Global Information Assurance Certification Paper

The Desktop Modem Threat

Joe Livingston
July 27, 2000

Introduction

Unauthorized or uncontrolled desktop modems are a bigger threat to a businesses security today mainly due to the change in computers networks. In the 1970's most enterprise critical software applications were ran on mainframes, security was fairly easy to enforce. The 1980's saw the increase in enterprise local area networks that ultimately increased the amount of data available to even more users. The main threat at this time was from abuse from within the network. Modems were used but weren't considered a big threat because computer access and control was centralized in a computer room. Dialup access was limited to simple-character based logins. If you couldn't provide a valid ID and password your access was denied. Security remained simple to enforce. The 1990's brought an increase in the number of wide area networks and the expectation that every business should have a presence on the World Wide Web. Customers and vendors expect to place business transactions on-line. This change caused tremendous security risks and vulnerabilities to surface. In the early 1990's, businesses connected to the Internet with virtually no firewalls and minimal protection. Several network compromises and business losses resulted in an explosion of the firewall industry virtually overnight. Today it is estimated that over 80% of businesses protect their wide area networks using firewall and intrusion detection systems. Security has become a huge challenge with the objective being to minimize and quickly recover rather than prevent damage caused due to intrusion.

The Problem

As the Internet grows and as businesses, large and small, migrate to high-speed dedicated Internet access, the emphasis on dialup access security becomes more obscure or is nonexistent. Part of this problem stems from specialization and segmentation of responsibilities and poor coordination between network professionals and telecommunications professionals. Another important contributor is the lack of tools in use or the reluctance to use these tools to accurately assess and monitor telecommunications systems for unauthorized or suspicious activity. In addition, most businesses fail to recognize, or choose to ignore, the potential vulnerability from unauthorized dialup access.

Businesses have made a large investment in deploying firewalls and intrusion detection systems in an attempt to protect their network perimeter from hostile activities. This protection is designed to minimize the intrusion threat from external sources using the front door. As we take steps to make it more difficult for intruders to access or penetrate our networks from the outside, the serious intruder keeps looking for the easy way to stage an attack. The easy way often involves finding a backdoor, a networked desktop computer with dialup capabilities. Security planners should also be aware that phone lines and desktop modems are no secret to insider employees. It is estimated that more than 70 percent of all computer crimes are committed by inside employees. Businesses that allow network users to attach personal modems to computers always lose control of their access security.[1] A 1999 CSI/FBI Computer Crime and Security Survey revealed that 62% of 521 respondents reported security breaches within the last year and

28% of the respondents reported dial-in modem breaches.[2] Unlike data networks, businesses have only limited visibility and control over telephone networks. This lack of visibility and control makes it possible for any user to connect the entire data network to the public telephone network using unauthorized or uncontrolled dialup modem access.

Possible Solutions (Best Practices)

- **Policy** - Minimize the desktop modem threat by developing a strong and enforceable policy. Keep this policy short and simple and include justification relevant to your business so that users can understand the rationale behind the policy. Avoid a policy that relies on user decisions and participation. Also develop a strong policy for authorized dialup users to follow.[3]

- **Scanning Tools** - Employ hardware and inventory scanning tools to verify the presence and configuration of dial utilities and modems. Consider implementing a firewall solution for your telephone networks. There are products available (e.g. Telewall™ from Securelogix and Phonewall Enforcer™ from Sentry Telecom Systems) that will enhance telephone security by providing real-time logging and alerts to administrators. In addition, these devices can be configured to control use by limiting or blocking unauthorized traffic on an enterprise or an individual basis. Periodically perform "war dialing" to ensure that users have not installed their own modems. Always remember to obtain the proper authorization prior to starting any war dialing activity.

- **Coordination** – Telecommunications and network professionals need to work together. They have a common business Objective - Availability, Confidentiality, and Integrity - through Information Assurance! This is not an issue of ownership of network resources. Network professionals should know when, where and why analog telephones lines are ordered and installed. Both groups need to be aware of all installed or pending analog service to include all facsimile service. Users should not be allowed to purchase either modems or telephone lines without first coordinating with both the telecommunications and networking groups. Ensure your policy clearly states these guidelines.

- **Offer Incentives** - It is improbable, if not impossible, for the telecommunications or network professionals to visit all user locations on a regular basis. Consider offering an incentive or special recognition to users/employees who make the effort to report problems when discovered. Early discovery could minimize potential losses or damage. Include this topic in your security awareness program.

Summary

The evolution of the networking environment and the increased presence on the World Wide Web has completely changed the approach to protecting business assets. A strong, clear and enforceable policy is the first and possibly most important step to be taken to minimize the threat of users installing and using unauthorized desktop modems. The insider threat is there and security precautions should be implemented to minimize this threat. The telecommunications arena can no longer be separated into telephone and data. You need continuous cooperation and

coordination between these professionals if you expect to achieve any level of success with alleviating the open back door, the unauthorized desktop modem. Solicit assistance from users and employees through clear policy and incentive. Emphasize the risk posed by unauthorized modems using your security awareness program. It may be time to invest in some tools to protect telephone networks and close those back doors before an actual intrusion occurs.

References:

1. Girard, J. "Modems on the Desktop? Nine Ways to Harm the Company." September 1999. URL: http://www.gartnerweb.com/public/ax1/reprints/securelogix/00083230.html (July 27, 2000).
2. Knowledge Base: Sentry Telecom Systems, Inc. "Threats of Modems to Computer Security." URL: http://www.sentrytelecom.com/knowledgebase/modem-security.asp?b=2 (July 27, 2000).
3. Girard, J. "CIO Alert: Modems on the Desktop Can Put Important Enterprise Elements at Risk." December 1999. URL: http://www.gartnerweb.com/public/ax1/reprints/securelogix/00085146.html (July 27, 2000).