

Palm Beach Atlantic University (USA)

3Com, TippingPoint Free Palm Beach Atlantic University From Crippling Virus Attacks

Organization: Palm Beach Atlantic University

Location: West Palm Beach, Florida, USA

Employees: 800

Market Segment: Higher Education

The Challenge

Millions of malicious self-replicating packets flooded the campus network. Internet access and e-mail ground to a halt due to all the unwanted traffic. The congestion prevented most students and faculty from retrieving their applications and data. Overloaded computers crashed, and the university's web site was not functioning. Connectivity to residence halls had to be shut down. Worse, the malware was emanating internally on the network because of the inadvertent actions of legitimate users. The university was crippled and had to take action immediately.

This grim scenario, the nightmare of network administrators worldwide, is precisely what the IT team at Palm Beach Atlantic University (PBA), www.pba.edu, confronted. In attacks that threatened several other universities as well, students at PBA inadvertently opened instant messages or web sites that contained a spate of malicious traffic like the sdbot worm. Although PBA uses a firewall to safeguard such confidential data as faculty research and students' medical and academic records, the device was unable to defend against worms and internal attacks threatening the school's authorized users.

The result was grave. Every available computer on the network was threatened as a plethora of bad traffic quickly congested the entire network—all but bringing services to a halt. Many students and faculty were unable to communicate with each other or with the Internet. The school's Web site became virtually inaccessible to the outside world.

"The worms all but disabled our school, compromising classes and other operations," said Chad London, infrastructure administrator for PBA. "Our firewall protected our perimeter against intruders, but it is not designed to protect against threats accidentally invited in by our students. We were in deep trouble and needed help very quickly."

Why TippingPoint, a division of 3Com

Several members of PBA had attended the 3Com Live event this year where they saw a demonstration of the TippingPoint™ Intrusion Prevention System. The system thoroughly inspects packets, blocking malicious and unwanted traffic while allowing proper traffic to pass unimpeded. The system is the industry leader, recently receiving Best Security Solution 2005 from SC Magazine.

Impressed by the solution's performance and capabilities, the PBA team requested an on-site demonstration. Recognizing the urgency of the university's need, 3Com and TippingPoint sales representatives worked together to install a TippingPoint system on a segment of the university's network the following day. Within the first hour of the system's installation, the device blocked

over one million attacks on the network and restored the school's Internet connectivity.

"We were awestruck by how effectively the TippingPoint system repelled attacks right out of the box using its default settings," said Herman H. Silva, network security analyst for PBA. "Right away, we knew we had the one solution that could safeguard our network from all the insidious exploits swarming about the Internet. We also appreciated the responsiveness of the 3Com and TippingPoint teams. They were committed to solving our problem and restoring order and functionality to our campus."

A proposal for a complete deployment of TippingPoint products was submitted to PBA's president and quickly approved. In March 2005, only 10 days after the initial TippingPoint demonstration, PBA installed three TippingPoint Intrusion Prevention Systems in addition to its already installed evaluation unit. It also deployed the TippingPoint Security Management System (SMS), a hardened appliance that enables administrators to monitor and control multiple TippingPoint devices.

PBA placed one TippingPoint system directly behind the firewall at its 15 Mbps DS3 Internet connection. It deployed the others at strategic locations on the network, including the links to the school's server farm and residence halls. Consequently, traffic from anywhere within the network must pass through a TippingPoint device.

"Deployment was a piece of cake," added Silva. "This is pretty remarkable considering the sophistication and power of the TippingPoint systems."

PBA installed the following TippingPoint products:

- **TippingPoint Intrusion Prevention System**
- **TippingPoint Security Management System**

The Benefits

With its TippingPoint solutions, PBA was able to safeguard its network traffic and securely continue its education of students.

Within four days of their deployment, the TippingPoint Intrusion Prevention Systems blocked over four million bad packets on PBA's network. Once PBA IT staff cleansed users' networked systems of self-replicating infections, the TippingPoint solution restored the performance of all services, including Internet access and e-mail.

"The TippingPoint systems are so effective because they look beyond packet header information right into application layer payloads, separating legitimate traffic from malicious code," said London. "One would think that such deep inspections would degrade networking speed, but on

the contrary, by eliminating all of the unwanted traffic, the 3Com solutions improved performance.

The capability of the TippingPoint systems to defend against threats that are internally-launched as well as those that emanate externally to the network was essential for meeting PBA's needs.

"Routers, switches, servers and even firewalls are all network components vulnerable to attack," explained Linda A. Ward, director of technology services. "Our TippingPoint systems safeguard these components, providing powerful protection for our entire infrastructure. What's more, they protect our network's availability and performance by eliminating the threats that undermine its stability."

The Digital Vaccine® service of PBA's TippingPoint Intrusion Prevention Systems ensures that the devices are always updated to thwart the latest threats and often protect in advance of attacks. New filters are delivered to customers weekly or immediately when critical vulnerabilities and threats emerge, guarding operating systems and other network components.

"Thanks to Digital Vaccine, we're able to block not only current threats like the Nachi worm, but their future permutations as well," said Silva. "What's impressive about TippingPoint's filters is that unlike most other intrusion prevention systems, they target not the exploits themselves but the vulnerabilities. This approach eliminates the weaknesses in networks that hackers exploit, protecting the infrastructure against future attacks."

Administrators use the TippingPoint SMS platform to control and monitor their intrusion prevention systems. It also provides comprehensive reports and real-time graphs on traffic statistics, filtered attacks, and network hosts and services.

"TippingPoint's SMS is a blessing because it simplifies management and reduces the cost of ownership," explained London. "We can administer all four of our TippingPoint solutions either together or individually. We use SMS to distribute the Digital Vaccine filters and can tailor each system for its particular needs easily and quickly, optimizing their effectiveness."

The TippingPoint Intrusion Prevention Systems also perform bandwidth management, so that customers can reclaim bandwidth by cleansing the network of malicious traffic and throttling non-critical traffic, such as Peer-to-Peer file sharing.

"Our TippingPoint solutions will minimize the unwanted traffic entering and clogging our system," said Ward. "They provide performance protection by keeping bandwidth free for only authorized usage."

"Thanks to 3Com, we're now positioned to offer our students the best education we can without fear of network disruption or failure," concluded London. "TippingPoint is the benchmark for network-based intrusion prevention."