Midrange Security News

Kisco
Information
Systems

Feature *Affordable IBM Midrange Software that makes you more productive*

Basic Security Improvements Worth Considering

A hard number illustrating the percentage of unsecured AS/400 and iSeries computers is difficult to come by. Wisely, many companies are reluctant to draw attention to their shortcomings, while others are simply unaware that trespassers have jumped the fence.

The confluence of scuttlebutt circulating in technical forums and the emergence of new security consulting organizations paint a disquieting picture. Trevor Seeney, Technical Director of Sentinex, an iSeries-AS/400 security-consulting firm based in New York states with a grimace, “There are around seven hundred thousand AS/400 and iSeries computers in the world and half of them can be broken into. Once a very secure proprietary machine, the four hundred has become more vulnerable because of its new openness. In terms of security, great care must be taken not to let it go the way of other platforms.”

The Bubble

Unwisely, some believe that they are operating safely within the construct of a detached bubble: “*With object level security in place, green screens and network connected PCs used only by employees, and no internet connection or external users, there is little at risk*.” To them, obscurity is security. Welcome in oh’ harbinger of chaos.

> ***“There are around seven hundred thousand AS/400 and iSeries computers in the world and half of them can be broken into. Once a very secure proprietary machine, the four hundred has become more vulnerable because of its new openness.”***
>
> *Trevor Seeney, Technical Director, Sentinex*

The Pin

Mischievous and vengeful internal users can smell vulnerabilities that lie beyond “secured menu access” a mile away. Tinkering, like Colombian coffee, is addictive. Once a renegade seeking truth realizes that he can access payroll records using a simple pc-based spreadsheet or database program, he may share this information with his inner circle of friends, who in turn tell their friends, and on and on until everyone knows.

Noteworthy is the fact that all breaches are not the product of folly or spite. A system user on a network connection can find himself in an application from which he is restricted, with a simple slip of the mouse, or can sit down at another’s desktop while it’s logged on with legitimate purpose and access anything the original user was authorized to.

Embarking on a full scale security initiative may not be in the cards and removing the network connection from the back of the computer is not the way to solve the problem so what do you do? First, don’t get hamstrung. There are ways to improve the situation and not be consumed in the process.

Security analysts and other intransient intelligencia will tell you that to protect your material assets, intellectual assets and reputation, all of the major tenets of computer security must be duly heeded. No one will dispute this. The hard part is maintaining easy accessibility for employees who need to do their work while keeping out the bad guys. This is where things often come undone. Have you ever approached a very secure looking computer room door only to find it propped open with an old Intel 486 machine?

Good computer security is a proactive process. You should continuously, even if informally, update your understanding of what computer resources are essential for the company to do its job, who poses a threat to these resources, how they might gain access, what they would like to see or do, how it would harm the company and what it would take to recover. Beware: The analysis process can grow and take on a life of its own. It can become a vast un-navigable morass of contradicting objectives: Software developers at your company may insist that they need all object authority to programs in production environments! Remember systems and procedures need to updated and the sooner the better.

NSafe/400 Lite makes the initial step toward a secured network environment easier.

Network Security, A Place to Start

Although OS/400 native object level security does a commendable job of keeping intruders out by limiting their access at the object level with passwords and ID's, it doesn't help when trying to control the activities of network connected intelligent desktop users. These users can view, copy, change or delete critical data. OS/400 menu security and user profile settings can be bypassed when users access the iSeries-AS/400 from a device attached via Ethernet, Token Ring, and other network topologies.

Third party software solutions are available that block exit points and elevate the level of control over accessibility. One new offering in this area is called NSafe/400 Lite. It is designed to make the initial step into a secured network environment an easy one, without making the system more difficult to use. This product intercepts incoming requests from clients accessing OS/400 server functions; it evaluates these requests using a set of predefined rules and security level settings and accepts or rejects them.

NSafe/400 Lite enables administrators to limit user access to designated server functions based on user profile, or disable specific server functions. It includes security logging and analysis features enabling administrators to monitor activity as it occurs, or later generate audit reports detailing which users accessed the system, which server functions they requested, what files or objects they accessed, and whether the request was accepted or rejected. NSafe/400 Lite is offered by Kisco Information Systems, (www.kisco.com). Kisco will credit 100% of the NSafe/400 Lite license fee to a SafeNet/400 upgrade. In addition to all the features in NSafe/400 Lite, SafeNet/400 offers on-line transaction testing and prototyping capabilities, object level control and APIs that allow technicians to call security routines from other programs, and other features.

Workstation Security

Another security issue not addressed by OS/400 pertains to workstations. Clearly OS/400 has the login process well covered, limiting the number of attempts with any given User ID and password. A logged-on, unmanned desktop however, is invariably a snoop's carte blanche to human resources/payroll, accounts payable, executive email and other files. Instituting a policy whereby users are instructed to log off if they walk away for more than ten minutes is a good idea, but as fallible as short-term human memory. An easy way to systemically protect your environment against this opportunistic form of intrusive behavior is with a security screen saver. These solutions automatically scramble a display and inhibit keyboard input without forcing a log off which can negatively impact the legitimate users productivity. There are only a few software developers who offer these products and most of them run only on PC based workstations. Again, Kisco brings to the table an innovative offering called ScreenSafer/400, which works on green screen devices, as well as PC's. The product will automatically enroll valid users and default to a safe screen configuration. It provides value upon installation and is very affordable.

In the absence of vigilance, only luck is shielding your data from the eyes of intruders. If you don't already have tools in place to augment native system security, many tools are available to help you get started and they are inexpensive and easy to implement.

Kisco Information Systems

7 Church St.
Saranac Lake, NY 12983
(518) 897-5002
Fax: (518) 897-5003
sales@kisco.com

http://www.kisco.com