Detecting and blocking fake mails

iQ.Suite Tips & Tricks for IBM Domino

By default, the iQ.Suite uses an address selection rule named InetSender to detect emails from the Internet. The operation checks the email's From field to see if it contains the expression *@*. and will deliver a reliable result in most cases. But the result can be completely false if incorrect details are inserted in the From field (mostly by spammers), in particular if locally present sender addresses are used. This causes anti-spam jobs, for example, to ignore such emails. These jobs typically run only for emails which have been received from SMTP senders (InetSender selection rule). It is possible to evaluate other fields in an email to see whether it has come from the Internet.

SMTP mails differ from Notes messages in respect of the SMTPOriginator and Received fields among other things. If your internal emails are not sent via SMTP, these fields can be used in conjunction with two Notes formulas to identify an Internet mail.

a) 
NotEmpty:=SMTPOriginator!="";
@if(@iserror(_NotEmpty);@false;_NotEmpty)

b) 
!@isNull(Received);

In our example we only want to run the anti-spam job for emails arriving from the Internet.

- Create two mail rules with the formulas shown above:

"Training - SMTPOriginatorExistsAndIsNotEmpty"

iQ.Suite Formula Rule

<table>
<thead>
<tr>
<th>Basics</th>
<th>Comments</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Name</strong></td>
<td>Training - SMTPOriginatorExistsAndIsNotEmpty</td>
</tr>
<tr>
<td><strong>Status</strong></td>
<td>Active</td>
</tr>
<tr>
<td><strong>Log level</strong></td>
<td>Loglevel 0 (value from NOTES.INI)</td>
</tr>
<tr>
<td><strong>Execution mode</strong></td>
<td>Dependent on job or global parameter</td>
</tr>
</tbody>
</table>
| **Formula** | _NotEmpty:=SMTPOriginator!="";
@if(@iserror(_NotEmpty);@false;_NotEmpty) |

Check correctness of formula syntax
Include them in your anti-spam job under "Dependency on positive rules". Choose "All true" as the logical operator:

This configuration ensures that only SMTP mails will be checked in future, i.e. only those emails that do not originate from a Notes environment. To avoid false positives, SMTP mails from senders on our whitelist are excluded from checking.

The configuration process is somewhat more elaborate when emails appear to come from SMTP senders who are in the user's own domain. These should not merely be checked for spam. They can be classified as spam on the basis of the sender alone and can therefore be placed in quarantine without further checking, provided that internal emails are sent as Notes messages.
Nowadays, it is unlikely that any spammers will send emails under their real sender address. Various measures can be used to detect and filter these fake mails or spoofing mails.

One of the key issues in setting up an anti-spam concept in our training and at our workshops is filtering of spam email on the basis of fake sender addresses. This is an important approach to fighting spam as elaborate content checking is then no longer necessary in certain circumstances.

Why not pay us a visit? We look forward to seeing you!