



## La soluzione integrata per proteggere la tua rete

### *Virus... Attacchi alla rete.... Intrusioni..... Perdite di dati....*

*"In base ad alcuni studi, nel 2005 sono stati scoperti oltre 7.000 nuovi virus. La grande famiglia dei virus, che conta oggi 80.000 varietà circa, si è quindi arricchita di 7.000 pezzi di codice pericoloso e contagioso. "*

*Danni provocati dal virus Klez: Violazione della privacy con invio di documenti riservati presenti sul computer della vittima, congestione delle reti dovuta a invii di grandi quantità di messaggi, e altri ancora*

*"Klez, Bugbear e Sobig: violano i computer e disattivano i programmi antivirus"*

*Secondo la società di consulenza londinese Mi2g, il SoBig, che si diffonde anch'esso tramite e-mail e allegati infetti, ha provocato danni per un ammontare compreso tra 500 milioni e 1 miliardo di dollari.*

*Con l'avvento della banda larga, gli utenti che non avevano aggiornato il proprio programma antivirus si sono trovati esposti ai virus del tipo Blaster lo scorso agosto. Questo virus penetra nei computer delle vittime attraverso la porta TCP 135 sfruttando una falla di sicurezza Microsoft. Ancora attivo e associato da Symantec a un livello 3 di rischio (moderato), si serve del computer infetto per lanciare attacchi di tipo "Denial of service" (DoS) contro il sito Windows Update. Queste azioni possono destabilizzare il sistema e provocarne il riavvio inaspettato. In base alle indagini effettuate dalla Mi2g, Blaster ha infettato oltre 300.000 computer in 24 ore e provocato danni per oltre 525 milioni di dollari.*

---

Da oggi la vostra rete sarà al sicuro grazie a **DHSBOX**, la soluzione integrata hardware / software studiata per la piccola e media impresa.

**DHSBOX** è una soluzione economica e scalabile, cioè si adatta al crescere della vostra azienda.

**DHSBOX** incorpora un potente firewall per prevenire attacchi da internet alla vostra rete interna, salvaguardando i vostri Server, computer evitando di compromettere il vostro business.

**DHSBOX** ha un potente sistema antivirus auto aggiornante che neutralizza i rischi connessi alla ricezione di virus.

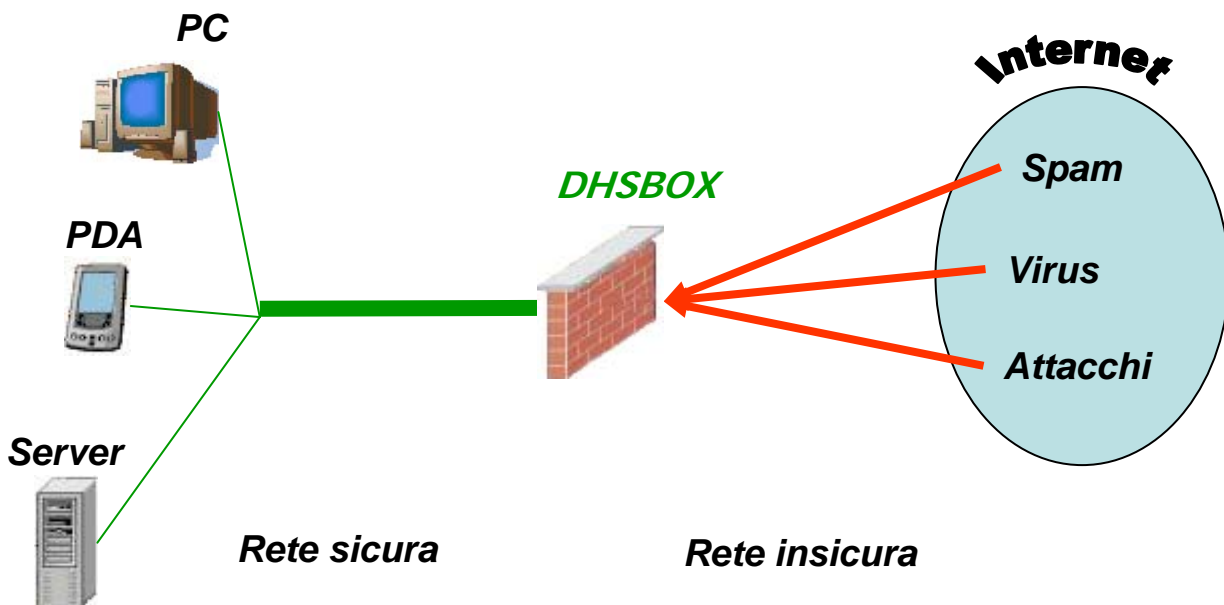
I servizi offerti da **DHSBOX** (antivirus, firewall) non possono essere disattivabili dall'utente, fornendo così una protezione della vostra rete 24 su 24 , 7 giorni su 7.



## La soluzione integrata per proteggere la tua rete

Come funziona **DHSBOX**

**DHSBOX** è un server opportunamente preparato e testato da Dhservice che utilizza Linux come sistema operativo. Si inserisce nella vostra rete tra la vostra connessione ad internet e la LAN in maniera trasparente per gli utenti e lavora ininterrottamente proteggendovi da attacchi e virus.



**DHSBOX** blocca tutti i rischi provenienti da Internet intercettando le email eliminando i virus (\*) trovati, impedendo di fatto che elementi nocivi possano entrare nella vostra rete.



## La soluzione integrata per proteggere la tua rete

**DHSBOX** identifica le email contenenti SPAM e ve le segnala, permettendovi così di risparmiare tempo prezioso.

**DHSBOX** si installa in poco tempo, è completamente trasparente agli utenti, non necessita di nessuna configurazione sui client.

**DHSBOX** è immune da virus in quanto utilizza il sistema operativo Linux, notoriamente esente da qualsiasi tipo di infezione.



**La soluzione integrata  
per proteggere la tua rete**

## **Caratteristiche Tecniche *DHSBOX***

### **Hardware (\*)**

Processore Sempron 2200+  
Mainboard Asus a7v400-mx  
Hard disk 40gb  
RAM 256 ddr 400 certificata

### **Software(\*)**

Sistema operativo: Linux  
Firewall: Ipcop v.1.4.0  
Antivirus: ClamScan,

### **Funzionalità(\*\*)**

Firewall con IPtables  
Server DHCP  
DNS Caching  
Antivirus  
Definizioni antivirus autoaggiornanti  
Proxy server (anche transparent)

## ***DHSBOX***

***Per informazioni: assistenza@dhservice.it***

(\*) a causa del miglioramento tecnologico Hardware e software, queste informazioni possono essere passibili di variazioni

(\*\*) Le funzionalità sono relative al tipo di contratto scelto dall'utente e possono subire variazioni e/o miglioramenti in seguito a test ed nuove implementazioni.