ASIA

Not having a security architecture

By Daniel Minoli

Network World |

28 AUGUST 2006 16:00 SGT

It seems like we read about an IT security infraction just about every day. This ought to be somewhat surprising, given the large amounts of emphasis placed on security over the past 25 years as measured by industry research, investments, resources, equipment, training, courses, certifications and books dedicated to the topic.

The problem is that most companies lack a comprehensive architectural framework for the uniform and organized treatment of all aspects of IT security.

So what is a security architecture? An architecture is a blueprint for the optimal placement of resources in the IT environment, with the goal of supporting the organization's business function.

A security architecture is a plan that describes (a) the security services that a system is required to provide to meet the needs of its users, (b) the elements required to implement the services and (c) the behaviors of the elements (including the performance goals) to deal with the threat environment.

Minimum requirements

To address security challenges in an effective manner, both of the following are needed:

1. An overall security architecture.

This is a master plan that includes security considerations for administration, communication, computers, emanations (radiation), personnel and physical issues.

Clearly, hardware IT/network components must be secure; software components must be secure; and personnel must be trustworthy (many infractions originate from within).

2. Policy specifications.

This describes how to implement and adhere to the architecture. Even if the right architecture is in place, if the policies fail the enterprise is at risk.

In addition, a robust security architecture must be based on the concept of multiperimeter protection, and it must embody the idea of separation of privilege. Layered frameworks are recommended, because layering has the advantage of defining contained, nonoverlapping partitions of the environment.

The seven-zone approach

Companies today have to deal with a broad set of IT environments, particularly with the increased reliance on connecting with external suppliers and business partners. Each of these environments has its own security exposure and each requires different approaches to asset protection.

Typically, there will be unsecured zones, semisecure zones and secure zones. Fortunately, these zones can be organized so that defenses-in-depth principles can be put in place.

Zone 7: Protecting physical assets and network traffic

If potential intruders have the ability to get physical access to some equipment or to intercept signals, no amount of firewalls, proxies or certificates will protect the organization. LAN wiring, PCs and some wireless services (nonsecure hot spots, home wireless routers without encryption, some cordless phones, Bluetooth-based devices) are examples of unintended radiation that can be intercepted.

Other wireless services (cellular, satellite, corporate wireless LANs and secure hot spots) are examples of radiation environments where appropriate signal protection is required to eliminate the risk of interception.

Zone 6: Protecting access

In this first-tier security zone, basic credentials and access privileges are validated, and a mediation function is often supported. Typically, this is a point in the intranet just outside the front-end demilitarized zone (DMZ) where communication sessions are proxied.

The repository of credentials, which should be part of the centralized enterprise directory, is typically in a more secure zone (beyond the back-end DMZ and accessed by the proxy server via an industry-standard protocol, such as Lightweight Directory Access Protocol). Intrusion detection/prevention systems may operate in this environment to deal with possible infractions.

Zone 5/4: Protecting internal data stores

These zones implement the defense-in-depth principle and are increasingly more protected than the first-tier zone by groups of firewalls and gateways. Security verification functions create internal zones where company-sensitive records, databases, directories, credential/certificate-management stores, and so on, are protected. Intrusion detection/prevention systems may also operate in this environment to deal with possible infractions.

Zone 3: Protecting applications

Applications have their own application level security functions. However, these applications should not replicate credential/certificate-management stores but rely on a centralized enterprise directory.

Zone 2: Protecting operating systems

Host operating systems have their own security functions to protect middleware, microcode and executables. Many infractions are related to weaknesses of the underlying operating system.

Zone 1: Protecting data at rest

Finally, the data should be encrypted when it is transmitted and when it is stored in a device such as a disk drive, RAID system, tape or virtual tape. The example of the risk involved when a laptop that has a content-rich disk drive is lost should make the need for this level of encryption clear.

Given the avalanche of daily security threats, the case for proactive management of these IT and network security risks does not require much more proof. But beyond a hard-to-maintain cornucopia of fragmented tools and one-off solutions, an approach based on security architecture provides a comprehensive and reliable methodology to enterprise risk management.

Minoli is an adjunct professor in the Stevens Institute of Technology's graduate school. He just published the Minoli-Cordovana's Authoritative Computer and Network Security Dictionary. He can be reached at minoli@att.net.

Security architecture models You don't have to roll your own; there are several standard security architectures that you can choose from.

International	This standard provides a general description of security services and

Standard ISO 7498-2	related mechanisms that can be ensured by the security reference model. It covers security attacks relevant to Open System, general architectural elements that can be used to thwart such attacks, and circumstances under which the security elements can be used. This model, however, is somewhat static and in need of modernization; a lot has been learned about security since this model was published in 1989.
Moriconi, Xiaolei and Miemenschneider Methodology	This architecture is formalized in terms of common architectural abstractions; then it is refined into specialized architectures — each one is suitable for implementation under different security assumptions.
Whitman & Mattord Methodology	This methodology makes use of the following architectural layers: physical, personal, operations, communications, network and information security.
NIST Special Publication 800-27, Security Principals and Practices	A comprehensive model for information security and an evaluation standard, it includes Lattice Model (a mathematical structure of elements organized by a relation); Bell-La Padula Confidentiality Model (sensitivity levels); and Biba Integrity Model, which defines integrity levels in terms of the Bell-La Padula levels.

Next read this:

- *9 career-boosting Wi-Fi certifications*
- *What is MPLS, and why isn't it dead yet?*
- *11 ways to list and sort files on Linux*
- *5 free network-vulnerability scanners*
- *How-to measure enterprise Wi-Fi speeds*

The 10 most powerful companies in enterprise networking 2022