



Measuring Vector Defense, Part II

infectionvectors.com

September 2004

Overview

In Part 1, the reasons for using metrics to evaluate security was introduced. Specifically, the means in which an organization may measure how prepared their employees are for virus attacks. Sampling the user population is an important step when assessing the overall network security posture.

This section discusses what to do once those measurements are taken. With those numbers, it is possible to estimate how well training programs are working and how much more should be invested in awareness.

Return on Investment

Security ROI discussions can be dry and uninspiring. However, the basic concepts are important to executives, and therefore to everyone else in an organization. The ROI numbers for security projects are often very fuzzy; many IA managers want to cling to fearful tales of “we can’t afford to not be secure” that don’t address specific issues within the company. There are many security issues where an organization can, in fact, afford to be vulnerable. It may be that the fix is more costly than the clean up or it may be that the company simply cannot afford to purchase additional technology.

Beyond purchasing new hardware and software, training expenses also play a big role in a network’s security. There are many ways to reduce the number of compromised machines every year, whether through technical or social means (see the discussion of finding the right tool for the right job, technical or social in the previous report and in the “Human Vectors” paper). Each solution, whether a new firewall, a client-based IDS, or awareness program has its own costs and benefits. Furthermore, each organization will find a different level of benefit from each plan. The optimal balance of technical and social programs at one place may be completely wrong for another. It is only possible to find the right balance by measuring the success of each program, calculating the costs, and then tinkering with the mixture.

The first part of this report discussed ways to measure the training portion of a company’s plan. There have numerous articles focusing on how to calculate the return on virus software, firewalls, and other technical components. Training, however, is often not included. It may be that a company finds that 2 hours of security training every quarter for every employee offers a much better return than a new IPS system or email-scanning suite of tools. This will sound like heresy to some engineers and technical consultants, but remember, every organization needs to find their own balance.

Make Sense of the Numbers

To find that correct balance, a very basic analysis of the return figures is all that is required. Identify precisely what is to be mitigated. Decide how much mitigation for each problem is required/desired. This can realistically be achieved only by charting the results over time, as the programs are rolled out. Over that time, there will be nebulous measures of success, subjective “How does it seem to be doing?” reactions. These are not worthless, but they are hard to spend money on. Taking the time to find out if training is working will help end disputes and greatly improve management’s ability to allocate funds for security initiatives.

Copyright © 2004 infectionvectors.com. All rights reserved.