Communicating With Sam

Autonomic Network Security

Sam Johnston

Question:

Recent legislative changes in Canada and the U.S. along with new viruses and worms have created a real awareness within our senior management team of the need to properly protect our information and ensure compliance. We have taken measures to protect the high-risk points. Our Internet connection is protected by a firewall; we have anti-virus software and intrusion detection software to monitor our AS/400 for host security breaches. We also regularly force our users to change their various network and system access passwords, and we randomly do security checks. Despite these actions, senior management is concerned that we may not be taking all the security measures necessary to protect our valuable data. What more can be done to reduce security risks?

Answer:

The key to unlocking the answer, and demystifying the solution, is rooted in the fact that there is a need to protect all valuable data and all network resources. If you start by accepting that security is a network-wide need and demands a system embedded in the utility of the network, like the immune system in our bodies, then you will be successfully prepared to fight the battle.

The strategic implication of today's connected world is simple. If security is not focused on the entire network, and if it is not a system that is planned and considered on the same playing field with other mission critical applications, then you as an organization are exposed and unprepared to effectively do business in an Internet enabled world. True, the data on your host systems are the crown jewels, but think about how many portals and devices either provide access to this data, or contain fragments of this data, and it becomes clear that host protection is merely the last line of defense in security.

Even though many enterprise companies, and government organizations have invested heavily in various appliances and software technologies and are following the best practices, viruses and worms continue to disrupt business, causing downtime, lost productivity, and continuous installation of patches. The self-propagating nature of the latest attacks makes them damaging and pervasive. Existing anti-virus solutions, which rely on recognizing attack signatures, are unable to detect and contain "day-zero" viruses and the denial-of-service (DoS) attacks they create.

Servers and desktops that are not compliant with corporate security policy are common, and they are difficult to detect, contain, and cleanse. Locating and isolating these systems is time and resource intensive, resulting in infections that appear to be removed from the corporate network, but that reappear at a later time. The problem is compounded by the complexity of today's networked environment, which contains:

- Multiple types of end users – employees, vendors, and contractors
- Multiple types of endpoints – company desktop, home, and server
- Multiple types of access – wired, wireless, virtual private network (VPN), and dial

So now we know that we will be threatened and we are exposed, how do we architect a security infrastructure to protect our valuable assets that is Self-Defending?

To address this issue Cisco Systems has announced Cisco's Self-Defending Network, a new security vision that takes a fundamentally new approach to network security. Until now, network security and computer security were dealt with separately. Cisco's Self-Defending Network breaks from the traditional approach of creating separate security products for networks and the computers attached to them. Instead, it treats the network and end-point devices as part of the same system.

The Self-Defending Network's goal is to create greater security coordination between the network and its associated computers, servers and other devices. Much in the same way the human body identifies, prevents and responds to threats, the Self-Defending Network fights against the infiltration and spread of computer viruses, worms and other malicious programs across Cisco networks.

A key component of the Self-Defending initiative is the Cisco Network Admission Control (NAC) program. NAC will use Cisco routers to enforce admission privileges to end-point devices including, ▶

personal computers, servers, or PDAs – based on the security status of those devices and their compliance with a network's security policies. NAC is designed to dramatically increase the capabilities of data networks to protect themselves against viruses, worms, and other security threats.

This is not a Cisco only proprietary solution. Other members of the "Initiative" are leading anti-virus software companies, including Network Associates, Symantec and Trend Micro. Such industry collaboration is key to the success of the NAC program, since the network will need to know what, if any, protection end-point computers have before allowing them network access. This lets businesses leverage their existing investment in Cisco network infrastructure and anti-virus software to protect themselves.

The NAC program includes the Cisco Trust Agent, a small piece of client-based software that resides on computers and other end-points and communicates end-point security information to the Cisco network via the Cisco Secure Access Control Server. The Access Control Server will execute admission controls to permit, deny, quarantine or restrict end-point network access.

The Cisco Trust Agent will collect security state information from multiple security software clients, such as anti-virus clients or the Cisco Security Agent, Cisco's laptop/desktop and server host intrusion prevention and distributed firewall software that identifies and prevents malicious behavior before it can occur. The Cisco Security Agent is capable of stopping Nimbda, CodeRed, Slammer and Blaster worms with out-of-the-box policies. The NAC program will initially support end-point devices running Microsoft Windows NT, XP and 2000 operating systems.[1]

Other devices that enforce network admission control policy include routers, switches, wireless access points, and security appliances. These devices demand host security credentials and relay this information to policy servers, where network admission control decisions are made. Based on your defined policy, the network will enforce the appropriate admission decision that can include: permit, deny, quarantine, or restrict.

The Cisco Secure Access Control Server (ACS) evaluates the endpoint security information relayed from network access devices and determines the appropriate access policy for them to apply. Cisco ACS is an authentication, authorization, and accounting (AAA) RADIUS server. It is the foundation of the policy server system. ACS works in conjunction with Cisco's "Initiative" partner's application servers, (such as anti-virus policy servers) to provide deeper credential validation capabilities.

Management of the security process is provided by CiscoWorks VPN/Security Management (VMS). This provisions Cisco NAC elements, while CiscoWorks Security Information Manager Solution (SIMS) provides monitoring and reporting tools. Cisco "Initiative" partners provide management solutions for their endpoint security software.

The initial release of Cisco NAC will be available in the first half of 2004. The development of the Cisco Self-Defending Network is a multiphased security initiative that will be enhanced in future releases to improve the ability of networks to identify, prevent, and adapt to security threats. The Cisco Self-Defending Network Initiative significantly advances Cisco's strategy of integrating security services throughout IP networks. By delivering new system-level network threat defense capability in this manner we approach a security model that is truly autonomic. TUG

***Sam Johnston** is a partner and Chief Technology Officer of Intesys Network Communications Ltd., providing value-added networking and e-commerce solutions to the iSeries community. He can be reached at (416) 438-0002 or via e-mail at sjohnston@intesys-ncl.com. Any TUG member wishing to submit a question to Sam can forward their typewritten material to the TUG office, or to Intesys. The deadline for our next issue is Friday April 8, 2004.*

[1] Source: Cisco Self-Defending Networks