COMMUNICATING WITH SAM

Network Security: Where Are the Real Threats? Part I

Sam Johnston

Question:

Over the past year, it seems that high profile "hackers" have been in the news on a regular basis. These security breaches, many of which have impacted some of the world's largest companies, have created a real awareness within our senior management of the need to properly protect our information. We have taken measures to protect the high-risk points. Our Internet connection is protected by a firewall, and we have 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 physical security checks to ensure that users do not remain logged onto the network or systems while away from their desk. Despite these actions, senior management is concerned that we may not be taking all the security measures necessary to protect our valuable data. Based on your experiences, what points in the network represent risk, and what can be done to reduce security risks?

Answer:

Security is perhaps the most discussed, and to a certain extent the most misunderstood, information technology discipline that we currently deal with. It is not uncommon for information technology trends to reflect the views commonly expressed in the mainstream business press. However, as an IT professional you need to be aware that by the time a topic is a regular item in the popular press, you better have a sound strategy for dealing with issue, because playing catch-up when you are under the senior management microscope can be a painful experience.

Your question, due to the sensitivity of the issue, is extremely complex, but believe it or not, the answer you need is based upon a simple principle. The key to unlocking the answer, and demystifying the solution, is rooted in the fact that in this connected world of interlocking dependencies there is a need to protect all valuable data and network resources. More simply put, if you can abandon the temptation of protecting individual devices or hosts, and start accepting that security is a network-wide need that demands a system embedded in the utility of the network, then you will be successfully prepared to fight the battle.

The key to creating a successful security strategy requires you to embrace a few simple lessons on the criminal mind as it pertains to physical security that we often ignore or forget, but can be applied to IT security.

Security is only as strong as the weakest link: Our experiences as IT professionals says that we need to protect our mission critical host systems with vigilance – let them get to the doorstep of the vault, but not through the door. Prior to the truly connected world, this was perhaps an adequate strategy. As we permit semi-trusted traffic to enter our back office, risk increases when intruders continually reach our information vaults.

Security is more than just firewalls at the front door to our enterprise: We tend to focus on firewall protection from the Internet as the pinnacle of network security. Although it is always prudent to protect the obvious breach points, remember that it is the discreet points of entry that attract the criminal mind.

Security from those we know and trust is always more difficult to achieve: We tend to spend all our effort focusing on the unknown outside intruder, letting our guard down when it comes to internal security efforts. Your own employees, who have trusted access and insider knowledge, are the risk you should fear most given that internally security enforcement is often quite low.

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 defence in security. The host systems are just another device within a complex network, hence, the need for organization to evolve to a network security model.

The obvious implication of migrating from the traditional system-based security approach to a network utility model is the overall technology architecture that is needed to support the strategy. The network model requires moving intelligence usually found in only servers and hosts to appliances that reside at various points and layers within the network. To fully understand the value of a security approach embedded in the network, you need to understand targets you need to protect.

Routers are at the forefront of your network, as they provide the access from every network to every network, and they advertise networks, using filters to control access. Given the role of a router is to provide access, like a front door, it becomes an obvious hack point. Risk can be significantly reduced through simple practices such as locking down telnet access to the router, turning of unneeded services, or by requiring strong authentication for access to the device.

LAN switches have many of the same security risks associated with routers as they act as access points, however, this risk is somewhat mitigated by the fact that routers connect to the outside world, while LAN switches form the core of your intranet. However, if we accept that internal security risks far exceed external threats, than this may be a false sense of security. The security practices that apply to routers also apply switches. However, there are other precautions that are necessary for LAN switches, such as disabling unused ports so hackers cannot easily attach to the LAN. Ports without any need to trunk should have trunk settings turned off as opposed being set to auto which prevents a host inadvertently becoming a trunk port and receiving all traffic that would normally reside on a port.

Networks themselves, in addition to the specific devices, are vulnerable, with distributed denial of services (DDoS) being the vulnerability that we hear about most. A DDoS is created when numerous machines simultaneously send spurious data to an IP address, which then cripples the entire network. Typical DDoS attacks are ICMP floods, TCP SYN floods or UDP floods. The challenge is that this traffic can appear to be legitimate, and it is challenging to block this traffic without impacting legitimate traffic. However, using techniques such as CAR (Committed Access Rate) to limit outbound traffic from the ISP will assist here.

Hosts, as you have noted, are perhaps the highest risk point because of the visibility to the user, and the fact that hosts often provide applications to other hosts that request services. Further many of the operating systems that run our mission critical hosts are very familiar to a large number of trained individuals who understand the weaknesses of these systems. It is crucial for you to properly maintain these hosts with current software releases, version, patches and fixes, as often these updates are directly related to security needs.

Applications, due to the human element both in creating and using them, present the greatest security threat. The challenge in managing application security is weeding out benign threats related to the application executing a task incorrectly, and malignant threats related to general architectural flaws that permit a security breach. As you have noted, host-based intrusion detection systems (HIDS) can assist here, and we will discuss this later as part of an overall security architecture.

Cisco Systems has published a list of the top fourteen security vulnerabilities, and they are worth review as they emphasize the importance of focusing on a network security model. They are:

1. Inadequate router access control: misconfigured router ACLs can allow information leakage through ICMP, IP, NetBIOS and lead to unauthorized access to services on your DMZ servers.
2. Unsecured or unmonitored remote access points are one of the easiest means of access to your corporate network.

3. Information leakage can provide the attacker with O/S and application versions, user groups, shares, DNS information zone via zone transfers, and running services like SNMP, finger, SNMP telnet rusers, sunrp, NetBIOS.
4. Hosts running unnecessary services (such as sunpc, FTP, DNS, SMTP) leave ways in.
5. Weak, easily guessed and reused passwords at the workstation level can doom your servers to compromise.
6. User or test accounts with excessive privileges.
7. Misconfigured Internet servers, especially CGI scripts on Web servers and anonymous FTP.
8. Misconfigured firewalls or router ACL can allow access to internal systems directly or once a DMZ server is compromised.
9. Software that is unpatched, outdated, vulnerable, or left in the default configurations.
10. Excessive file and directory access controls (NT shares, UNIX NFS exports).
11. Excessive trust relationships such as NT Domain Trusts and UNIX .rhosts and hosts .equiv files can provide hackers with unauthorized access to sensitive systems.
12. Unauthenticated services like X Windows.
13. Inadequate logging, monitoring, and detection capabilities at the network and host level.
14. Lack of accepted and well promulgated security policies, procedures, guidelines and minimum baseline standards.

Source: Cisco Systems, "Make Your Network Safe for E-Business"

The interesting link among the top fourteen security vulnerabilities is the fact that most can be resolved through simple adherence to good IT practices. Despite the fact that the popular press paints a picture of a network of sophisticated hackers that are capable of cracking the Pentagon using black magic techniques to attack your data, the reality is that digital security is no different than physical security. More often than not, the criminal is able to make the victim vulnerable because the victim makes it easy for them! So now we know where and how we will be threatened, how do we architect a security infrastructure to protect our valuable assets? **In Part II, in the next issue of this magazine,** we will examine how the appropriate security architecture is driven by security policies that reflect the unique nature of your business... T🖫G

Sam Johnston is a partner and Chief Technology Officer of Intesys Network Communications Ltd., providing value-added networking and e-commerce solutions to theAS/400 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 March 30th, 2001.