



The University of Texas Health Science Center at Houston Prescribes TippingPoint for a Healthy Network

The University of Texas Health Science Center at Houston was created by the UT System Board of Regents and supported by the Texas Legislature in 1972. Located in the world renowned Texas Medical Center, it brings together a dental school (established in 1905), a graduate school of biomedical sciences (1963), a medical school (1969), a school of public health (1969), a school of nursing (1972), a school of health information sciences (1997), a psychiatric center (1986) and an institute of molecular medicine for the prevention of human diseases (1995). The university pursues its mission through a comprehensive approach to health. The network is comprised of approximately 8,000 workstations and servers.

The_Problem

According to Randle Moore, Senior Network Security Analyst, the university was experiencing worm and virus infections that were attacking servers, consuming network bandwidth and causing considerable network downtime. The university's main decision to purchase the TippingPoint Intrusion Prevention System was to prevent vulnerable (unpatched) systems from being exploited until patches could be adequately tested and rolled out.

The_Solution

After implementing the TippingPoint Intrusion Prevention System, a high-speed device that blocks malicious traffic, the university has blocked an average of approximately 100,000 attacks per month. In 2003, the university blocked over 100,000 Sobig.F virus infected e-mails per hour for almost a month. The university also regularly blocks new Welchia

infections from users bringing their laptops from home onto the network.

Value_Proposition

With TippingPoint, malicious traffic is automatically blocked before damage is done. Per Mr. Moore, the most beneficial aspect of the TippingPoint implementation is "the capability to not only see what is going on, but also to be able to do something about it."

Return on investment (ROI) can be calculated several different ways. ROI calculations should be different for each organization, and are dependent on external forces and formula variations.

In this case, a very basic formula for ROI on intrusion prevention is:

$$(\text{REPAIR TIME X ATTACKS BLOCKED X WAGES}) = \text{ROI}$$

"Since introducing the TippingPoint appliance into our network, it has more than paid for itself by preventing numerous worms and viruses from even entering our network. Over the past three days alone, the device has stopped between 30,000 to 45,000 virus-infected emails per hour from the Internet"

Randle Moore
Senior Network
Security Analyst
UT Health Science
Center—Houston

Mr. Moore estimates the following numbers apply to the university:

1. Time to patch a system: ~20 minutes
2. Time to fix an infected workstation ~2 hours
3. Average system administrator's hourly wage: \$25 per hour
4. Estimated cost savings of the TippingPoint IPS?

which at a minimum, equate to spam. Using his extremely conservative \$0.05 of wasted productivity per spam e-mail a user has to deal with, those savings equal \$250,000.

Total savings from TippingPoint implementation = \$400,000, which more than covers the cost.

Given Mr. Moore's conservative estimate of preventing ~3000 actual infections to-date, the above numbers give a savings of \$150,000. Mr. Moore reports the university has also blocked many millions (~5) of virusinfected e-mails,

Corporate_Headquarters: 7501B North Capital of Texas Hwy. > Austin, Texas 78731 USA > +1 512 681 8000 > +1 888 TRUE IPS
European_Headquarters: Herengracht 466, 2nd Floor > 1017 CA Amsterdam, The Netherlands > +31 20 521 0450
Asia_Pacific_Headquarters: 47 Scotts Road #11-03 Goldbell Towers > Singapore 228233 > +65 6213 5999