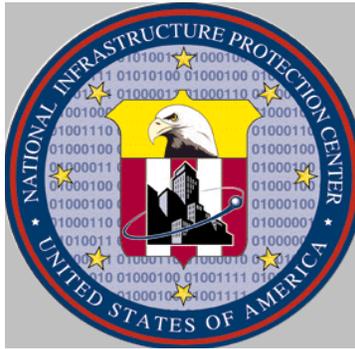


NATIONAL INFRASTRUCTURE PROTECTION CENTER

HIGHLIGHTS

A publication providing information on infrastructure protection issues, with emphasis on computer and network security matters.



Issue 4-01
April 18, 2001

Editors: Linda Garrison
Martin Grand

- ! Teleworkers: Increasing Risks to Corporate Infrastructures?
- ! 911 Under Attack: Emergency System Vulnerable to Denial of Service Attacks.
- ! Computer virus protection: Layers of protection are key to safeguarding systems.
- ! National Infrastructure Protection Center (NIPC), Analysis and Warning Section, Watch and Warning Unit.

For more information, or to be added to the distribution list, please contact the NIPC Watch at nipc.watch@fbi.gov or call (202)323-3204. We welcome your comments and suggestions for improving this product. To provide comments, please participate in our reader survey, or contact the Editors at (202) 324-0334 or (202) 324-0353. A reader survey form is attached. This issue has an overall classification of "Unclassified." This publication may be disseminated further without express permission.

Teleworking: Increasing Risks to Corporate Infrastructures?

Employees connecting to their offices remotely, can be the weakest link in a corporate network's security, and the risk is growing as new broadband technologies proliferate.

Numerous studies indicate that telecommuting is growing in the United States. The International Telework Association and Council (ITAC) states that the number increased from 19.6 million persons in 1999 to 23.6 million in 2000. The number of workers requiring remote access to corporate networks, due to telecommuting, travel, or taking work home at night, is expected to continue to increase.

With the growing numbers of telecommuters, organizations are experiencing new security issues and threats to the enterprise network. For example, many home users do not utilize personal firewall and virus protection products that are as up to date or as robust as corporate products. A malicious person can gain access to a corporate network by compromising a home user's system, and then capturing the latter's steps as he logs in and accesses his organization's network. Adding to the security risks of remote users are the high speed, "always on" Internet connections such as cable modems and Digital Subscriber Line (DSL). Unlike traditional dial-up connections, broadband connections are not terminated when users end their on-line sessions. Another reason for concern is the static IP address associated with these connections. These factors significantly increase the chances for being included in an automated scan for vulnerabilities. The improvement in Internet connectivity technology has increased the level of risk to intrusions on corporate systems. While companies can take steps to protect the computers employees use at work, they have little direct control over the employees' home computers.

The Center for Strategic and International Studies recently issued a warning regarding an instance of an employee's computer being used as a backdoor into a well-known corporate network. Although the company denied that the hacker accessed any source code, the fact that a large company with significant resources fell victim to this type of attack was cause for great concern.

There are several steps that can be taken to protect systems used for teleworking. In addition to installing antiviral software and ensuring that it is kept current, personal Firewalls and Intrusion Detection Systems are available. Disabling any unused or unneeded services such as file and printer sharing can also help prevent attacks. Telecommuters using broadband connection services may wish to re-authenticate with their Internet Service Provider (ISP) to obtain a new Internet Protocol(IP) address, thereby decreasing exposure. Employer-sponsored training programs aimed at teaching employees how to secure their home systems can go a long way in helping to minimize the risks of teleworking. Implementing state-of-the-art technologies such as Virtual Private Networks (VPNs) to encrypt communications or simply turning off one's computer while not in use should also be considered. The most important step is for employees and employers to work together through awareness and education to maintain the security of their systems.

911 Under Attack: Emergency System Vulnerable to Denial of Service Attacks

Instances of denial-of-service attacks in recent years highlight the dependency of 911 services on other Critical Infrastructure sectors.

On February 16, 1968, the country's first 911 call was placed in Haleyville, Alabama. Basic or enhanced 911 services have been implemented in nearly every US emergency services jurisdiction, and the 911 concept has been imitated in many foreign countries.

Virtually every person in the US has become familiar with the ability to summon police, fire, or emergency medical services by dialing 911. However, this system is vulnerable to unintentional or malicious overload. A minor incident may prompt onlookers to dial 911, flooding the 911 Public Safety Answering Point (PSAP) with repetitive information. Furthermore, there have been a number of computer viruses that were designed to automatically and repeatedly dial 911. 911 services rely on the telephone network. Failures in this network, a fire in a telephone switching office, and accidental configuration changes have all resulted in temporary degradations of 911 services in a number of instances.

On March 10, 1997, a Massachusetts juvenile allegedly used his personal computer and modem to access an optical digital loop carrier and interfere with telephone service to the community of Rutland, Massachusetts. The juvenile "intentionally and without authorization@ accessed the loop carrier and "sent a series of computer commands that altered and impaired the integrity of the data thereby disabling the system. Public health and safety were threatened by the loss of telephone service."

In another case, a Swedish computer hacker was convicted of a misdemeanor in 1997 for causing a denial of service attack against several Florida PSAPs. From January through March 1996, a self-styled "phone phreaker" (a person who illegally obtains phone service) obtained the seven-digit phone numbers associated with the 911 trunk lines and apparently used a compromised PBX (Private Branch exchange) to initiate several conference calls between 911 operators in multiple Florida jurisdictions, tying up valuable emergency services resources.

