NETWORK PROTECTION

Mail Server protection

The best solution is the one that protects right from the beginning

Datawasher provides a comprehensive protection because it cares not only for the customer's e-mail but also for the customer's mail server.

Its technology protects the companies' mail server because it is the main door where attempts, infected or unwanted messages get into customer's networks.

Unfortunately, mail servers are threatened by aggressive and powerful attacks, which are very difficult to stop, which can affect seriously the customer's security.

Two examples of dangerous **mail server's attacks are DHA and DoS.**

Directory Harvest Attacks

Datawasher protects company's mail server from DHA, a harmful SMTP threat that cannot be identified and blocked by traditional software or conventional anti-spam solutions.

To carry out Directory Harvest Attacks, spammer or e-mail list broker take advantage from the usual process of e-mail delivering:

before an email can be sent to a server you have to control first of all if the delivery address is correct. If it is not, the sending server receives an SMTP 550 error message or a DFNs (delivery failures notifications). If the answer is affirmative, it means that the address is valid and the messages can be delivered.

Spammers exploit this simple functionality sending thousands of messages to a target domain, making a combination using dictionaries of the most diffuse names and surnames and tracking all addresses, listing those that are not sent back or that can generate an error or a DFN.

Denial of Service Attacks

Datawasher protects, as well, from attacks characterized by an explicit attempt to prevent legitimate users of a network service from using that service. The most common method is to flood a network with useless traffic, overloading the server and network's capacity.

Datawasher sits between Internet and the company's network, analysing and cleaning the whole traffic **before** it arrives at the customer's mail server.

Datawasher protects, in real time, not only from harmful SMTP connections but from other dangerous network's attacks, using the following specific techniques:

Connection Analysis

Datawasher verifies that the connection to a mail server is lawful and protects from those containing harmful commands which take advantage of server's vulnerabilities such as Buffer Overflows.

This malicious connection seizes server's vulnerabilities seeking to gain partial or total control of it. As these kinds of attacks enable anyone to take total control of a server, they represent one of the most serious threat.

Datawasher verifies, as well, that sender e-mail's structure and IP's address involved on the communication are lawful.

IP Reputation

Datawasher analyses the reputation of the sender IP address and his previous activity as a supposed spammer, checking it in an extensive and proprietary database containing the most active spammers.

The effects of a server's failure or a breaking off of its connection can cause irreparable damage for the company.

DISASTERRECOVERY, never lose your e-mail

Datawasher's solution includes the Disaster Recovery service. If the customer's server is not running or its Internet connection is interrupted, Datawasher's systems keeps users' messages until their server will be operative again.

In this way Datawasher avoids the loss of Business information and protects the image of the Company.

DATAS AG. Via Calloni, 9. 6900 Lugano. Switzerland **Phone.** 0041 (0) 91 2206420 **Web.** www.datawasher.com **Email.** sales@datawasher.com