Management of Information Systems

Security and Related Topics

Curt Ireton

Screened Subnet/DMZ

The Screened Subnet/DMZ firewall architecture is used most importantly to prevent attacks or threats from an outside network, such as the internet, to an inside trusted network, such as a data server. The Screened Subnet/DMZ firewall architecture is considered best practice.

The architecture is set up in a three-tiered architecture with (1) external networks, such as the internet for e-commerce, (2) applications which are stored on dual-homed Bastion servers, and (3) data servers where information is stored and retrieved.

Incoming data is screened by an external packet filtering router, sent to a DMZ (demilitarized zone) consisting of dual-homed Bastion host that are currently patched (protected from known attacks). These servers are hardened, which means that all unnecessary services and ports have been turned off and the computers are physically locked down, and contain primary application servers which, for instance, can be used to act as a medium between the web server and the database server. These dual-homed hosts are often used for network translation and configured for performance. Data can then be processed and sent through an external packet filtering router into the internal network, and vice versa.

The security benefits to a company with e-commerce, or data-related web pages, would be that when a packet containing information comes in to the company it is first filtered by a router, then sent to the DMZ instead of directly into the company network, and will be screened to allow only the application meant to handle the transaction serve the data to the internal network. This is further screened by an internal firewall, and will never allow a threat or attack get into the trusted network.

Cyber Attacks

The Morris Worm is considered the first worm to invade the internet. It was created in 1988 and worked by exploiting known vulnerabilities, including passwords, of computer systems. It could infect computers multiple times and slowed them down to the point of being unusable.

In 1994 Russian Vladimir Levin hacked into Citibank's system using passwords obtained by intercepting Citibank customers' phone calls and obtaining account numbers and PINs when they punched in this information. He then transferred an estimated $10 million to dummy accounts in several countries.

Mitnick's Synflood Attack took place against Tsomura Shimomura who worked at the San Diego Super Computer Center, in 1995. Shimomura's network consisted of one server into which many clients were connected. Mitnik used a synflood attack to keep one system from being able to transmit. While it was in a mute state the attacker assumed its apparent identity and hijacked the TCP connection. This could be done because it was a trusted network with no need for a user name or password.

The "Mellissa" virus was the first to affect the newly commercial internet in 1999. It propagated itself from a file called list.zip, which was supposed to contain passwords for adult web sites, by exploiting a hole in Microsoft Outlook when users downloaded the file.

The "I Love You" virus redirected the victim to a malicious web site where a malicious program called "WIN-BUGSFIX.EXE" was downloaded onto their computer. This Trojan Horse would find passwords and send them to an internet account in the Philippines.

Yahoo/Amazon DDOS (Denial of Service) Attacks represented the evolution of the previous DDOS attacks by using more people in the attack. Computers were exploited and programs were installed to be called by their handlers, when the attacker called the handlers.

Code Red II worm infected computers pseudo-randomly and used a pattern of repeating "X" characters to overflow the buffer, exploiting this vulnerability and allowing the worm to execute arbitrary code and infect the machines. The Nimda (Admin spelled backwards) worm spread within 22 minutes. It was thought to be a political attack.

In 2002 vulnerabilities in SNMP (Simple Network Management Protocol) could enable an intruder to gain unauthorized access, launch denial of service attacks, or cause unstable behavior.

The Slammer worm caused denial of service in 2003. It spread rapidly, infecting most of its 75,000 victims within 10 minutes. It exploited a buffer overflow. Its growth rate followed an exponential curve with a doubling time of 8.5 seconds. This also was thought to be political.

This all tells us that the scope and size of hacking is increasing. What used to be simpler, single-person hacking for money has escalated into concerns of multi-person hacking for political reasons. A problem is that as hacking gets easier, security measures are tougher to enforce. The main solution to this problem is including security as an integral part of system requirements.

Sphere of Security Model

The implication of the Sphere of Security model is that security consists of technology and people and we must have both.

The model consists of four spheres of technology: information, systems, networks, and internet. These are protected by, among other things, access controls which consist of authentication: confirming the identity of the entity accessing an area; and authorization: determining what that entity can do in that area. These protect information, systems, and networks. Authentication mechanisms consist of three types: something you know, like a password (this is the weakest type); something you have, like a token; something you are, like fingerprints or biometrics; or something you produce, like voice or signature. At least two different mechanisms must be used for strong authentication. Authorization includes authorization for each authenticated user, for members of a group, or across multiple systems.

Contrasting access controls, the people side of the model protects these same areas with security planning, and policy and law which is the only protection shown for the outer circle, or the internet.

