OARtech
10/13/2004

Introductions
Virus and Spam products

[was late, sorry]
Ohio Northern - open source, spam assassin, sophos
Wright State - spam assassin, sophos
U of Rio Grande - Symantec Enterprise, IpSwitch imail with Symantec
Heidelberg - Symantec on desktop, open source on servers
OARnet - McAfee on Desktop
AFIT - Symantec on desktop and for gateway use Norton mail gateway
Mount Union - Sophos, Norton on Desktop
Sinclair - tagging spam, McAfee on both desktop and server
U of Akron - spam assassin and McAfee
?- Norton
Edison - Antigen, Sophos
Denison - McAfee, Sophos and Spam Assassin
Kent - McAfee, Spam Assassin

Virus - 50/50 McAfee vs Norton
Spam Assassin - [missed count]

Computer Associates Etrust (?) virus product used at one institution. Found they were much more responsive on new virus than other products they had used.

Wright state did a test of several packages to find out how they wanted to use anti-spam products. They thought that spam was important to users and moved up the implementation. They only have 2500 people out of 23000 that have signed up to use the anti-spam product. They feel that education of the user is critical. The other thing they have done is that the front end mail gateway runs mail through virus (Sophos) then goes to anti-spam gateway. For those not in the anti-spam they are labeling some of the spam as spam or fraud.

Has anyone begun looking at spyware campuswide? Pest Patrol is used on one site. It was noted that these products are expensive. It has been heard that McAfee will be adding some anti-spyware to their product.

Kent was finding so many resnet computers with viruses that they stop all SMTP to their own gateway and off campus from the resnet and forced the users to use web mail. Other sites have done this as well.

Some have installed Perfigo or Bradford Manager to help with

management of resnet. Ohio Northern is using Perfigo without the client. They had a real smooth startup. They sent out a CD with anti-virus software to students before they arrived on campus. The only problem with Perfigo is they are using it for some bandwidth management as well. Denison is using Bradford Manager and found it worked well for quarantining open and infected systems.

Question - who was actually quarantining their spam? [missed total count] One site described that they did to implement it and used GWguard which has a web interface to the quarantine.

Lots of sites are blocking ports at the firewall and some use OARnet to set blocks. Recommend that users use VPN to access any tools that require special ports.

One site had OARnet block port 445.

It was noticed that Blubster will quickly overwhelm the packetshaper with the number of connections.

How many sites are looking at blocking peer to peer all together? About 4 sites. University of Rio Grande described how they went about blocking it completely.

There was a working group within the I2 group and Case Western felt there were valid reasons for using peer to peer in an academic environment. There is a peer to peer working group and a bandwidth management working group in I2. If you are interested in what is happening with I2 on these areas see the I2 website and look for their working group info. Some sites have looked at contracting with Napster to provide to the campus.

OARnet update
Linda Roos

http://tfn.oar.net - tfn updates, map, etc....
Columbus metro ring is carrying production traffic.
Cincinnati, Dayton, Toledo ring in production
All others have been tested and accepted.

All sites will be connected to the TFN via 1 method: directly connected, via old pops, or via circuits.

Last Mile - SBC has signed contract with a number of schools for GigE and OC3 with costs in the DS3 range. Linda will be sending another spreadsheet with actual prices from SBC for the schools. After circuits are

ordered, it will take about 90 days to get the circuit up.

Support
http://portal.oar.net has links to Stat Scout and other tools available for the various sites.

Upcoming meetings: Regional TFN meeting at Cleveland State 10/18, OSteer meeting next week at the Holiday Inn on the Lane.

Is there a place on the web where advantages/services that Oarnet provides are listed? There is no place currently, but Linda feels it would be a good thing to have in an FAQ.

You can call the support center and they can send you a copy of the router configuration.

Does Oarnet provide any guidelines for doing H.323 and other distance learning tools? There are guidelines for using the Oarnet MCU. There is no central document. If OARtech were to come to some agreements on the standards and write the documents Oarnet would be willing to help. SIP protocol is coming alive for desktop distance learning. But there are several security concerns with SIP. 384 is the standard, but some are starting to use 768.

What is the most prevalent protocol for Video Conferencing? Oarnet is an H.323 provider so that is what they see. They are constantly asking that the H.323 equipment be placed outside the firewall and packet shapers.

Question on Stat Scout. The site wants to look their router but had to go through a number of other Dayton equipment to get to it. Have things changed? They are using a new naming convention for all the sites. Mount Union, Antioch and Sinclair may be having problems getting Stat Scout information on their router. Check again in a few days and see if it is fixed, if not call the support center.

Is anyone putting cable TV multicast over their network? 1 site raised a hand. The questioner's campus doesn't have a cable head end on their campus and are looking at the network as a possible way to distribute the channels.

