United States General Accounting Office

GAO

Testimony

Before the Subcommittee on Technology, Committee on Science, House of Representatives

For Release on Delivery
Expected at
10 a.m.
Thursday,
June 24, 1999

INFORMATION SECURITY

Recent Attacks on Federal Web Sites Underscore Need for Stronger Information Security Management

Statement of Keith A. Rhodes
Director, Office of Computer and Information Technology Assessment
Accounting and Information Management Division

GAO/T-AIMD-99-223

Madam Chairwoman and Members of the Subcommittee:

Two months ago, I testified before this Subcommittee on the "Melissa" computer virus, which temporarily disrupted the operations of some agencies by forcing them to shut down their e-mail systems. Since April, the federal government and the private sector have tangled with additional viruses, some more vexing than Melissa. For example, many agencies are now contending with "ExploreZip," an e-mail-delivered virus program that can destroy electronic files, degrade network performance, and eventually cause a denial of service on electronic mail servers.[1]

Today, I am here to discuss a different type of malicious attack—the recent series of break-ins of federal web sites. Like "Melissa" and "ExploreZip," these attacks demonstrate just how vulnerable federal information systems can be to computer attacks and, once again, underscore the need for better agency and governmentwide protection over systems.

Benefits and Risks Associated With Establishing Web Sites

Web sites clearly benefit federal agencies—they enable them to provide better customer service, improve internal communication, and reduce communications costs. Web sites also benefit citizens, allowing them to access needed information rapidly. For example, in just seconds federal web site users can

- obtain information on applying for passports, U.S. visas and foreign entry requirements, and travel warnings;
- electronically file a product incident report with the U.S. Consumer Product Safety Commission;
- download federal tax forms from the Internal Revenue Service and submit questions on tax preparation;
- access the Federal Jobs Data Base maintained by the Office of Personnel Management and submit applications for job openings;
- research the Patents Database maintained by the U.S. Patent and Trademark Office; and

[1]According to the CERT Coordination Center (originally called the Computer Emergency Response Team), ExploreZip is both a Trojan horse (i.e., it initially requires a victim to open or run an e-mail attachment in order for the program to install a copy of itself) and a "worm" (i.e., once installed, it may propagate itself, without any human interaction, to other networked machines that have certain writable shares). The center began receiving reports of sites affected by ExploreZip during the second week of June 1999.

- get the latest forecasts and weather warnings from the National Oceanic and Atmospheric Administration.

For the private sector, web sites are becoming an increasingly popular avenue of doing business. A recent study jointly sponsored by the University of Texas Center for Research in Electronic Commerce and Cisco Systems, Inc., for example, found that the Internet economy generated more than $300 billion in U.S. revenue and was responsible for 1.2 million jobs in 1998. A business that establishes its presence on the web, in fact, is no longer just a "storefront"; rather it is a "worldfront" with a presence across all time zones and geographic barriers. It is also a 24-hour-a-day/7-day-a-week operation.

While there are significant advantages associated with establishing web sites, caution must be exercised to avoid or mitigate damages resulting from the types of attacks recently experienced by a number of federal agencies, as well as more pervasive system intrusions. By exploiting bugs and configuration problems found in web server software programs, operating systems, and the communications protocol, for example, unauthorized users can do any one or a combination of the following:

- Change web site content to embarrass the web site owner.
- Flood the web site with fake requests for pages. Known as denial-of-service, this type of attack can (1) make it difficult or even impossible for legitimate customers to access a web site or (2) cause the targeted system to crash.
- Gain unauthorized access to resources elsewhere in an organization's computer network.
- Insert a "fake" web site between the user and the "real" web site so that the attacker can watch and record data such as account numbers and passwords as well as insert, delete, or change data sent in either direction.

According to the World Wide Web Consortium,[2] web servers themselves vary in their ability to restrict access to individual documents in the server. Some servers provide no restriction at all, while others allow a web site administrator to restrict access to directories based on the address of the browser or to users who can provide the correct password. A few servers

[2]The World Wide Web Consortium serves as a repository of information about the World Wide Web and develops common protocols to ensure Internet interoperability.

provide data encryption as well. As a rule of thumb, according to the consortium, the more features a server offers, the more likely it is to contain security holes.

Similarly, according to the consortium, some operating systems are less secure to use as platforms for web servers than others. Specifically, operating systems with a large number of built-in services, scripting languages, and interpreters are particularly vulnerable to attack because there are simply so many portals of entry for hackers to exploit. Furthermore, if not used carefully, the protocol used to write web site program tasks (known as CGI or Common Gateway Interface protocol) can be a major source of security holes.

