Part I

Network Security Landscape

IN THIS PART

Chapter 1

State of Network Security

In order to properly implement security, it's important to understand what we mean by security and problems with the current implementations. At the heart of securing the critical information of organizations are managing and controlling risk. While vulnerabilities are the common exploitation path into an organization, it's important to understand the ever-changing threat in order to make sure an organization focuses its limited resources in the necessary areas.

This chapter describes the formal definition of security and explains why so many attacks are occurring. It also discusses some of the key concepts of security, which you'll need in order to understand the rest of the book. Understanding the threats and vulnerabilities will help an organization properly focus its energy and resources.

IN THIS CHAPTER

Understanding the current state of network security

Determining the key characteristics of cyber security

Learning why attacks are successful

Cyber Security

Cyber security is all about understanding, managing, controlling, and mitigating risk to an organization's critical assets. Whether you like it or not, if you work in security you are in the risk-management business. Security is not about firewalls, IDS, or encryption; while these can be used to mitigate risk, the focus is on protecting an organization's information. Therefore, if you work in security, the following are pieces of information you must know in order to start addressing risk:

- What are an organization's critical assets or key information, the exposure of which would have a major impact on the organization?

- What are the top five business processes that utilize or require this information in order to perform their functions?
- What threats could affect the ability of those business functions to operate?

Once an organization knows what it's trying to protect, it can then start to implement security. All the money in the world isn't going to help if you don't have a clear definition of what you are trying to accomplish.

After you define the problem, all energy and effort should be focused on reducing risk. Therefore, before you spend a dollar of your budget or an hour of your time, you should be able to answer the following questions:

- What is the risk you are reducing?
- Is it the highest priority risk?
- Are you reducing it in the most cost-effective way?

These questions get to the heart of the problem — that it is all about risk.

Defining risk

While risk is covered in detail later in the book, it's important to define risk and its key components because it is at the heart of security. At a basic level, risk is defined as:

$$\text{RISK} = \text{THREATS} \times \text{VULNERABILITIES}$$

Risk is the probability of loss, which means there is some uncertainty involved. If something is guaranteed to happen, it is not risk. While some people say that security is a losing battle, that is clearly not true. If risk were not something that could be managed and controlled, insurance companies would have gone out of business long ago. The fact that insurance companies are still around and make a profit shows that, with proper analysis, risk can be properly managed.

When some people look at the preceding formula for risk, they say that it's missing key components, mainly likelihood and impact. To deal with those, the risk is plotted on a two-dimensional matrix with the two axes being likelihood and impact.

Threat is the potential for harm. Anything from a hurricane to a virus to a worm can be viewed as a threat that impacts an organization. Vulnerabilities are weaknesses that allow a threat to manifest itself against an organization. Two of the most common vulnerabilities are unpatched and misconfigured systems.

Background: How did we get to this point?

Many businesses, either after being attacked or hearing about other businesses being attacked, have invested money in perimeter defenses in an effort to avoid losses. These losses come in many different areas, from revenue and resources to a company's reputation, a continuing concern.

State of Network Security 1

From the late 1990s through early 2000, everyone's concern seemed to focus on Y2K and its impact on legacy systems and software. With that bullet dodged and most businesses coming out relatively unscathed, IT budgets diminished rapidly and the focus was placed back on company operations.

The world was challenged on many different levels, and Internet and local network security issues did appear from time to time, but after a little quick-fix perimeter tightening and a few internal scans and recoveries, life went on. Technology was being introduced into more facets of our nation's critical infrastructure. Remote control, minor auditing, and autonomous operations were becoming more the norm.

Early on, some industries, especially the financial and medical industries, experienced security issues with their customers. Concerns about personal security, privacy, and identity theft began to flourish worldwide. Methods were slowly being developed to manage our resources through implementation of PKI (public key infrastructure) and SSL (secure socket layer) protocols for communication.

A major drawback began to be evident throughout these years: we wanted to put technology in place yet lacked an understanding of its weaknesses and its security capabilities and shortfalls.

So this brings us to our current state. Where are we in network security?

Many companies and software applications offer the ability to protect our communications, protect our devices, encrypt and protect our data, and maintain our mission operations or status quo.

Our nation's network infrastructure is such that many facets and their weaknesses have impact on other critical infrastructure components. A lot of trust is placed on SCADA (supervisory control and data acquisition) devices throughout our electrical, water, and gas grids. These devices, most of which are remotely controlled from many miles away, are growing much more complex. In earlier days, these devices were either on or off, and if a fault was detected by some means, the devices would fail to a default state. Now, we have smarter SCADA devices that can "think" for themselves to determine a timeframe or amount of actuation based on circumstances. We still have remote communications for management and monitoring, but these communication channels are not always encrypted or dedicated and thus separate from other Internet traffic. And if the monitoring or management station does happen to have a dedicated circuit, it may still be connected to a larger network through other network routing devices, thus providing another way in.

