lo statuto dei lavoratori