GIAC
CERTIFICATIONS

Global Information Assurance Certification Paper

Copyright SANS Institute
Author Retains Full Rights

This paper is taken from the GIAC directory of certified professionals. Reposting is not permited without express written permission.

Interested in learning more?

Check out the list of upcoming events offering
"Security Essentials (Security 401)"
at http://www.giac.org/registration/gsec

Managing Email with Brightmail – One ISP's Account
John Kane
GSEC v1.3
April 3, 2002

Introduction

Unsolicited commercial email and email-borne viruses are an increasingly difficult problem for service providers of all sizes. Even the largest ISP's have had their services interrupted by the constantly growing wave of SPAM being directed at email users everywhere. Users are becoming more and more disenfranchised by the amount of unsolicited mail they receive, the majority of which is at best annoying and unreliable, at worst offensive and fraudulent. Customers are looking to their service providers to stop the unwanted messages, and feel that the problem is something for them to deal with.

Spam and Viruses make a considerable impact to the bottom line of all service providers. Spam and viruses cause increases in facility costs, increases in hardware and software, and higher resource requirements for frontline call center staff as well as dedicated systems administrators. Spam is also a major contributing factor to customer churn, which has significant financial impacts to any organization.

Our company is a medium sized regional ISP who has been having the same issues as both our small local colleagues, and the big national providers. We have been working to build brand loyalty and strong customer retention, which can lead to even higher levels of Spam, due to the longevity of the accounts. Given the resource restrictions, our company decided to try for a managed solution to deal with all of the SPAM and email-borne viruses we receive.

Abstract

This paper will discuss the current trends in Spam and email-borne viruses, in the recent past and the estimates on future rates. The paper will look at the way in which customers view unsolicited email, and the impacts to service providers in dealing with unhappy customers.

The main focus of the paper will then be to present our company's approach to dealing with this problem, the Brightmail Solution Suite. The paper will explain how the Brightmail product works, from the component elements of the Probe Network, to Brightmail's Logistics and Operations Center, and the relationship with Symantec. The paper will then briefly explain the way in which our company has implemented the Brightmail Solution Suite's Anti-Spam and Anti-Virus products, the results we have seen in our initial rollout, and our future plans for augmenting the service.

Managing Email

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

Providing a quality email service to customers is becoming an ever-increasing problem for service providers. Even the largest of the national providers has not gone unscathed when dealing with overwhelming levels of unsolicited commercial email or "spam", and email-borne viruses. To make matters worse, the trend does certainly not appear to be changing. Brightmail, the San Francisco based company who monitors spam on the internet, found 10 percent of all messages sent in 2001 were classified as spam. That number, based on their findings looks to be in the 30 – 40 percent range this year and is growing. Jupiter Media Metrix estimates the average mailbox in 2001 received 571 unsolicited messages, and they estimate that the number will grow to 1500 messages per mailbox by 2006.

As the numbers of people and devices that become online continues to grow, so will the levels of spam. Sending large quantities of email to thousands of people is relatively cheap for the sender. The cost of the mailing is passed on to everyone else along the way.

Customers want it to stop

A 1999 Gartner Group study showed more than 80 percent of the people surveyed at least disliked the spam they received, the majority of them selected "dislike a lot" as a selection. For the majority of the respondents, the single biggest issue in dealing with the spam was the time wasted in deleting the messages from their inbox. This defeats the defense of most spammers, who simply tell people who do not want to read the content of their mailings to simply delete them. In fact, Computer Mail Services of Southfield Michigan came up with a calculator for determining the impacts to a business when employees receive large quantities of spam. According to their numbers, a company with 500 employees, receiving 5 unwanted messages per day, at 10 seconds per message to delete them loses 105 days of productivity and $40,000 in wages for wasted time per year.