Recent Attacks Primarily Involved Vandalism and Denial of Service

The recent series of attacks on federal web sites have primarily focused on defacing, or "vandalizing" web site content and/or initiating denial of service attacks in order to crash servers. For example, in late May, a denial of service attack was launched against the Federal Bureau of Investigation's (FBI) web site allegedly in retaliation for the bureau's pursuit of hackers who have broken into federal systems. In response, the Bureau temporarily took its web servers off line. Shortly thereafter, the same group of attackers reportedly broke in and defaced the U.S. Senate's home page with comments criticizing the FBI. The Senate also temporarily took its site off line. Similar attacks were also committed on web sites maintained by the Department of the Interior and a federal supercomputer laboratory in Idaho Falls, Idaho. Also last month, several cyberattacks successfully took down sites at the Department of Defense, the White House, and other agencies.

Web site attacks have not been confined to federal agencies. Recently, computers maintained by an Internet service company were reportedly jammed by denial-of-service attacks similar to the FBI's experience. According to the IBM Global Services' Internet Emergency Response Service, other private sector web sites that have experienced attacks include those belonging to the New York Times, BMW, and Motorola.

Fortunately, the consequences of recent attacks on federal web sites have been largely confined to agency embarrassment and temporary shut downs in web site service. In fact, web site attacks can have much more serious consequences. For example, according to Carnegie Mellon University's

Software Engineering Institute (SEI),[3] the hardware and operating systems that support web sites could be used as a staging area for intrusions into an organization's network. In turn, this could result in breaches of confidentiality, integrity, or availability of information resources. Such systems could also be used as a staging area for intrusions into external sites.

For private sector organizations, web site security problems could impede the ability to do business on the Internet. While the Internet may represent hundreds of millions of potential customers, it also represents extensive security risks. For customers, the primary security concern with shopping on the Internet is credit card fraud. According to Internet Fraud Watch, operated by the National Consumers League, complaints in this area have increased 600 percent since 1997. Thus, in conducting business on the web, businesses must not only ask how secure the business needs to be, but also how much security it needs to provide to customers.

Underlying Causes of Web Site Security Problems

Just like computer viruses such as "Melissa," and "ExploreZip," the recent attacks on federal web sites are a symptom of broader information security concerns across the government. Over the past several years, we and inspectors general have identified significant information security weaknesses in each of the largest 24 federal agencies. These weaknesses include the inability to detect, protect against, and recover from viruses, web site break-ins, and other attacks; inadequately segregated duties, which increase the risk that disgruntled employees as well as intruders can take unauthorized actions without detection; and weak configuration management processes, which cannot prevent unauthorized software from being implemented.

Recently, for example, we reported[4] that the National Aeronautics and Space Administration (NASA) did not effectively evaluate its information security risks or needs, implement sound security policies and controls, monitor policy compliance, or provide adequate computer security training. Tests we conducted at one of NASA's 10 field centers showed that some of the agency's mission-critical systems at that center were

[3]SEI is a federally funded research and development center sponsored by the U.S. Department of Defense and operated by Carnegie Mellon University.

[4]Information Security: Many NASA Mission-Critical Systems Face Serious Risks (GAO/AIMD-99-47, May 20, 1999).

vulnerable to unauthorized access. These included systems that support the command and control of spacecraft as well as the processing and distributing of scientific data.

Overall, our work at NASA and many other agencies shows that federal information security is seriously hindered by three narrow approaches taken by agencies.

- *System versus organization focus*. Agencies tend to look at security from a system perspective, but not an organizationwide perspective. This focus, however, is unworkable in a networked environment.
- *Static categories versus managing risks*. Agencies often reduce information security to protecting static categories of information, e.g., sensitive versus nonsensitive or classified versus unclassified. This approach fails to encompass the multifaceted nature of managing security across varying levels of risks to the integrity, availability, and confidentiality of information supporting agency operations and assets.
- *Technical versus management function*. Agencies frequently treat information security as a technical function rather than as a management function. This removes security from its integral role in program management.

In view of these and other pervasive security weaknesses, in February 1997, we designated information security as a new governmentwide high-risk area.[5] In performing audits at selected individual agencies, we and the inspectors general have also developed hundreds of specific recommendations aimed at improving the effectiveness of information security programs, including the development of entitywide information security management programs.

Since our 1997 High-Risk Report, the recognition of the importance of addressing information security problems has greatly increased and led to significant actions. In late 1997, for example, in response to our recommendations, the Chief Information Officers (CIO) Council designated information security a priority area and established a Security Committee. Also, in May 1998, Presidential Decision Directive 63 was issued, establishing entities within the National Security Council, the Department of Commerce, and the FBI to address critical infrastructure

[5] High-Risk Series: An Overview (GAO/HR-97-1, February 1997) and High-Risk Series: Information Management and Technology (GAO/HR-97-9, February 1997).

issues. This directive also required each major department and agency to develop a plan for protecting its own critical infrastructure.

Short- and Long-Term Solutions That Can Address Web Site and Other Security Problems

Agencies can undertake a number of immediate actions to quickly bolster security over their web sites. For example, SEI suggests that organizations pay close attention to systems and networks, investigate unusual activity, and react quickly to intrusions. Organizations can also begin to include explicit security requirements when selecting server and host technologies, isolate the web server from the organization's internal network, and offer only essential network services and operating system services on the server host machine.

