Realtime publishers

"Leading the Conversation"

The Essentials Series: Understanding & Responding to Network Threats

Keeping Pace with Security Threats Understanding

sponsored by

NOKIA

by Dan Sullivan

Copyright Statement

Keeping Pace with Security Threats

One of the defining characteristics of information technology (IT) is that it is in a constant state of change. This change does not just occur with vendors developing new products and improving existing technologies, it happens inside businesses and organizations every day. Servers are reconfigured, applications are modified, and networks architectures are revised. There are external changes as well, such as evolving malware, which is becoming more difficult to detect, new forms of attack that leverage browser vulnerabilities as well as operating system (OS) weaknesses, and the rapid adoption of personal mobile devices for use with enterprise systems. How can IT professionals keep pace with these kinds of dynamics? In this, the first of three articles in the Essentials Series: Understanding and Responding to Network Threats, we will examine security threats faced by businesses today; the next two articles in this series will address evaluating and managing security technologies that can address these threats.

There are no simple answers, but a small number of principles can provide the foundation for a sound strategy for keeping pace with security threats.

- First, recognize that change is constant and understand what kinds of change are most important with respect to security.
- Second, what you do not know about your network and other IT infrastructure can hurt you. You need to understand the security impact of changes or risk disrupting business operations.
- Third, every security investment, by definition, should contribute to protecting the integrity, confidentiality, and availability of systems and data, but it should also support security management within a dynamic environment.

This, the first of three articles on understanding and responding to network threats, describes how changes in infrastructure and security threats can compromise security and how the first step to responding is understanding the state of network operations.

Managing Change and Maintaining Security

Maintaining a secure environment under constant change can be viewed as a set of three distinct challenges:

- Understanding change in infrastructure
- Understanding change in security threats
- Balancing risks, demands, and resources

Unlike well-planned projects with sequential tasks and well-defined milestones, you face these challenges simultaneously and without clear expectations that the job of securing an environment will ever be done.

Understanding Change in Infrastructure

IT infrastructure consists of servers, workstations, network devices, mobile devices, and software ranging from OSs and network systems to application servers to databases. Changes in this environment can come in several different forms, all of which can have an impact on security:

- Hardware may be added or removed from the network. Systems administrators and network managers need to understand how the introduction of a new server, router, or network appliance will impact security. Some changes, such as the addition of a server for a specialized application, may have limited effect on the overall state of security; others, such as the addition of Voice over IP (VoIP) applications can radically change the kind of traffic on a network and introduce new types of vulnerabilities.
- When applications, servers, and network devices are patched, existing vulnerabilities may be removed and others may be introduced. One problem with patching is that currently functioning applications may break after a patch is applied. This is especially true in environments running distributed systems with complex sets of dependencies between components. In situations such as these, systems administrators may roll back a patch leaving a vulnerability unaddressed or they may change some part of the system configuration to work around the problem and, in the process, introduce yet another vulnerability.
- If a long-standing-but-unknown vulnerability becomes publicly known, the state of security changes. One example is the recently discovered weakness in the Domain Name Service (DNS), which could be exploited to poison DNS caches and route URL requests away from the correct server to a malicious system. The flawed code has been in use for some time, but once the details of the vulnerability were leaked, the security position of DNS systems changed dramatically.

- Malicious software changes in response to countermeasures. Malware now targets browsers as well as OSs. Although email was once the dominant means of spreading malicious code, drive-by downloads from compromised Web sites is now common. To avoid signature-based antivirus detection, viruses, worms, and Trojan horses use code-mutating techniques to change their binary signatures without changing functionality.

These changes are representative of the kinds of changes one faces with respect to IT infrastructure, but there are types of changes in security threats as well.

Understanding Change in Security Threats

In addition to malicious software, there are additional threats that can compromise confidentiality and availability of IT systems, especially with regard to content moving across the network.