The Coalition Against Unsolicited Commercial Email (CAUCE), cites the majority of spam as chain letters, moneymaking schemes, adult content, offers surrounding sending or buying lists for spamming, stock offerings for unknown startups, health products and pirated software. While the "take rate" for spammers is considered to be quite low, when you can send something to 100,000 people with little to no cost, if only 10 percent of that group sent in a dollar, you would still gross $10,000. Not bad for a dishonest day's work.

Spam's Effects on the Service Provider

The effects of Spam on the service provider come in a variety of ways. The first, and potentially most financially impacting is in customer churn. According to the Gartner survey, and from the experience of the frontline staff in my organization, the overwhelming majority of Internet users feel it is the responsibility of their ISP to block the unwanted messages from their message stores, and 7 percent of those who changed ISP's sited spam as a major factor in choosing to switch. Even more alarming is that 36

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

percent of those surveyed would drop their current ISP if they felt it would eliminate the unwanted mail.

Service providers also have to deal with increasing hardware and software maintenance costs to build systems capable of handling extremely high loads, even when their customer base does not necessarily require it on their own. Customers who receive large quantities of Spam can force an ISP to have to upgrade everything from disks and CPU's, to employing a full mutli-platform load balanced environment long before they reach the theoretical limits of their current infrastructure based on "valid" usage requirements. Service providers will also have to continue to maintain even larger numbers of staff, both at the helpdesk level and in their operations group to handle the impacts of unwanted mail. Many customers who receive unwanted mail forward those messages on to their ISP's "abuse" mailbox or call in to technical support. All of the extra activity focused around this drives the operational costs higher and higher, pushing some of the smaller ISP's right out of the game. All this and we still have not considered the effect on backbone requirements or the costs of outages caused by overwhelming floods of activity.

Email Virus Attacks

Estimates for the costs of having systems infected with viruses have been in the trillions of dollars. Not everyone in major organizations runs properly updated virus software on their machines, and the likelihood of residential customers keeping up-to-date anti-virus software is even less.

Email is becoming the top method for spreading viruses around the net. With the myriad of worms, Trojan horses, html and macro viruses circulating and ever metamorphosing into new and varied strains, ISP's are struggling to keep up. At first glance one may wonder why the ISP would be responsible for a customer getting infected with an email virus. The reasons are simple. First, there are the calls to the ISP's technical support number. For the majority of customers, the tech support line for their ISP is the one stop shop for all of their PC inquiries. Customers who call feel it is the ISP's responsibility to help them regain their lost data, and most feel it is the responsibility of the ISP to prevent the virus from getting to them in the first place. Secondly, the customer with the DSL connection who gets infected with a virus has the potential to severely impact the rest of the ISP's customer base, or even worse still, another ISP causing the ISP to find it's IP address space on a blacklist somewhere.

Our Company's Plight

On February 18th and 19th AT&T's WorldNet servers were brought to a virtual standstill under an unprecedented tidal wave of spam. This is widely believed to be the first incident of spam rendering major ISP's mail servers inaccessible for normal use. If it is possible for this to happen to one of the giants, what can a medium sized regional ISP do?

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

One of the key determining factors for how much spam a mailbox is likely to receive is the length of time for which the mailbox has been active. For us this is a major issue since the majority of our customer base is based on the acquisition of smaller ISP's that had loyal customers in some cases for a very long time. A key part of our service during the acquisition phase was the idea that we would preserve these addresses as aliases for our customers, in addition to the new mail store they were given. Compounding this issue is the fact that some of the ISP's acquired ran very old versions of their mail software, which allowed their users addresses to be harvested. In the case of one particular domain, when polled against a known spammer's database, over 3000 accounts were found.

Given the competitive nature of the business, the high costs of customer churn, and the high resource requirements on our systems and staff, our company decided to attempt to do something. After researching what was on the market and what could be done "in-house" given our resource constraints, we decided to go with a managed package solution for dealing with spam and email-borne viruses.

Brightmail Solution Suite

Brightmail is a San Francisco based company that provides message management solutions to service providers of all types. The company boasts such partners as Sendmail, Symantec, Openwave and Critical Path. Their clients include such names as AT&T's WorldNet and Earthlink.

