



Measuring Awareness
infectionvectors.com
October 2004

Overview

Awareness training can significantly cut the time and expense involved in cleaning up virus infections. Although it is not the only answer to the malware problem that exists, it can be an important layer in the malware strategies of most enterprises.

Recently, a number of articles have been aimed at promoting or bashing end user training as a means to control virus spreads. Articles that favor education point out that users are the “weakest link” in information assurance, while still saying that security is a complicated business. Writers that decry awareness training also state that the complexity of technology means that only improved technology can solve the problem. Many writers also point out that advanced black hats will always understand the technology (and how to beat it) better than users trying to defend their PCs. This is absolutely true; moreover, it points out precisely why awareness training is necessary: trying to solve social problems with technical answers is the proverbial square peg in a round hole. There is no way to keep up with professional crackers with additional technological “fixes.” There are many Internet problems that mirror “real world” issues: knowledgeable individuals deflect all scams, cons, theft, etc. Often, technical tools help this defense, a home security system is a great tool to deter and identify theft. However, tools can be left off, disabled, or provide false positives/negatives. If someone saw a stranger in their house, they would not ignore them simply because the alarm system did not fire. Giving users the impression that they can trust their antivirus or IDS without question as an infallible system ignores the great benefits of an informed user base. Users can be a very powerful layer in an enterprise anti-virus strategy.

How can the training program be measured? It is incumbent upon nearly all corporate programs to provide a metric for measuring success or failure, costs and benefits. Measuring the success of virus defense has been addressed in other infectionvectors.com reports. This report looks specifically at user virus-awareness training.

Awareness

Defining what a company hopes to achieve through virus awareness is an important first step. This can often be answered with the answer to “why are we implementing the training?” Many times it is in response to a recent outbreak. In these cases, it is likely that the organization is hoping to reduce the costs associated with cleaning up infections.

More generally, however, the goal should be to empower users to make critical decisions about the security of their computers and the information for which they are responsible.

Once a user understands why he/she is a target, the basic tactics a criminal will employ, and what puts them at risk (and how to deflect those vectors), they will make decisions that benefit the enterprise. Security training does not have to be complicated; there is no magic to the tenets of information assurance for a user: don't trust things that are intrinsically untrustworthy, report changes in ordinary system activity, ensure security software is doing its job.

Measuring Training

There are lots of ways to measure training programs, from testing users with a quiz to testing them with real-life scenarios. The best test is to see how many infections are reported each month by the anti-virus console and how many hours the administrators spend cleaning up after worms.

This excerpt from the "[Measuring Success](#)" report explains a number of the possibilities:

Virus Culture Metrics

Self/Company Assessments

In addition to asking users what they know about safe computing practices, it is important to gauge how secure they feel on the organization's LAN. Questions such as "How safe and reliable is data stored on company servers?" may be very helpful in uncovering the perceptions the users have about the network.

Response Audits

"What would you do if you received the following email, pop-up, warning, etc.?" type questions are distinct from the previous assessment in that they determine how a typical user would respond to specific incidents. These measures can be used to diagnose the awareness of the user base. Further, with respect to such issues as phishing and mass mailer tactics, the questions alone may spur dialog that helps train the user how sophisticated an attack may look.

Simulations

Basic scripting or coding knowledge would allow a security administrator to create a simulated "mass mail message" or pop-up warning for a random sample of users (broad scale simulations will likely result in a lot of help desk calls), just in an effort to judge what the response would be. Simulations can also take the form of focus group style meetings, to ask questions similar to those above.

External Groups

Reputable outside organizations can offer a number of tests, from the simple surveying above to real "pop quiz" style assessments and penetration attempts.

With any type of assessment, the goal is simply to create a reliable test that produces a measured score and can be reproduced regularly. It isn't important that the score is imprecise, as long as it does give an accurate reflection of the overall security posture.

The numbers can be charted, progress monitored, and presented to higher level decision makers for action. A steady decline in virus knowledge may be the impetus for additional security training (as opposed to the traditional catalyst for additional education: a major outbreak within the organization).

The value of virus awareness will manifest itself in responsible reactions to phishing scams and opening of attachments (both of which may protect mission-critical data from entering the wrong hands or from destruction). Companies with well-trained users can expect a new and strong layer in their virus defense, one that is not easily affected by new technical tricks (such as the URL-masking of phishers) as users will be skeptical of the underlying, untrustable technology in the first place. Aware users know to ask critical questions about the integrity of messages and protections, even without knowing all of the technical lingo that makes the concept of computer security unapproachable to many employees.

References

“The weakest security link? It’s you” News.com
http://news.com.com/2100-7355_3-5278576.html

“User education is not the answer to security problems” Jakob Nielsen
<http://www.useit.com/alertbox/20041025.html>

“User training is not the answer” Mitch Wagner
http://www.securitypipeline.com/policy_privacy/51200348

“Nothing beats education for beating computer crime” Wayne Rash
<http://www.securitypipeline.com/showArticle.jhtml?articleID=47205281>

Copyright © 2004 infectionvectors.com. All rights reserved.