Combating Spam Server-side

Purpose : to provide insight into the steps an organization can take to close the Spam Floodgates.

Introduction

- Working in the IT sector since 1996
- Specialty is Network Solutions and Wireless (NYCwireless)
- My E-mail Address (source on my website) :


```
<script type="text/javascript"><!--
document.write('<a href="&#109;&#97;&#105;&#108;&#116;&#111;&#58;' +
'&#98;&#101;&#110;@' +
'&#114;&#101;&#101;&#102;&#115;&#111;&#108;&#117;&#116;&#105;&#111;&#110;&#115;&#46;&#99;&#111;&#109;' + '">' +
'&#98;&#101;&#110;&#64;&#114;&#101;&#101;&#102;&#115;&#111;&#108;&#117;&#116;&#105;&#111;&#110;&#115;&#46;&#99;&#111;&#109;' + '</a>');
// -->
</script>
```

Spam Definition and Types

- Definition of spam – unsolicited commercial e-mail sent by an organization/person that the recipient has had no prior contact with.
- Types of Spam: Adult, Business Opportunities, Nigerian Scam, Viruses, etc.

Steps to Close the Spam Floodgates

- Content Filtering, Hashes/Signatures, Bayesian Filtering, Use of RBLs, Change mailto links (to JavaScript http://nilbs.com/techbabl/str2hex.htm), Cleanse E-mail Archives, Switch to Forums
- Client Side -> change default view in Outlook, user training to stop "unsubscribing"

Content Filtering

- RegExFlt (http://www.2150.com/regexfilter). for Exchange 2000, Communigate Pro (Win only), and Merak Mail (icewarp.com, I use this for my gateway deployments).
- Pros: Tuned already, free, highly customizable, fast, low memory & cpu requirements.
- Cons: Requires configuration and learning. No phone support, supported by peer to peer web forum (& author).

Other Popular Methods

- Hashes/Signatures –low false positive rate, requires monthly service cost
- Bayesian Filtering – excellent (very accurate), Unix backend, requires client configuration. Highly cpu intensive. Free.

Deployment Options

- Server, Client, or Gateway
  - Server -> requires modifying production environment.
    - Client -> requires more training and support than centralized solution.
  - Gateway -> deploy at your own speed, reduce workload for main mail server, more “gateway” feature rich than Exchange, anti-virus solution cheaper, use of non-server licenses, removes main mail server from internet contact (e.g. MS KB 331953, a major vulnerability without a patch for NT 4.0).

Introducing your Mail Gateway

- Deploy Mail Gateway on NT, 2000 Pro/Server, or XP.
- Put it behind a firewall or use OS built-in filtering (Win2K IPSEC filters).
  - Add Records for DNS (dual MX).
- Remove MX Record (or modify firewall) when ready.

Monitor, Tune, Monitor

- After Deployment, watch carefully for False Positives, and tune where needed.
- Allocate a few hours each week to monitor it for the 1st month, then a hour a week and to bi-weekly (train others as well).
- Make Users feel part of the solution - setup an abuse e-mail address

ROI – Return on Investment

- Provide Week 1 and 2 Reports, then continue with Monthly Reports to insure value is understood.
- Explain False Positives, and Make Extra Effort to Insure this is minimal for Management

Conclusion

- Deploy Mail Gateway and enjoy all the benefits (reduction in spam & costs) from it.

- ROI Feedback is important. IT tends to undervalue it.

Bonus

- Stopping Browser Pop-ups - Mozilla, Netscape, and Opera. Default to these for clients, then use IE as backup. I prefer Opera and then Mozilla.
- Spyware is also a major threat, utilize the free detection software from Lavasoft. It's called Ad-Aware www.lavasoft.de