Lunch

Sophos
Anti-virus and anti-spam for business

Don Landers and Charles Waelde

Convergence of Virus and Spam has allowed Sophos to work in both arenas. They focus on corporate environments and universities. They do not do retail sales.

They have virus labs all over the worlds and are able to catch viruses from Asia and Europe before they get to the US. They make changes to the virus patterns up to 8 times a day based on the information they get in the labs. Sales and support offices have failovers in several areas of the world.

They are seeing a convergence of virus and spam with more mass-mailing windows viruses and backdoor trojans that open the way for remote access tools. They have purchased Active State (now their product Pure Message). Their new engine now can find the variants of viruses.

They cannot legally remove spyware because someone has clicked on an approval message to put the software on the system.

They have enterprise level solutions that run on almost any platform. Their products are Sophos Antivirus, Pure Message, and Enterprise Manager.

Sophos Antivirus runs on desktops, laptops, and file servers and has on-access, on-demand, and scheduled scanning modes. They have central notification and alerts and auto-update. They use checksums to speed up the scanning process to eliminate multiple un-necessary scans.

Pure Message is an email gateway filtering software and provides consolidated protection against viruses, spam and other email-borne security threats. Subscription software with 24/7 support and automated updates that is inclusive in the license for the software. Pure Message runs on UNIX and Windows/Exchange servers. The UNIX version is written in sieve so is very flexible in how it functions. It can give end users control. It can control the email it what is quarantined and when you want things released from quarantine. The Windows version can do either quarantine or delete of suspicious attachments. Also allows end users to control their quarantine.

Small Business products are for small sites with a small number of servers.

They use multiple techniques to identify spam and compute the spam probability rating for each message (0%-100%). The anti-spam rules are continuously updated by the labs.

They have headquarters in Boston, Vancouver, England and several other areas throughout the world.

Pure Message
They did a demonstration on both the Linux and Windows products. Their software runs on several versions of UNIX (Solaris, Linux, SUSI, etc). It can run with Postfix on Linux and can use Postgresql. They are not working with Oracle at this time. Their anti-spam rules are configured similar to firewall rules and do allow users to opt-out of the anti-spam. You can set some users to get their mail and for others to have it quarantine. The sieve script can be saved and pushed out to other servers throughout your organization. You have control over what you want users to be able to do and what you don't want them to do. You can control what is considered internal and external servers. They check spam in other languages as well as English. You have access to see how they check for various spam identifiers. The software does both blacklists and white lists and allows you to test the rules. The quarantine interface allows you to scan the quarantine via from/to/subject/date etc... The users can view the spam via a webpage or via a digest email. Users are able to opt out of the digest, and are able to indicate the hold time. The administrator can look at the user's white and black lists. You are able to report on several different areas. They have canned reports for the most common requests and you can have standard reports email regularly as you wish. You can have one machine manage multiple machines with Pure Message. They have a request support screen that will attach the information needed for troubleshooting. They do have the functionality of the allowing the users to look at a message without releasing it, but have found they prefer the users to release the messages since they do not allow virus messages out.

How do they know the users? The software is LDAP and Active Directory capable and use the email address to determine the quarantine users. You can create separate users if you wish.

Windows version will run with any SMTP server in addition to exchange. The UNIX/ Linux version is a little more flexible. It has the capability of controlling what users can get scanned and any you want to have opt-out and has the ability of blocking messages based on number of recipients, subject attachment names, etc.... You can also take actions based on the type of threat (infections, spam, attachment threat, etc...) and can change the subject tags for several types of spam. In the Windows product you tell the server how to handle the spam based on the spam score. You do have control on the digest content and when they are sent. You are able to add a disclaimer to messages if you wish and the software creates a log that you can look at and parse if you wish.

Where is the heart of the load balancing between multiple records? They run at the application layers so the load balancing does not affect their software. They can work in both the networked environment and in a cluster environment. In the UNIX/Linux version the users will come to the consolidated quarantine to look at their messages. The end user server can point to the consolidated and gives you redundancy for access to quarantine.

Can it run with IpSwitch email? He hasn't but if it is an SMTP email server there shouldn't be a problem.

Demo disks are available. If you are interested in more information you can contact Donald.landers@sophos.com.

T-shirts, memory sticks, and an IPOD were given away.

Ransel Yoho
Ransel requested suggestions for future meetings? Patty Vendt suggested that at either the beginning or end of the OARtech meeting we have a security meeting. Minutes would not be taken and it wouldn't be streamed to allow a more closed section for that time. The general consensus seems to be positive for this idea.

Suggestions:
How you integrate things? IDS, etc...
How you do rate limiting and how "smart" you can make a switched network.

Minutes were approved.
Meeting adorned 2:20