PuntoSicuro

ARTICOLO DI PUNTOSICURO

Anno 9 - numero 1807 di lunedì 22 ottobre 2007

Rischi interni o esterni per le reti informatiche aziendali?

I risultati di una recente indagine sulle minacce alla sicurezza IT.

4 aziende su 10 ritengono che il rischio più concreto per la sicurezza della rete informatica provenga dall'interno, dai dipendenti. Ad affermarlo è una indagine condotta da Sophos, azienda nel campo della sicurezza informatica, relativamente alle tipologie di collegamento che le aziende giudicano più rischiose per la sicurezza delle proprie reti.

Dal sondaggio condotto è emerso che il 31% delle società considera il collegamento da remoto o via - mobile la fonte di minacce più serie. Il 25% ritiene che l'accesso al network di ospiti o collaboratori esterni rappresenti il maggiore veicolo per fenomeni di malfare (codici dannosi). Infine, il 44% delle organizzazioni è del parere che il rischio più concreto per la sicurezza della rete provenga dall'interno, da comportamenti anche involontariamente pericolosi.

Molte delle aziende intervistate hanno manifestato, in particolare, difficoltà nel garantire che l'accesso alla rete dei propri dipendenti "mobili" rispettino gli stessi criteri di sicurezza imposti a chi è collegato internamente. Ciò è dovuto al fatto che spesso non sono in grado di stabilire se i computer remoti sono dotati del software necessario, delle patch di sistema e delle applicazioni di sicurezza aggiornate.

Inoltre, gli esperti di Sophos hanno constatato che i collegamenti da remoto di ospiti e collaboratori esterni passano a volte inosservati, aggirando completamente questi controlli di sicurezza. Di conseguenza, le probabilità di esporre la rete ad attacchi di ogni genere aumentano drasticamente.

"Anche se gli utenti che si collegano da remoto non sono mossi da cattive intenzioni, - affermano gli esperti di Sophos- se autorizzati ad accedere alla rete, possono involontariamente esporla a una miriade di rischi per la sicurezza. Senza una soluzione che controlli chi e cosa è autorizzato ad accedere al network aziendale in base a criteri uniformi, le organizzazioni hanno molte più probabilità di aprire vie d'accesso ai cybercriminali".

Riguardo ai pericoli " interni" dei dipendenti che sono connessi alla rete in modo permanente, è stato osservato che se non vengono rispettate le politiche di sicurezza aziendale si può mettere a repentaglio la rete, sia navigando su Internet in maniera irresponsabile, sia utilizzando applicazioni peer-to-peer o programmi di messaggistica istantanea, oppure semplicemente perché il proprio PC non è configurato in maniera corretta.
"È sorprendente ? affermano gli esperti di Sophos - quante aziende non siano consapevoli che i computer, utilizzati sulle proprie reti, non sempre sono conformi ai criteri di sicurezza, persino quelli connessi in modo permanente".