PuntoSicuro

ARTICOLO DI PUNTOSICURO

Anno 3 - numero 339 di venerdì 18 maggio 2001

Elaborato il "personal firewall" per contrastare gli attacchi di hackers e virus

Questo sistema specifico per la singola workstation va ad integrare tutte le soluzioni di protezione recentemente implementate.

Per contrastare i più recenti attacchi di hackers e virus si sta lavorando da qualche tempo all'elaborazione di sistemi di protezione multistrato, grazie ai quali il controllo e il monitoraggio di eventuali "intrusioni" sia distribuito su vari livelli dagli strati più esterni della Rete Internet, fino ai singoli PC collegati in rete locale (cfr. il numero 327 della nostra rivista).
Il "personal firewall" costituisce l'ultima frontiera per la protezione delle singole workstation ed è stato elaborato con l'obiettivo di monitorare tutte le connessioni a Internet, effettuate mediante modem o linea Isdn (dette "dial up") oppure attraverso linea Adsl (connessione tipo "broadband").

Il compito del personal firewall è bloccare le violazioni, non individuate dal firewall di rete, secondo schemi e procedure che dipendono dal modello di sicurezza sul quale è stato strutturato.
Secondo la struttura base il sistema analizza pacchetti di dati in base ai loro "headers", ovvero ai loro meccanismi di "presentazione", comparando i risultati ottenuti con l'insieme di regole, che agisce da filtro sugli "strati" più esterni della rete.

Alcuni componenti fondamentali di un personal firewall sono ad esempio "Agent", che è in grado di monitorare tutti gli attacchi in corso, anche i semplici tentativi, o il meccanismo di "User mode security", in grado di proteggere le applicazioni utente in esecuzione. Un altro importante elemento dell'architettura di un personal firewall è il modulo di "Remote control", che controlla il logging,
ovvero l'acquisizione e la registrazione, su un apposito file, di tutti gli eventi che si verificano sulla rete aziendale.

Un'ultima fondamentale precisazione: il "personal firewall" è in grado di garantire la massima efficienza solo se funziona insieme ad un antivirus, aggiornato con regolarità.
