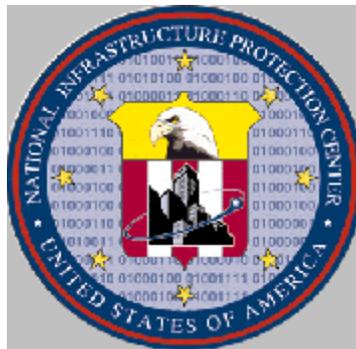


NATIONAL INFRASTRUCTURE PROTECTION CENTER

HIGHLIGHTS

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



Issue 9-01
October 10, 2001

Editors: Linda Garrison
Martin Grand

-
- ! Security Programs: Key to Success Is Coordination and Integration**
 - ! Wireless Networks: Security Concerns**
 - ! Foreign Hacker Awareness of Infrastructure Vulnerabilities**

For more information, or to be added to the distribution list, please contact the NIPC Watch at nipc.watch@fbi.gov or (202)323-3204.

We welcome your comments and suggestions for improving this product. To provide comments, contact the Editors at (202) 324-0334 or (202) 324-0353.

This issue has an overall classification of Unclassified. This publication may be disseminated further without express permission.

Security Programs: Key to Success Is Coordination and Integration

Although often overlooked, physical security is an integral component of a comprehensive cybersecurity program.

The most elaborate boundary control program of firewalls, intrusion detection, and virus filtering will be of little help if an intruder is able to gain physical access to servers, networks, or information. Therefore, it is crucial to understand the interrelationship between physical and cybersecurity in the current technology environment.

Technology Trends

Certain technology trends are exacerbating the risks to information systems posed by deficient physical security.

- In the corporate environment, the increased rate of laptop computer theft increases the risk of damage to or loss of proprietary information and sensitive correspondence. In addition, a laptop may contain networking information that could enable a thief to subsequently gain access to a corporate network masquerading as a legitimate user. Encryption of files and e-mail messages can prevent exposure of sensitive data while locking anti-theft cables, training, and awareness can aid in mitigating the risk of theft for business travelers with laptops.
- Some major credit card issuers now require e-commerce merchants to undergo a detailed security audit; one of the audit requirements is hardened server rooms for storage of credit card information.

Organizational Security

Effective security response requires coordination between several groups, including representatives from business, legal, information technology (IT), and corporate security departments. A current trend is the integration of IT and physical security into a single unit. One major technology vendor announced earlier this year that it had combined its IT security and physical security efforts into one group known as the information assurance program designed to develop an overall seamless security program. Organizing security under one umbrella has the benefit of having a single chain of command in place and a clearer understanding of roles and responsibilities to better facilitate coordination.

The following steps can help facilitate coordination of physical and cyber security:

- Risk assessments should be completed to identify specific physical vulnerabilities in their business model as well as in their networked operations.
- The security implications of emerging technologies such as wireless networks must be thoroughly examined from both a physical and cyber perspective.
- Physical as well as cybersecurity units must have clear lines of communication and authority as well as a transparent working relationship in order to encourage information sharing and coordination.
- Management should be committed to employee training and enforcement of security-related policies and procedures for all aspects of enterprise security.

Wireless Networking: Security Concerns

Wireless networking offers great convenience for mobile users, although the technology's immaturity has led to serious security concerns that must be addressed.

Numerous corporations around the country, including operators of critical infrastructures, are implementing wireless networks in an effort to extend the benefits of their enterprise computer networks to an increasingly mobile work force. However, researchers and attackers alike have found several security-related design flaws in protocols that serve as the basis for most wireless networks.

Drive-by Surfing

The media, for example, has reported instances of external computer users being able to access wireless networks, in a phenomenon that has been dubbed "drive-by surfing." The following reports graphically illustrate the relative ease in which such access can be achieved:

- A computer consultant in the Silicon Valley reported that he was able to map several computer networks merely by driving down the street with a wireless-enabled laptop.
- One individual stated that while sitting in a cab in New York, he was able to browse a portion of the network of a nearby financial institution through his laptop.
- One large technology-based company found that unauthorized wireless access points within its facilities could be accessed from public roads running near its headquarters.

As with the appearance of any new technology, wireless network access will require close monitoring until its security features mature. When one combines the immaturity of wireless security features, a lack of understanding and experience regarding the proper configuration and management of wireless networks, and the readily available attack tools now available over the Internet, the growing concerns surrounding current implementations of wireless networking become self-evident.

At the present time, critical infrastructure operators should consider enhancing their security posture with regard to wireless networking by taking steps such as the following:

- Developing or updating enterprise-wide wireless access policies and standards.
- Demanding products that resist casual snooping.
- Monitoring for any unauthorized wireless access points that a department or user may establish on their own initiative.
- Utilizing application-layer security products to protect data in transit.
- Centrally managing wireless access using network access control, authentication of users, encryption, desktop firewalls, and intrusion detection.

Foreign Hacker Awareness of Infrastructure Vulnerabilities

Computer hackers based in foreign countries have targeted information systems in the United States with a wide array of motives ranging from a desire for financial gain to political activism.

Most of the U.S. information systems victimized from abroad have been targets of opportunity; for example, some victim sites ran an operating system that had a widely publicized security flaw. In some instances, however, intruders have managed to penetrate information systems involved in the provision of critical infrastructure services. Observers have noted with concern an increasing interest in and awareness of the strategic value of network-related vulnerabilities in the United States' critical infrastructures among the global computer underground.

Interest by Foreign Hackers

- One recent example appeared in a monthly magazine disseminated among the computer underground in Russia and Eastern Europe. A July 2001 column began with the following rhetorical question:

Have you ever gotten the crazy idea to hack something serious? I don't mean Microsoft's site, but rather, let's say, an electric power system, a sewer system, an oil station or gas cut-off junction, so that people would understand the fragility of material possessions.

The column, entitled "Hackers and Electricity," asserts that in America, information systems are increasingly being used to control the power grid [sic]. As such information systems may be connected to the Internet, the author suggests that hackers operating from anywhere in the world could potentially find a way into them. While the column did not explicitly call upon its underground audience to attack American electric power systems, its irreverent tone did seem to suggest that it might be amusing to hack into a power system and become the "main electrical administrator" of some U.S. state.

- A West European hacking group that has shown a marked interest in the security of on-line financial sites has posted a number of materials at its web site about "financial information warfare." One of the group's statements of its "vision of things" notes that "the best way to earn money in a world under the control of the financial markets is to attack the image, the reputation, and the financial information that defines an enterprise."
- An additional factor to consider in the case of foreign attackers is an injudicious national pride that may drive the perpetrators to attack high-value sites in the U.S. For example, in the case of a Canadian juvenile charged with a number of attacks on large U.S. Internet sites, Crown prosecutors quoted the defendant as stating, "I showed the world that the best hackers come from Canada."

While the actual extent of dependency of the energy industry on information systems is debatable, there are potential vulnerabilities associated with any networked environment. The global computer underground is continuing to develop an understanding of the vulnerabilities present in the United States' networked systems, as well as their strategic significance. As high-value Internet hosts in the U.S. may present tempting targets for attackers motivated by a diverse range of factors, this heightened awareness among potential attackers must enter into the assessment of the constantly evolving threat profile faced by the operators of the country's critical infrastructures.