Security and planning consists of incident response (IR), which handles a security breach, and disaster recovery (DR) and business continuity (BC) which both involve planning how to recover in case of a major catastrophe. The obvious strength of policy and law is simply that people won't do something because they might get caught.

Education and training protects information because it is handled properly.

Though there are many protections and more spheres to protect on the technology side, there are only two spheres on the people side of the model because people bypass the other spheres as end users accessing the information. Both sides of the sphere of protection must be in place to make this model work to accommodate the technological security and the implementation of the human protection, to provide for an overall safe system.

NSTISSC Security Model

This model represents three dimensions central to information security as both an extended line graph and a 3-D cube. It includes the components of the CIA (Confidentiality, Integrity, and Availability) Triangle which focuses on protecting data, information, networks, and other assets while ensuring they are complete, accurate, and usable. Security is usually shown somewhere in the middle of the triangle, with give and take being elements that have to be bargained with, however in this graph they are extended along an axis to relate to the other fundamental phases of security.

Confidentiality means that only those authorized may access certain information. Some of the threats are hackers, unauthorized users, unprotected download of files, people disclosing data, or simply the loss of a flash drive.

Integrity is the quality of being whole, complete, and uncorrupted. It means trusting that the data that comes out of the computer is the same as the data that went in. This should be in accordance with the Sarbanes-Oxley act. One of the measures taken to ensure data integrity is file hashing where an algorithm attaches to a file, and returns a number when it downloads that can be checked to confirm that it is the same file.

Availability enables the user to have information when they need it, in a useful way. It is protected against denial of service and other obstructions. One measure used is reliability which means given some inputs, how accurate are the outputs?

The line graph depicts that as the extension of the components of the CIA Triangle reach confidentiality, technology functions have been extended past policies and education of end users, and data has been securely stored, processed and transmitted. This line graph is meant to show an extension into a cube.

The cells of the cube represent intersections among the three dimensions of the graph, and all 27 intersections must be addressed to secure information systems, and manage organizational risk. These together comprise an overall security program.

Data Warehouses

The data in this data warehouse is shown as a data cube that views the dimensions of location, product, and date from the multi-dimensional data warehouse. Since data warehouses may have many subjects, breaking these subjects into data cubes at the onset is useful for decision support based on patterns associated with this summarized data, though not necessarily useful for determining meaning.

For example, “slicing” this data cube would find a subset of all sodas sold in the Southeast. The “dice”, or subset of the member values of the slice of Southeast for Orange sodas (sold) on 1/1/2000 is 85; whereas the amount on the next day, 1/2/2000, may be higher or lower. This may have occurred on a sunny day, a weekend, or some other factor which is not necessarily significant to the reason the sodas were sold, but might define a pattern. If we “drill down” into this segment we will find different levels of data, such as states sold in, cities, and stores, and even time of day. “Rolling up” we may find such data as manufacturer of the sodas, countries the soda was bottled in, etc., removing detail from the dimension.

Since data cubes consist of many layers and a tremendous amount of data, data warehouses can be quite large. Manipulating data in a data warehouse and extracting information for an ad hoc query is the analytics through which data mining discovers patterns. The operator may determine significance. It is important to note that it is difficult to do things like ad hoc queries unless the data warehouse is designed to do them.

End Users

End users are non-IS professionals who use computers, and end user computing is the activities performed on computers by those professionals. Since the focus of an IS group is often on maintaining enterprise infrastructure and work process systems, the IT needed for specialized tasks, encountered by various groups operating in the corporation, can be easily overlooked.

End user computing includes the use of smaller work process systems, email, and other basic software. Often the end users need specialized software for particular tasks such as analyzing or designing, and need to have programs custom built. Also, end users build and maintain/support their own systems. Sometimes there will be a group where expertise exists, apart from IS, formed to create such systems. These systems are often not aligned with IS structure.

As personal computers are more prevalent, innovation of systems are adopted for specialized needs. This is due to a perceived lack of support by the IS.

End users support others use/acquisition of IT, learn to use the IT, and maintain the systems. One main advantage is the ability to do ad hoc reporting which is considered a tremendous strength. The end users must learn to use databases, and for common reports and queries these databases need to be part of a formal system. To put these systems on an enterprise level would be cost prohibitive, and unnecessary because they are often used by only a few people.

With IT focusing on enterprise level, smaller groups may use IT as they see fit. Systems are developed by these groups that are often outside the standards of the organization's IS. However as long as end user computing is managed within the bounds of traditional IS, as a shared partnership of responsibility and authority, end users can enhance their productivity by adapting, or developing, systems to meet their needs. It is suggested that policies and controls remain with the end user organization and not IS.