Businesses face the potential for data leaks and data loss on their networks and with their mobile devices. Attackers have an array of ways to capture confidential information ranging from keyloggers capturing usernames and passwords to hacks into databases putting large volumes of data at risk. Information is not the only asset at risk, though.

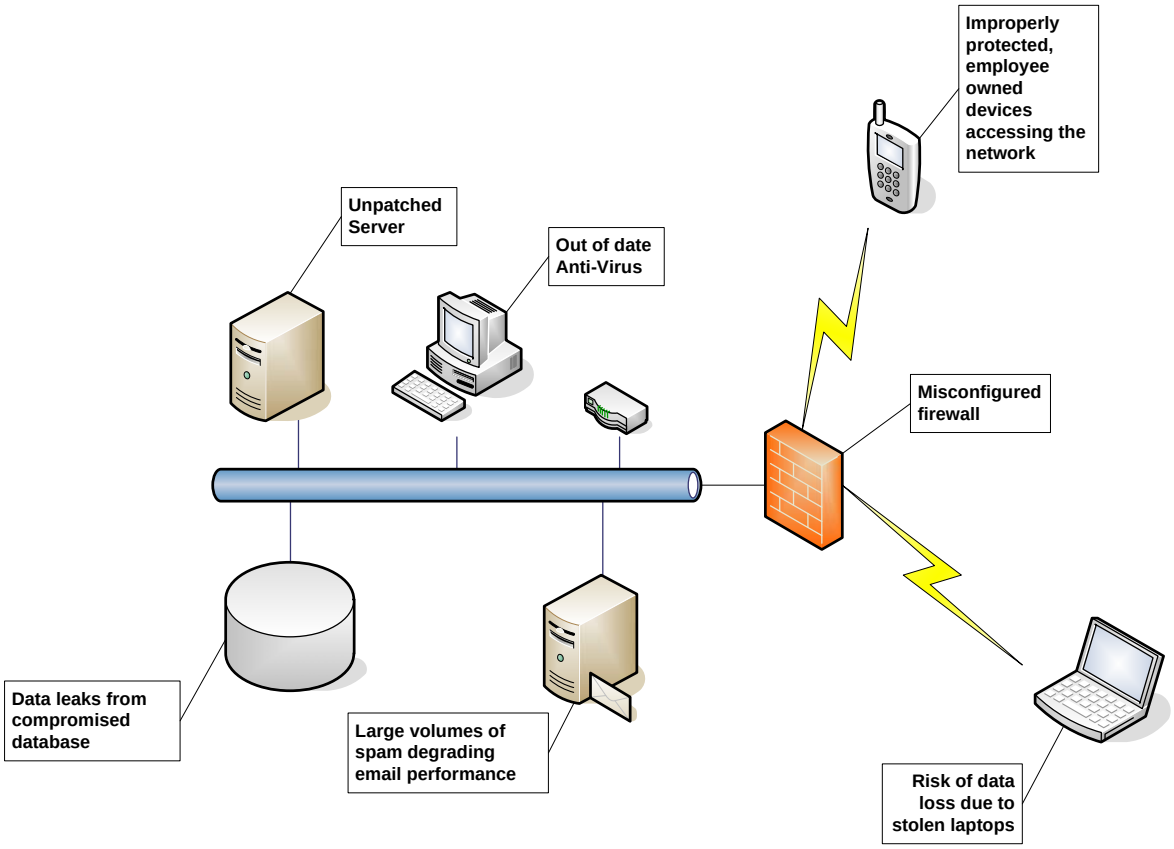

Figure 1: A wide array of security threats require attention to virtually every point on the network.

Botnets can commandeer the compute, storage, and network bandwidth resources of an organization. Compromised devices have reduced capability to perform business operations because CPU cycles are stolen for malicious activities such as generating spam and launching Denial of Service (DoS) attacks.

