Using whitelists to prevent quarantining of business emails

iQ.Suite Tips & Tricks for IBM Domino

Fighting spam has become one of the central tasks for mail administrators. A lot of time (and euros) are channelled into the implementation of various methods that filter out unsolicited mails and ensure that they do not block work processes unnecessarily. It is annoying but not critical when one or other of the spam mails is not recognized as such and delivered (false negative). However, it is critical when business mails are identified as spam - false positives. If the user is not informed promptly about his quarantined mails, it can have unpleasant consequences. An offer is not accepted within the prescribed period, you lose a big order because you did not answer the inquiry, a customer is annoyed because he feels he is not getting good service and terminates his contract. The financial loss in such cases may be huge. What is usually more serious, however, is the image loss suffered by your company. Just the opposite of what you want to achieve actually happens!

The current methods used to combat spam are extremely good at detecting spam. We now therefore need to concentrate on identifying business-relevant mails and making sure they are not filtered. One of the most effective ways of doing this is whitelisting. The principle is beautifully simple: a mail that comes from a sender or domain that is known not to send spam is not subjected to the spam check and cannot be filtered. A list of these senders and domains is known as a "whitelist".

Setting up a whitelist

We showed you how to set up a simple whitelist based on a mail address rule in our December 2007 issue of Tips and Tricks.

You can create several such address rules or include all addresses in one - this is a subjective decision. You should always proceed in such a way that you and your colleagues can trace your steps later.

The whitelist needs regular manual maintenance by the administrator. The domain of a new customer can be added fast and easily. This is a viable method for the administrator provided it doesn't need to be done several times a day. When multiple entries need to be made or recipients have an email address in a domain that cannot be globally defined as "good" (e.g. max.mustermann@yahoo.com), it is sensible to set up automatic whitelisting. The iQ.Suite offers this function via a wall job, which has to be configured once and does its job automatically from then on.

The whitelist job works according to the following principle:

If local user (Alice) sends a mail to an external recipient (Bob), it can be assumed that Bob is not a potential spammer. He is therefore put on the whitelist. The following sender-recipient entries can be generated depending on the configuration:
Entry for Bob as person (e.g. bob@foobar.external) or
Entry for Bob’s domain (e.g. *@foobar.external)

and

Entry for Alice as person (alice@group.de) or
Entry for the entire domain (e.g. *@group.de) or
Entry for ”all”

These entries are made in the default setting of the database ”iQ.Suite Black-/Whitelist” (g_connect.nsf)
under a list named ”GeneralWhiteList”. A person-person entry then looks like this:

Wall - Utilities - Black-/Whitelists:

It is easy to configure the job:

Copy the default whitelist job with priority 7400 ”DEFAULT - Whitelist Job”, insert it and rename the
copy so that you can identify it as ”your” job. Open it in Edit mode, activate and save it. No other
adjustments are necessary. From now on, a person-person entry is generated for each email sent from a
sender in the address book to an external recipient: the sender is entered as recipient, the recipient as
sender.

Entry in the list is not sufficient in itself. If a list is to be used as a whitelist in the black/whitelist DB, the
next step will be to incorporate it to a mail black/whitelist rule. This has already been done in the rule that
is supplied, ”WLRuleAntiSpam”. This rule must now be incorporated in the dependence on negated rules
the in anti-spam job. Apart from the address whitelist rule and the ”MailResentFromQuarantine” formula
rule, the ”WLRuleAntiSpam” rule now prevents spam checks on known ”good” senders. Do not forget to
link the rules with ”All false”!
Correct handling of blacklists and whitelists requires due care. There is, above all, no general answer to the question whether, and if so, to what extent users can maintain these lists themselves. At our training courses, we take a detailed look at black- and whitelisting in sessions on anti-spam measures.

Come and see. We look forward to your visit!