911 and other emergency services communications traverse computers and switches that continue to be vulnerable to computer hackers and phone phreakers. Providing enhanced security measures to protect this equipment from unauthorized tampering, combined with the development and implementation of back-up procedures, should be a priority for 911 planners and those who rely on these services.

Computer virus protection: Layers of protection are key to safeguarding

systems.

Meeting the evolving virus challenge requires concurrent efforts to adequately address the problem.

The importance of anti-virus (AV) product and procedures was underscored this year as several high-profile viruses made headlines and many companies experienced significant losses associated with these infections. Despite the fact that organizations are spending record amounts on AV measures, the problem persists, as indicated by the following:

- A recent Computer Security Institute (CSI) survey found that 94% of respondents detected computer viruses within the past year.
- The CSI study showed 68% of respondents reported viruses causing monetary losses, despite 96% of these same participants employing some form of AV protection.
- ICSA Labs' Virus Prevalence Survey reported that 41% of respondents' organizations experienced 2000's "Love Letter" virus at a level categorized as a "disaster" (25 or more computers infected at the same time), while only 15% of respondents experienced the earlier "Melissa" virus as this level.
- A recent test by Virus Bulletin, found that only 6 out of 17 companies' AV products detected 100% of a representative sample of viruses.

These figures demonstrate that although AV products are being used, companies are still vulnerable to infection. Reasons include: not all products detect all viruses; there is an inherent lag time between a new virus appearing and the time to deploy a new signature; and users may not be downloading the latest definition files and may not be following other best-practice security procedures.

A general consensus in the computer security community is to approach the problem with a model using layers of protection, including the employment of multiple methods in multiple locations, combined with an overall security policy that clearly addresses proper procedures. There are several technologies to consider when evaluating AV products, such as activity monitors, integrity checkers, and scanning functionality. A combination of these technologies is usually recommended, since the aim is to balance the strengths and weaknesses of the different products. Other factors to consider include whether or not a product can disinfect after a virus; the timeliness of definition files and the ease of updating the existing software; and product support/customer service.

Deciding where to deploy AV technologies is critical. Most experts recommend protections at every point of entry: gateways/firewalls/proxy servers. Servers and client desktops also require protection. Special attention should be placed on protecting e-mail servers, as this has been a primary method for introducing viruses into an enterprise.

High-level organizational policy regarding security procedures, such as employee training, regular virus scanning, proper media handling, should also be addressed. Entity-wide configuration settings requirements for word processors, web browsers, and e-mail can also assist in avoiding certain types of prevalent viruses.

**National Infrastructure Protection Center (NIPC)
Analysis and Warning Section**

Watch and Warning Unit

The NIPC Watch and Warning Unit, housed at FBI Headquarters in the Strategic Information and Operations Center (SIOC), serves as the NIPC's primary information collection, coordination, and dissemination center. Supported by a staff of FBI, Military, and other federal government agency personnel, the NIPC Watch is a 24-hour, 7-days-a-week operation. The Watch is tasked with maintaining real-time situational awareness, providing rapid warning, and supporting the NIPC's response to critical national infrastructure events by coordinating with NIPC/FBI management and field Agents, federal agencies, state and local governments, and private sector entities. The NIPC Watch also monitors broad international cyber and infrastructure activity and maintains continuous external liaison with major national organizations.

The Watch produces the NIPC Daily Report which is disseminated to FBI, U.S. military, federal agencies, and InfraGard members. The purpose of the Daily Report is to provide our customers with a "snapshot" of events that we deem to be relevant to our current or future state of readiness in the protection of our nation's critical infrastructures. Significant Changes and Assessments, Military, International, Private Sector, and U.S. Government are all categories that are addressed in a group context, with each of the eight critical infrastructures addressed independently (Banking and Finance, Electrical Power, Gas/Oil, Transportation, Telecommunications, Emergency Services, Water Supply, and Government Services).

On a daily basis, the Watch receives and processes numerous cyber intrusion reports as well as telephonic and e-mail inquiries from all over the country and from around the world. Since its inception in February 1998, the NIPC Watch has disseminated eighty-five warning/assessment products. This past February alone, the Watch handled approximately 160 cyber/infrastructure related reports, and addressed over 3,400 e-mail correspondence.

Please direct any questions to the NIPC Watch online at www.nipc.gov or call (202) 323-3204

Questionnaire

In order to provide a service, which is relevant to our clients, we would like your opinions on this publication. Please execute this survey and return to the address at the bottom.

Please circle the most appropriate response

1. Highlights presents issues which are _____ to my concerns.
not relevant / relevant

2. The information is presented in a _____ fashion.
jumbled / clear and understandable / too technical

3. The quality of the information presented is _____.
low / adequate / high

4. The frequency of the publication is _____.
too seldom / adequate / too frequent

5. I find the length of the articles to be _____.
too short / appropriate / too long

6. Past articles have been informative. Yes No

7. What kind of articles would you find helpful in the performance of your duties?

8. Overall assessment.

What is your job title? _____
Would you like to contribute an article? If so, what would the topic be? Yes or No _____

Thank you for your time.

Please return this form to: Editor's, Highlights
 Room 11719, NIPC, Federal Bureau of Investigation
 935 Pennsylvania Avenue, N.W., Washington, D.C. 20535

Fax: (202)324-0311 or E-mail - lgarrison@fbi.gov or
mgrand@fbi.gov

The Editors of the Highlights would like to thank all those who submitted their comments via the questionnaire.