However, while these and other actions recommended by security experts sound simple enough, implementing them is a resource-intensive activity that requires "continuous, automated support, and daily administrative effort," according to SEI. Further, the scale of security practices may have to change as threats, system configurations, or security requirements change.

To help agencies implement the kind of management framework that is required to effectively respond to evolving security requirements, we issued an executive guide in May 1998 entitled Information Security Management: Learning From Leading Organizations (GAO/AIMD-98-68). It describes a framework for managing risks through an ongoing cycle of activity coordinated by a central focal point. The guide, which is based on the best practices of organizations noted for superior information security programs, has been endorsed by the CIO Council, and distributed to all major agency heads, CIOs, and inspectors general. By adopting the following 16 practices recommended by the guide, agencies can be better prepared to *protect* their systems, *detect* attacks, and *react* to security breaches.

Table 1: Sixteen Information Security Practices of Leading Organizations

Principles	Practices
Assess risk and determine needs	1. Recognize information resources as essential organizational assets 2. Develop practical risk assessment procedures that link security to business needs 3. Hold program and business managers accountable 4. Manage risk on a continuing basis
Establish a central management focal point	5. Designate a central group to carry out key activities 6. Provide the central group ready and independent access to senior executives 7. Designate dedicated funding and staff 8. Enhance staff professionalism and technical skills
Implement appropriate policies and related controls	9. Link policies to business risks 10. Distinguish between policies and guidelines 11. Support policies through a central security group
Promote awareness	12. Continually educate users and others on risks and related policies 13. Use attention-getting and user-friendly techniques
Monitor and evaluate policy control and effectiveness	14. Monitor factors that affect risk and indicate security effectiveness 15. Use results to direct future efforts and hold managers accountable 16. Be alert to new monitoring tools and techniques

Over the long run, it is also clear that more needs to be done to build and implement a comprehensive governmentwide strategy. At present, for example, there is no mechanism, such as required independent audits, for routinely testing and evaluating the effectiveness of agency information security programs. Also, there is no single governmentwide office that gathers and shares information about information security threats or acts as an emergency assistance center. Nor is any support agency responsible for providing technical assistance to agencies, undertaking research, engaging in proactive coordination, and generating more forward-thinking policy advice. Until such measures are implemented, it is likely that agencies will continue to address their web site and other information security problems in a narrow context and neglect to implement the management framework needed to thwart such attacks.

Conclusions

In conclusion, web sites offer enormous efficiency and productivity benefits to agencies and citizens alike. Moreover, they are now an integral part of the Internet economy, which is certain to continue to grow exponentially. Nevertheless, web sites open up yet another avenue of security risks that can range from the merely embarrassing to the theft of sensitive information. Thus, to maximize the advantages offered by web sites and the Internet, it is imperative that federal agencies implement vigorous security programs that will enable them to closely watch

information resources for signs of intrusion and to quickly react to intrusions when detected. Moreover, it will be important for the federal government as a whole to implement an effective strategy that will (1) ensure that agencies focus on security from an organizationwide perspective and implement a comprehensive set of security controls and (2) establish central tracking and reporting mechanisms that facilitate analyses of web site attacks and other forms of attacks and their impact.

Madam Chairwoman, this concludes my testimony. I will be happy to answer any questions you or Members of the Subcommittee may have.

Contact and Acknowledgements

For information about this testimony, please contact Keith Rhodes at (202) 512-6415. Cristina Chaplain made key contributions to this testimony.

Ordering Information

The first copy of each GAO report and testimony is free. Additional copies are $2 each. Orders should be sent to the following address, accompanied by a check or money order made out to the Superintendent of Documents, when necessary, VISA and MasterCard credit cards are accepted, also.

Orders for 100 or more copies to be mailed to a single address are discounted 25 percent.

Orders by mail:

U.S. General Accounting Office
P.O. Box 37050
Washington, DC 20013

or visit:

Room 1100
700 4th St. NW (corner of 4th and G Sts. NW)
U.S. General Accounting Office
Washington, DC

Orders may also be placed by calling (202) 512-6000 or by using fax number (202) 512-6061, or TDD (202) 512-2537.

Each day, GAO issues a list of newly available reports and testimony. To receive facsimile copies of the daily list or any list from the past 30 days, please call (202) 512-6000 using a touchtone phone. A recorded menu will provide information on how to obtain these lists.

For information on how to access GAO reports on the INTERNET, send an e-mail message with "info" in the body to:

info@www.gao.gov

or visit GAO's World Wide Web Home Page at:

http://www.gao.gov

PRINTED ON RECYCLED PAPER

United States
General Accounting Office
Washington, D.C. 20548-0001

Official Business
Penalty for Private Use $300

Address Correction Requested

Bulk Mail
Postage & Fees Paid
GAO
Permit No. GI00