In order to be able to deal with our often-overwhelming spam problem, our company decided to adopt the Brightmail MAILWALL solution. The mailwall application could be likened to an "email firewall" that resides either on top of, or in the case of our company, in front of the existing mail environment.

The mailwall system is in essence a complex series of filters, or as they call them rule sets, that attempt to identify what should and should not be sent on to the intended recipient. Brightmail builds these rule sets based on qualitative and quantitative analysis from their systems and technicians. The Brightmail Solution Suite, is comprised of three interlocking components, each with their own unique responsibility that provides the rule sets to all of the customers within the Brightmail network.

The first of the elements that make up the Brightmail Solution Suite is what Brightmail refers to as the Probe Network. The Probe Network is basically a bunch of mailboxes. These email addresses are specifically selected from various members of the Brightmail network, and are strategically placed into an elaborate web for trapping spam. The Probe Network can be viewed as the first alert system for the Brightmail Solution, and helps to feed into the mailwall system. This network of over 150 million mailboxes serves to detect and prevent spam from reaching its intended recipients.

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

The second element in Brightmail's product is their relationship with Symantec. Symantec is a known industry leader in anti-virus research and products, and their partnership with Brightmail allows their expertise to reach people in a whole new way. The Symantec Security Response center utilizes a system of heuristic scanners to identify new virus profiles and Trojan horses, in addition to identifying the constantly morphing existing strains. These updates, once identified are then sent on to the final element of the Brightmail Solution, the BLOC.

The BLOC, or Brightmail's Logistics and Operations Center is the heart of the Brightmail product. This is the epicenter that is fed data from the Probe Network and the Symantec Security Response center to build the complex rule sets that are sent out to update all of Brightmail's customers. The BLOC is comprised of technicians and systems whose sole responsibility is the development of filters for their clients, designed to ebb the flow of wanted or corrupt mail, while allowing legitimate mail to pass through unabated. The rule sets a built based on the data collected via the Probe Network. Messages are screened both analytically by the BLOC's systems to determine message counts and frequency and also qualitative analysis is done by the technicians at the BLOC, who carefully screen the contents of the messages and use them to define rules that will best identify future copies of the same or similar messages.

In this respect, the work being done by the BLOC is essentially the same role our Postmaster was providing, with the key exceptions that our Postmaster is only one person, and is not chained to his desk 24 hours a day doing nothing but reading spam. Using the Probe Network messages in the BLOC also allows clients of Brightmail to essentially share resources amongst one another. For example, if ISP A gets a large volume of spam relating to some new get rich quick scheme, the BLOC will see these messages via the Probe Network and send out an update. The update will ideally prevent some of the messages from reaching customers for ISP A, but if ISP B has not yet seen the messages, they likely never will, since they receive the same rules. In this way, the messages seen by one ISP help to prevent similar messages from reaching other networks.

Brightmail Anti-Spam

The goal of Brightmail's Anti-Spam product is simply to capture all unwanted messages destined for a client mailbox, without preventing the delivery of wanted mail. This lofty goal is achieved via the constantly evolving rule sets sent out by the technicians in the BLOC to the Brightmail clients around the world. The message transfer agent (MTA) of the client system is then configured to send all incoming messages into the Brightmail server process.

The Brightmail server process is the set of applications residing on the client MTA to filter the incoming messages. These messages are filtered using the latest rule set provided by the BLOC technicians. These rule sets are constantly being evaluated, both for what is new and for what is successful. Rules that are no longer being used, i.e.

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

the messages of that type are no longer being sent, are removed from the updates, preventing them from growing to such a size they would become unmanageable.

Once identified as spam, the client has several options for dealing with the message. The options are to sideline, Grey Mail, x-header modification or subject line tampering. Subject line tampering is basically the inclusion of a custom defined text string that can be added to the message upon discovery. The end user would then be able to build mail-handling rules on their machine to automatically move them to another folder, delete or forward the messages as they see fit, and depending on the abilities of their mail client. X-header modification works in essentially the same way, except the modification is not as obvious to the users.

