

SoBig? *So what!*— thanks to GWAVA

"I slept pretty well last night, actually," said Peter Oemichen, one day after the SoBig virus tore through computer systems around the world.

His GroupWise network was protected by GWAVA. While his colleagues throughout Wisconsin were scrambling to disinfect their systems from the August 2003 variant of the SoBig virus, the head of information services for the state-run Wisconsin Historical Society was able to rest easily.

"GWAVA didn't even slow down," he reports.

SoBig-F arrives in e-mails with innocuous subject lines like "Your Details," "Your Application," "Thank You!" and "Wicked Screensaver." If the recipient opens the .pif or .scr attachment, SoBig-F strikes, infecting the computer, then e-mails itself to other computers using the infected computer's address book.

The August attack made many networks grind to a halt until IT staff could cleanse the computers. Mr Oemichen, his staff, and their users, were spared the trouble and frustration of having to do so, because GWAVA kept their network inoculated.

GWAVA's four strengths: post office protection, virus blocking, ease of administration and flexible rules meant that GroupWise administrators could say "So what," when asked about "SoBig."

Letter of Thanks

"My hat off to GWAVA!!! We were bombarded by the SoBig over the last couple of days. Yesterday in particular—literally thousands of them. It was so bad we had to stop archiving blocked attachments to save space on the e-mail volume. Can't thank you enough," he wrote to the GWAVA developers the attack was deflected.

The state agency's GroupWise network boasts more than 200 and 250 users and shares resources with other networks, like the University of Wisconsin. Academic users send many kinds of attachments to each other, and then leave the documents on the mail system for further study. "We have a lot of librarians, and archeologists and museum curators who retain their data for a long time," Mr Oemichen explains. "We have 125,000 attachments in our message system."

Despite the colossal load of attachments, more than eight gigabytes in fact, GWAVA was able to weed through them, analyze and block SoBig, all the while allowing legitimate e-mail and attachments through.

"We never missed a beat," Mr Oemichen marvels.

GWAVA's Post-Office level scanning means that even infected GroupWise networks can be disinfected. Even infected systems benefited from GWAVA 2.5x on GroupWise 6.5. Adding the *.SCR and*.PIF attachment blocks and performing a post office sweep eliminated SoBig-F from their post offices.

Easy Administration

Staff providing information technology services have a different work day every day. "I wear the e-mail administrator hat and the network administrator hat." With many responsibilities, tools making life easier are a must.

Once GWAVA is installed on the MTA, the licence key entered and the rules are set, Mr Omeichen says, "you let it run." The heuristical analysis, real time blackhole lists, attachment blocking and easy rule creation operate without supervision. Blocked messages are set aside automatically. GWAVA's archive viewer makes examining messages that were flagged as spam, or suspicious attachments a simple task to complete upon request.

"The other thing I like is the flexibility."

Because so many users on his system send attachments, Mr Oemichen says he had to cap the size of appended messages. Fortunately, rules are easy to generate and customize.

"If I want to block at four megabytes, but I trust you enough to not to leave that on the server for a long while," he cites the example of a public relations employee who must transfer massive files to the media, "I can create an exception to that rule."

All the ingredients for success

Today's GroupWise administrators can count on the technologies GWAVA provides: post office protection, virus blocking, ease of administration and flexible rules. These strengths make GWAVA the outstanding choice for maintaining a functioning network even when faced with the most serious threat.

GWAVA protects Novell GroupWise inside and out. Period.

Background

GWAVA is the leading eSecurity software for Novell GroupWise. Post office level scanning allows GWAVA to monitor all e-mail in GroupWise 6 to ensure communication is both virus and spam free.

"GWAVA is uniquely focused on eSecurity software for Novell GroupWise," notes Charles Taite, Chief Technology Officer for Beginfinite, makers of GWAVA. "We have made a conscious decision to invest resources in Novell and its GroupWise platform. Thanks to Novell and DeveloperNet's invaluable assistance, we have been able to build GWAVA: a tightly integrated YES Tested & Approved eSecurity solution for GroupWise. The rapid adoption of GWAVA, and the very positive response from the GroupWise community, is proof-positive of the value of working with DeveloperNet and Novell's YES Testing program to develop high-quality solutions for Novell platforms."