



Enterprise Reporter Assists San Diego High School in Preventing Potentially Fatal School Shooting

Client:

San Diego City Schools

Web Site:

www.sandi.net

Number of Users:

136,000

Requirements:

Web Filtering and Reporting

Solutions:

R3000 Internet Filter and Enterprise Reporter

“Our Enterprise Reporter was key in collecting the exact data we needed in a very short amount of time. Within 24 hours the information procured helped narrow the number of suspected students to less than a dozen.”

Grant Gutstadt
Security Administrator

Profile

San Diego City Schools (SDCS) serves approximately 136,000 students. It is the second largest district in California, and eighth largest urban district in the United States. The student population is extremely diverse, representing more than 15 ethnic groups and over 60 languages and dialects. The district has more than 200 educational facilities with 14,500 full-time equivalent staff positions representing more than 15,800 employees. The district's educational facilities include 113 elementary schools, 23 middle schools, 27 high schools, 4 atypical schools, 10 alternative schools, and 25 charter schools, totaling a user count of approximately 50,000. The district's mission is to improve student achievement by supporting teaching and learning in the classroom.

Challenge

In late May 2005 a teacher at one of the district's larger high schools in San Diego, CA received an anonymous death threat via his school email account. Through the verbiage used in the email it was clear that it was written by one of the teacher's students. Due to the life-threatening nature of the email, and the fact that the student had imposed an actual date that the violence would occur, it was critical that the student who sent this email be identified immediately and handled accordingly.

The email was forwarded to the high school's Network Technician, who then brought in Grant Gutstadt, the District's Security Administrator, to help him work the case.

Solutions

“The initial information I was able to obtain from the forwarded email and headers was the actual time the email was received by the teacher, the sender's email address, and what email account the sender was using (a Yahoo! account originating from a Hong Kong-based server). From the header originating IP address it was apparent the source host was located at the high school site itself - indicated by the fact that the public IP address was that of the sites external network interface,” Gutstadt says. Using this data, his next steps were to isolate the host computer's source IP address used by the individual at the school and provide the site technician and school police with the information necessary to identify the classroom that contained the computer where the message originated, and possibly isolate the machine used. To do this Gutstadt utilized Marshal8e6's Enterprise Reporter (ER).

The Enterprise Reporter is the only stand-alone appliance that reports on Internet usage without compromising filtering speed/performance or any other server/network functions.

Built on a dedicated MySQL server database that works in conjunction with the 8e6 R3000 filtering appliance, the ER processes and generates detailed or summarized reports in a fraction of the time of competitive products, making it the fastest and most flexible reporting solution developed to date. Using data procured via the

district's ER, Gutstadt was able to obtain the exact time stamps on when the Yahoo user logged in and sent the threatening email in question, and the internal IP address of the Cisco content engine through which the sender was connected. From corresponding log information in the Cisco caching engine the specific Yahoo user's host IP address was obtained. A network scan of the IP address revealed it was online and fingerprinting identified its configuration as likely a student computer. With its subnet belonging to one of the site's internal wireless networks, the host's network card MAC address was determined and identified as currently logged into a specific classroom's Access Point, one of ten computers currently in use in that class. "Our Enterprise Reporter was key in collecting the exact data we needed in a very short amount of time. Within 24 hours the information procured helped narrow the number of suspected students to less than a dozen," he explains.

"Fortunately these kinds of incidents don't happen very often at this particular school, but with violence in schools being an ongoing issue throughout the U.S., it is important for schools to take the proper precautions and be prepared to react quickly when these situations arise. All schools should have a solution in place like the Enterprise Reporter, which was the critical element in preventing a potentially fatal tragedy at our school," Gutstadt added.

Result

Due to all of the data Gutstadt was able to collect using the 8e6 Enterprise Reporter, the site technician was able to isolate the exact computer used to email the death threat. With the supervision of a police officer, the computer in question was identified by matching the machine's keyboard's wireless network card's MAC address to the information provided by Gutstadt. Finally, by using the physical computer checkout records from the day and time the email was sent the site technician was able to identify the student to whom that machine was checked out that day. The suspected student was then apprehended and arrested, and will be legally punished accordingly.

By using the data provided by the ER, the school district's network and security personnel were able to prevent a potentially fatal incident from occurring at the school. "Our Enterprise Reporter server has provided us important data on critical occasions such as this one, which is invaluable to any school system," Gutstadt says. "With more than 50,000 users, Marshal8e6's solutions afford us excellent protection for students and staff, and allow us to maintain a single policy across our 200 school sites. This simplifies our support needs and we are able to allocate our resources - which are always in short supply - to other critical support needs."

About Marshal8e6

Marshal8e6 is a global provider of Secure Internet Gateway products for organizations of all sizes. Marshal8e6 is the only security company capable of delivering comprehensive content security across multiple delivery platforms, including software, appliances and Software-as-a-service (SaaS). The company's complete security portfolio delivers the tools necessary to manage and secure email, Web and the endpoint as well as protect against data leakage. Today, more than 16 million end users in more than 20,000 companies in 96 countries rely on Marshal8e6 solutions to protect their businesses at the email and Web gateway.



Corporate Headquarters Marshal8e6

828 West Taft Avenue
Orange, CA 92865
United States

Phone: +1 (714) 282-6111
Fax: +1 (714) 282-6116

International Headquarters Marshal8e6

Renaissance 2200
Basing View, Basingstoke
Hampshire RG21 4EQ
United Kingdom

Phone: +44 (0) 1256 848 080
Fax: +44 (0) 1256 848 060

Asia-Pacific Marshal8e6

Suite 1, Level 1, Building C
Millennium Center
600 Great South Road
Auckland, New Zealand

Phone: +64 (0) 9 984 5700
Fax: +64 (0) 9 984 5720