Sidelining is simply the spooling of the mail indefinitely into another directory. This method prevents the users from requiring modifications to their mail clients to get rid of the messages, but also runs the risk of messages that were sidelined incorrectly from ever reaching their intended targets. Customers would be required to contact the ISP and request the message be found, and then have the admin send the message on to them. Grey Mail is essentially the same as sidelining, except that it provides a web-based client enabling customers to login to view the messages intended for them that were flagged as spam. Depending on the configuration requirements of the ISP, these messages could simply be deleted after a period of time, or in some instances can be configured to count against the customer's mailbox quota, requiring that they periodically clean out the message store.

Brightmail Anti-Virus

The Brightmail Anti-Virus solution utilizes the industry leading expertise in virus detection from Symantec and marries that with the rule sets updated by the BLOC technicians. The SSR sends the latest virus alerts and identification parameters to the BLOC. The technicians at the BLOC then write new rule sets for viruses based on the data from the SSR, test and then send them out in the next update.

Messages are scanned on the client MTA, with the same process the messages are filtered for spam, with the exception that all messages setting the virus alerts are sidelined into a temporary directory. Once sidelined, the temporary folder is then periodically "cleaned" using the anti-virus engines provided. Once the message has been cleaned, it is then sent on to the intended recipient, with an explanation that a virus was detected and cleaner for them. If the message had an attachment that contained a Trojan horse, then the message is sent on, without the attachment, and an explanation of the event is added to the content of the message.

Introducing Brightmail into our Environment

Our company chose to role the Brightmail Solution into production using a Sendmail Gateway. We did this for a couple of reasons. First, there was some issue with using the mailwall product with our current MTA. The second reason was to ease the use

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

of the product into our production environment with little to no impact to our customers. This deployment also gave us flexibility in deployment given the diversity of services within our network. Since not all of our acquisition mail platforms have yet been assimilated into our main mail service, this gateway configuration grants us the ability to filter on those accounts, regardless of the platform they currently reside on. We also made the decision to sideline the mail, since we did not want our customers to receive the unwanted messages at all, and given the time constraints we were under to get this into the network, Grey Mail was not an option for us at this time. Grey Mail would have also required some significant provisioning modifications since it would not reside on the same system as the existing mail service.

The gateway system was built on a midrange Sun server running Solaris 8. For the MTA, we chose the Sendmail Switch product, using the managed MTA software, which is based on Sendmail v 8.11. The server was initially configured to allow two of the domains currently used by a small subset of our customer base to relay through it, and then the mailertable was modified to route all traffic for that domain to our existing mail platform. Once the domains were added to the Brightmail configuration, the MX records for the domains were modified to send all SMTP traffic destined for those domains to the new gateway system.

We were initially shocked at the amount of messages that were sidelined by two domains with only a few customer accounts within each. The sidelined messages were closely monitored for the first few days, ensuring that the messages being sidelined were not valid messages our customers would miss. This has not yet proven to be an issue, as in three weeks of running the product we have not had a request for a lost message that turned out to have been sidelined by the product.

We have also noticed a significant decrease in the number of calls to our helpdesk staff complaining about the type and amount of spam messages they are receiving. This is a great improvement over where we were and we look forward to increased customer experience due to the product. There has also been a very substantial decrease in the amount of time our mail administrator has been spending dealing with spam complaints and trying to write filters on our existing mail server to stop the flow of spam. This has always been a loosing battle since the majority of the spam we receive comes at times of the day when our administrators are not on duty, and we are too small an organization to have someone on staff 7x24 to attempt to monitor the ever changing spam flux.

