venerdì 18 luglio 2008

Dalla privacy alla sicurezza

a cura di Vincenzo Miccolis

Come una sana vita telematica in azienda può evitare violazioni normative, perdita di dati personali e problemi software

I recenti fatti di cronaca relativi alle dichiarazioni dei redditi del 2005 pubblicate dall'Agenzia delle Entrate hanno riportato alla ribalta l'argomento della riservatezza dei dati personali. La sensibilità delle aziende italiane alla **privacy** è ancora minima. I controlli sono pochi e chi trascura questo aspetto della struttura tecnico informatica aziendale non teme conseguenze. In Italia è diffusa l'idea "ingiustificata" per cui se un illecito è molto frequente questo smetta di essere perseguibile.
L'adeguamento alla norma sulla riservatezza dei dati personali (regolata in Italia dal decreto legislativo n.196 del 30 giugno 2003) è ancora vissuto come un ulteriore peso per le PMI italiane. Tale adeguamento ha un risvolto che non andrebbe trascurato: **l'educazione, in azienda, ad una sana vita telematica**. Non è raro vedere in uso, nelle imprese italiane antivirus e sistemi operativi non aggiornati, piattaforme peer-to-peer e software pirata. La privacy diventa così un risvolto di un problema molto più vasto e pericoloso.
Questo risvolto è confermata dallo studio annuale sulla pirateria software nel mondo, realizzato a livello internazionale da **International Data Corporation** (IDC) per la Business Software Alliance (BSA), pubblicato il 14 maggio 2008, che vede attestarsi al 49% il tasso d'illegalità nel nostro paese. Tali atteggiamenti rendono molto più vulnerabili le reti aziendali mettendo in pericolo i dati, i progetti e i documenti interni, vero "tesoro" di ciascun'impresa. Si mettono a repentaglio inoltre i dati personali di clienti, dipendenti, partner e ignari individui.
Se, oltre a subire danni direttamente, si è anche causa indiretta di danni altrui, le conseguenze diventano molto più gravi, giungendo anche alla responsabilità penale. Essendo la norma raccolta in un testo unico non è impossibile, per le piccole aziende, gestirla in autonomia, senza sobbarcarsi ulteriori spese di consulenza. Sarebbe sufficiente per molti osservare semplicemente le "misure minime di sicurezza" (Decreto legislativo 30 giugno 2003, n. 196 - Titolo V - Capo II - Misure minime di sicurezza).
Vediamo ora in che modo aumentano i rischi in azienda con i comportamenti incauti di cui stiamo parlando. Partiamo dai s**oftware cosiddetti pirata** o crackati, privati illegalmente degli automatismi che ne impediscono l'utilizzo senza licenza. Questi costituiscono in Europa il 35% delle vendite complessive di software. quanto asserisce il Colonnello Vittorio Mario Di Sciullo, Comandante del Gruppo Marchi, Brevetti e Proprietà Intellettuale, Nucleo Speciale Tutela Mercati della Guardia di Finanza, in una recente intervista apparsa sul portale www.confesercenti.it.
Il dato rende evidente come non solo in Italia sia diffuso l'utilizzo di software illegale. Ma vediamo in che modo questi programmi possono minare la sicurezza di una r**ete aziendale**. Per chiarezza approfondiamo le modalità con cui si trova e si usa software pirata. Alcune delle vie possibili sono: download di programmi di sprotezione o productkeys; download di software già "crackato".

possibile ottenere i cosiddetti tool di sprotezione da siti web o dalla rete p2p. Alcuni scelgono di utilizzare i keygenerators, software che generano una chiave falsa da inserire per attivare la licenza d'uso del prodotto, ingannando le procedure di controllo.
Altri scelgono di "crackare" i software utilizzando programmi che rendano inerti i meccanismi di controllo della licenza del software trial che in questo modo diventa "eterno". Le versioni di software trial sono solitamente programmi con le stesse funzionalità della versione completa a pagamento, che smettono di funzionare dopo un determinato intervallo di tempo. Un sistema più semplice consiste nel rintracciare le chiavi di prodotto (*product keys*) false da siti web o reti p2p. sufficiente introdurre questo codice all'atto dell'attivazione della licenza, evitando così l'uso di keygenerators o altri software. Questo metodo è molto più semplice anche se è molto pià arduo trovare i codici.
Una via ancora più "comoda" per procurarsi questi software consiste nel **download diretto** di versioni già crackate da siti internet o dalle reti peer-to-peer. Come è evidente i fattori comuni ai vari metodi individuati sono l'utilizzo di siti internet potenzialmente "pericolosi" e della rete p2p. Si deve quindi considerare i rischi legati alla fonte di approvviggionamento. Secondo un altro studio di IDC ("The Risks of Obtaining and Using Pirated Software") commissionato da Microsoft nell'Ottobre del 2006, il 25% dei siti web che offrono prodotti contraffatti, productkeys, software pirata, key generators e altri tool di crack eseguono codice malizioso (malware) o installano software indesiderato (adware).
A prescindere dalla fonte si aggiungano inoltre i rischi rappresentati dai software modificati e non controllati oggetto dell'attività di ricerca. Il software scaricato, che si tratti di keygen, passwordcracker o semplicemente del software specifico che si stava cercando, è **potenzialmente pericoloso perch incontrollato**.
Nello studio "The Risks of Obtaining and Using Pirated Software" di IDC è indicato che l'11% dei key generators e dei tool di crack scaricati dai siti internet e addirittura il 59% dei key generators e dei tool di crack scaricati dai circuiti peer-to-peer, contiene software malizioso ed indesiderato. Facilmente il computer come la **rete aziendale** rimane così vittima di malware, adware e virus.
L'utilizzo di piattaforme p2p, come si è visto, può comportare gran parte dei rischi già individuati, inoltre aggiunge i pericoli dovuti alla condivisione delle risorse locali ed all'utilizzo di porte di comunicazione che, aperte, mettono a repentaglio la sicurezza di reti e computer.
L'attitudine a curare adeguatamente la **sicurezza informatica** della propria infrastruttura tecnologica, seguendo le misure minime di sicurezza dettate dal T.U. sulla privacy, e la giusta valorizzazione dei dati gestiti in azienda sono atteggiamenti che possono ridurre drasticamente i rischi descritti e, soprattutto, ridurre fortemente l'impegno di risorse economiche dovuto al recupero dai disastri.
Come sottolineato nello studio di IDC sull'approvvigionamento di software pirata, il costo che le organizzazioni sostengono per recuperare i dati in seguito ad un singolo episodio su di una singola workstation può superare facilmente il migliaio di dollari. Il costo per un'organizzazione relativo alla perdita di dati corrotti su server o su intere LAN può raggiungere facilmente le decine di migliaia di dollari per episodio. Le beghe legali per le responsabilità indirette possono facilmente superare questi limiti. Il vantaggio economico raggiunto negli anni mediante l'uso di software pirata può essere facilmente azzerato da un singolo attacco. Chi rischia lo faccia consapevolmente.

Versione originale: http://www.pmi.it/sicurezza/articoli/3181/dalla-privacy-alla-sicurezza.html