Our networks are becoming more and more interconnected and dependent on each other in matters of function, resilience, and fault tolerance. Air traffic control is dependent on power grids and both are dependent on weather alerts and national disaster monitoring for smooth and reliable operation, as well as for awareness of fault levels or preparation levels for shifts in the environment or state of the grid.

Intelligent people and companies have devised ways to manage our security, implement the control lists we develop, and use the secure protocols we design for secure transactions — but not without limitations.

Network attacks are so successful because we ourselves do not fully understand, or choose to understand, the vulnerabilities of our own appliances and applications. We do not fully test, document, certify, and periodically retest for validation the systems we choose to rely on for our security.

Cyber security's balance comes from implementation of the appropriate security measures based on one's knowledge of system weaknesses — knowledge necessary to assure mission success.

Moving beyond reactive security

A paradigm shift has to occur in how we handle security. Today most organizations focus on threat-based security, which leads to a reactive approach to security. Organizations wait for a new worm, virus, or exploit to come out, and then they react to the problem by patching the system or configuring the system in a secure manner. As the window closes on how quickly attackers break into systems, reactive security does not scale. This is because by the time you react to an attack, the damage is already done. The proper approach is to focus on vulnerabilities or ways attackers get into systems. In other words, do not simply react to security breaches; be prepared ahead of time by identifying vulnerabilities that can be used to compromise critical assets. Take a proactive security approach that enables you to fix the problems before the attacker breaks in, not after the attacker has already succeeded.

Trends

While functionality has been the driving factor behind the current Internet wave, it is this same functionality that is causing the current security problems. The ironic part is that the vectors of attack are often enhancements that no one is using, except the attacker. Removing these vulnerabilities would have minimal impact to the user but greatly increase overall security. For example, two of the biggest risks today are phishing attacks and cross-site scripting, both of which occur because of HTML-embedded e-mail. Very few organizations/people require HTML-embedded e-mail in order to do their jobs, so if this feature were removed, it would not have an impact on the user but would increase overall security. By carefully analyzing and understanding what functionality is needed, a least-privilege approach can be created.

End-point security is also critical. As long as an individual has administrator access to a local system, optimal security will never be achieved. Through the use of newer operating systems, users can be given privileged access without affecting security. Key factors are removing the ability to install or download rogue programs and to disable security features.

An overarching trend is the movement from reactive measures to proactive security. This shift will emphasize mission resilience, homing in on the critical business processes of an organization. We have to accept the fact that networks will be compromised. But we can make sure that whatever happens, the key operations of the business will continue. This is what will differentiate between organizations that survive a new series of cyber attacks and those that don't.

Key characteristics of attacks

The following are some of the key characteristics of current attacks.

Attacks are growing dramatically

In today's technology-centric society, threats continue to plague business and government. As better ways are found to defend against attacks, attackers develop new and different ways to bypass this protective technology. As this criminal activity increases, the number of attacks and instances of malware also are increasing dramatically.

Threats are more sophisticated

Threats have gotten more sophisticated with a change in the type of criminal. The attacker profile has moved from an individual looking for notoriety by shutting down a system or defacing a Web site, to more a dedicated attacker motivated by financial gain and a desire for control through the use of criminal activities. As a result, attack profiles now reflect the presence of organized crime, terrorists, nation states, and espionage. This change appears to be a direct result of the realization of the value of information; as a result, attacks have moved from traditional denial-of-service (DoS) to more information stealing and control by stealth.

Knowns outnumbered by unknowns

Knowledge of one's adversaries has always been a key aspect of winning battles. Intelligence on their activities, capabilities, and resources allows you to focus your efforts on defending against their particular types of attacks. You might think that because we've developed software and hardware and made them work together, we would understand them inside and out and be able to protect all known vulnerabilities. But we have not, in fact, developed all our resources, and we rely mostly on third-party applications and appliances. So we do not have full knowledge of the entire structure. Therefore, we can only focus on what we know while being alert and ready to respond to each and every attack, including attacks we aren't currently aware of.

Current approach ineffective

Because of the ever-changing nature of the attacks on our systems and applications, we've tried to mitigate the threats by putting more resources into research and development in an effort to curb vulnerabilities.

But new types of cyber-defense solutions have become necessary to counter new types of threats. Traditional attacks were focused primarily on the network and operating system, but as strides were made to protect those areas, the value of information also increased, and the attacks have now moved up the stack. They presently tend to target the application itself and the hosting infrastructure, in an attempt to gain both access to information and control of machines from which to launch other attacks. In short, mitigation approaches by themselves are no longer sufficient to address the level and type of attacks that are presently occurring.

Summary

People often talk about how much more proficient the attackers (offense) are than the people defending networks. This is not true at all. The defense simply has a much harder job than the offense. The offense has to find only one vulnerability in order to compromise a network, but the defense has to find every vulnerability in order to forestall attacks.

The new trend is not to be reactive and randomly repair vulnerabilities, but rather to proactively prioritize vulnerabilities and focus in on risks that have the highest impact and are most likely to cause harm to the most mission-critical systems.