The actual performance of the product since we converted the remaining domains over to the Brightmail Solution has been impressive. In just over three weeks of running the product in a full production environment, almost 2.5 million messages identified as spam were blocked from their intended recipients. We have had days where the percentage of sidelined mail was over 40% and average in the 30's. This has also made a significant improvement to the performance of our existing mail platform, since the majority of the mail it deals with is actual mail intended for, and wanted by the recipient. In the same time frame, the Brightmail Solution has also identified and cleaned for our customers close to 17,000 viruses. This is to us one of the biggest impacts to our service,

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

since its effects are so widespread, from customer contentment to system requirements and most of all, facility requirements. Based on these results, we have deemed this initial rollout of the Brightmail Solution Suite to be a success.

Conclusion

Service providers across the globe are engaged in a never-ending battle with those who would look to exploit their resources and their customers for profit. Spammers, and the purveyors of viruses account for trillions of dollars in wasted time, damages and lost profits worldwide. Dealing with spam grows increasingly more difficult as there is no international regulations preventing it, and as it continues to grow exponentially with the rise in online people and devices. Viruses continue to be released, and old ones continue to morph, constantly barraging the world's networks. The costs levied on the service providers are extensive including customer churn, hardware and software expenses, increased bandwidth requirements and human resource requirements. One of the many products on the market designed to fight this is the mailwall product, part of the Brightmail Solution Suite.

The Brightmail Solution Suite is a combination of the network of email addresses used for detection known as the Probe Network and the updates from the Symantec Security Response center being fed into the Brightmail Operations and Logistics Center, where the data is used to build sophisticated rule sets designed to filter and handle unsolicited email and viruses before they reach their intended target. The technicians at the BLOC constantly define and redefine these rule sets, then push them out over their extensive network to all of their clients. Incoming messages are handled by the Brightmail server, and if identified as spam, are dealt with according to the configuration settings of the client system. Viruses are sidelined into a temporary directory where they are cleaned or attachments are deleted, then the message is sent on with a customized message explaining what was found and how it was handled.

The ISP I work for has implemented the Brightmail Solution Suite via an email gateway into our existing mail service. The product has been configured to attempt to block the vast majority of the spam and viruses destined for our customers from ever being seen. The results to this point have been very favorable, as we have in only three weeks stopped 2.5 million spam messages and 17,000 viruses form hitting customers in our network. In addition to the customer benefits, we are also experiencing reduced system load on our existing mail platform, as well as reduced resource requirements for our call center and our mail administrators.

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

References

1. Brightmail. “Email for the Twenty-First Century: The Mailwall™ Solution” http://www.brightmail.com/pdfs/mailwall_white_paper_v1-0.pdf
2. Gartner Consulting. “ISPd and Spam: The Impact of Spam on Customer Retention and Acquisition”. http://www.brightmail.com/pdfs/gartner_rebuilt.pdf
3. Slayton, Joyce - SF Gate. “The Rising Tide of Spam.” 18 March 2002 http://www.sfgate.com/cgi-bin/article.cgi?file=/gate/archive/2002/03/18/spmlmt.DTL
4. Graff, Joyce - CNET. “No easy solution for spam”. 25 March 2002 http://news.com.com/2009-1023-867954.html
5. Wiser, Leslie G. Jr. “Statement for the Record on Cyber Security” 29 August 2001 http://www.nipc.gov/pressroom/pressrel/wiser082901.htm
6. Black, Jane - Business Week Online. “The High Price of Spam”. 1 March 2002 http://www.brightmail.com/external_cache/BW_Online___March_1__2002___Th.html
7. Olsen, Stephanie - CNET. “Spam flood forces companies to take desperate measures” 21 March 2002 http://news.com.com/2009-1023-864815.html
8. GFI Software. “Why Anti-virus Software Is Not Enough: The Urgent Need for Server-based Email Content Checking” http://rr.sans.org/email/GFI_antivirus.php
9. GFI Software. “Protecting Your Network Against Email Threats: How to Block Email Attacks & Viruses” http://rr.sans.org/email/GFI_email_threats.php

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.