Defending against virus attacks.

Print

Date: *May 1, 1990*
Words: *1091*
Publication: *Security Management*
ISSN: *0145-9406*

VIRUSES ARE A FORM OF MAlicious software, usually consisting of computer instructions or code embedded in an otherwise useful and trusted program. Whenever the program is run by the user, the malicious code is also executed. The computer system executing the instructions has no way of distinguishing between the instructions of the main program and those of the malicious embedded software. As far as the computer is concerned, a code is a code and it must be okay because it was run by the user.

Viruses are a potentially serious problem that could affect many computer users. The threat of a virus is also a problem because it can generate fear and confusion. There have been hundreds, perhaps thousands, of reported incidents involving real or perceived computer viruses, network intruders, and other intentional acts against large and small computer systems. To date, though, viruses have not caused major damage to critical systems. However, some users have had valuable data destroyed, and some computer systems have not been available when needed for processing. Many hours of valuable staff time have been lost in reacting to both real and perceived threats.

The incidents of data destruction and loss of system availability have occurred in systems that had inadequate security controls or that were not properly managed. Such relatively unconstrained environments often include personal computers and local area networks, where program files can be freely shared. In special-purpose or highly structured systems, such as funds transfer systems or airline reservation networks, viruses have generally been less of a threat because special hardware, software, and procedural control measures are available.

Viruses and other malicious software are not a new or even an unanticipated problem. We must not be complacent about the threat of viruses, but we must not permit the current paranoia - fueled partially by technical ignorance and often fanned by people with solutions to sell to make us lose sight of the many other types of risks involving the use of computer systems and the many types of controls that must be in place to protect those systems.

Accidents and software errors are a more serious threat to computer systems than malicious software. Assuring the quality of software is a major challenge with the increasing dependence of society on computer and network systems and the increasing complexity of the software.

NIST has long advocated establishing control measures to protect information from both

accidental and malicious threats to information's confidentiality, integrity, and availability. Many of the basic controls are already available, but new technology, standards, and controls will be needed as technology changes and new uses are made of computers.

The problem Of computer viruses must be addressed as part of an overall information security program, and the problem itself must be attacked on several fronts-through a combination of technical mechanisms, user awareness, and good management.

There must be organizational awareness of the problem and management commitment to make information security a priority. Programming errors and malicious software can be detected and eliminated through rigorous software development and maintenance procedures and through effective hardware and software access control mechanisms. Virus threats exist where little has been done to control software quality and distribution.

To protect against virus attacks, managers must consider the nature or value of the data being handled or the services being provided by the system, the Motivation and resources of a would-be adversary, and the potential technical vulnerabilities of the specific computer and network environment.

The overall objectives of information security require a systematic, rational examination of the trade-offs between risks and the cost of control mechanisms. Managers must adopt policies, procedures, and technical controls appropriate for the data and the services provided.

Under the Computer Security Act of 1987, NIST is responsible for technical, management, physical, and administrative standards and guidelines for the cost-effective security and privacy of sensitive information in federal computer systems. NIST currently has a $2.5 million program to implement the requirements of the act. The President's fiscal year 1990 budget requested an additional $3.5 million to provide a total computer security program of $6 million.

NIST responded to the 1988 Internet virus incident by working with the Department of Defense, the Department of Justice, the National Security Agency, and other federal agencies in identifying ways to respond to future attacks. One identified need was for emergency response centers to serve various communities of computer users by providing technical advice, ensuring effective response to incidents such as virus attacks, and educating users in protecting information assets. NIST has worked with several agencies to establish this network of response centers. The Defense Advanced Research Projects Agency (DARPA), for example, established the Computer Emergency Response Team coordination center (CERT).

NIST developed and issued a guide for technical managers on reducing the risk to their computer systems and networks from attack by computer viruses, unauthorized users, and related threats. This publication, Computer Viruses and Related Threats: A Management Guide by John P. Wack and Lisa Camahan, discusses the combined use of policies, procedures, and controls to address security vulnerabilities that can leave systems open to attack. (The publication is available for sale from the Superintendent of

Documents, US Government Printing Office, Washington, DC 20402.)

We issued a news release in late September to warn computer users and managers about the potential danger from the reported Columbus Day virus and offered steps that could be taken to protect their systems. We advised users not to overreact but to take prudent actions.

In summary, I would like to temper the current fears about computer viruses with a little sound judgment and perspective. The problem is real, and the potential for damage - especially in certain environments-is quite significant. There are, indeed, many things both technical and otherwise-that need to be done, including developing better tools for preventing, detecting, and removing malicious software and establishing cooperating facilities to react to incidents when they do occur. We already have many of the tools necessary to manage the problem.

Under our expected funding for this fiscal year, we will continue to focus on developing technical and management solutions that address general computer security problems. Although we will not be able to respond to every threatened virus attack, we plan to follow the developments that take place. We believe the general guidance that has already been issued will help users and managers develop their own controls to counter future threats. We will have to rely on the private sector to develop future solutions, and we will try to work with other organizations in getting those solutions into use.