Spam continues to be a significant problem, with some studies finding more than 90% of all email messages are unwanted, unsolicited content. Although spam filters are quite effective, spam still consumes valuable resources and puts unwarranted demands on network resources.

It is also worth noting that attackers are changing tactics. As we become better at hardening servers and protecting the lower levels of the network stack, hackers are targeting the application level. Database applications may be subject to SQL injection attacks, browsers may be vulnerable to HTML attacks, and Ajax—a popular set of Web development techniques for creating rich Internet applications—applications present a larger attack surface for hackers. On top of this, IT departments are facing increased demands for their services.

Balancing Risks, Demands and Resources

Despite the fast-paced changes facing IT professionals, there is no assurance that their staffs and budgets adapt as fast. IT departments are faced with more demanding Service Level Agreements (SLAs), rapidly changing business requirements, and stagnant growth in budgets. The combination of a dynamic environment with static growth in resources leaves few options for IT professionals other than to constantly improve the ways IT operations are performed and to constantly strive for greater efficiency out of existing resources. Part of that extra efficiency will come from understanding how decisions about security changes impact day-to-day business operations.

Networks: What You Don't Know Can Hurt You

The state of constant change in IT infrastructure requires that we know as much as possible about the state of the network. Any change made in response to an emerging threat, no matter how well meaning, can inadvertently disrupt business operations. So what are systems administrators and network managers to do?

For starters, we must understand what kinds of applications are on the network and what kinds of traffic patterns these generate. Are there significant amounts of streaming audio and video on the network? Are rich Internet applications generating large-volume data transfers from servers to clients? Network managers need to know the types of traffic, the expected volumes, and the corresponding network performance associated with the applications running on the network.

This kind of information can be essential for evaluating network security measures, such as content filters and intrusion prevention systems (IPS). For example, how will an IPS scale to the traffic on your network? Will adding an IPS or content-filtering appliance degrade performance to the point that business functions are adversely impacted? Are some users more likely to be adversely affected than others?

One must also monitor how well existing security technology continues to function in the face of changes in the environment. As the volume of traffic increases, does the firewall become a bottleneck? Is unwanted variation in the time to deliver packets adversely affecting the quality of services, such as VoIP or streaming video? Attackers devise variations on existing threats to avoid security measures. For example, do anti-malware and anti-spam technologies continue to block unwanted content when delivered by Web site drive-by downloads rather than email? Continuing to monitor the performance of existing security technologies is essential to comprehensive security management.

The last question raises another key area of concern: knowing who is on your network. The key issue for network administrators is to understand how users are authenticated. If there are multiple authentication systems, which system controls access which resources? Is there synchronization between multiple authentication systems at the business-operation level? Not knowing how fundamental network services work can leave one making security, or even basic configuration, decisions that disrupt business operations. At the very least, network managers should know:

- How are users authenticated?
- What devices are connected to the network?
- Do remote access devices meet minimum security configuration requirements?
- Is the network at risk of access from rogue wireless access devices?
- How are employees, contractors, and business partners restricted to the resources they are authorized to use?

Knowing who and what are on your network at one point in time does not guarantee an accurate picture of who and what is on the network at another point in time. There is a constant challenge to know, for example, the patch levels of key pieces of infrastructure. Are servers that were considered hardened 6 months ago still hardened in light of new vulnerability discoveries? Client devices are even more problematic when users have administrative privileges. How can IT support staff know the configuration of antivirus, anti-spyware, personal firewalls, and other client device security measures without automated controls?

There are so many ways that a lack of information can adversely affect an organization that IT managers need to maximize the amount of information they can get from their security and asset management investments. The state of a business' IT infrastructure is constantly changing. Sometimes these changes are under the control of IT professionals and sometimes they are external changes; in either case, one must have accurate, up-to-date information about the infrastructure to protect and manage it properly. The remaining articles in the Essentials Series: Understanding and Responding to Network Threats will provide further details on how intrusion prevention and multi-function security products can help control the threats described here.