The seven layers of IT infrastructure

Bryan McKinney

Liberty University

Professor Jeffrey Humphries

CSCI 561 - Ethics, Legal Issues, and Policy!

December 12, 2018

Research Objectives

- Describe the seven layers of IT infrastructure.
- Discuss the how each layer plays a role in a typical IT network.
- Discuss the advantages and disadvantages of each layer in a network.
- Discuss the potential security concerns that can be associated from each layer.

What are the seven layers of IT infrastructure? The seven layers of any IT infrastructure are as follow: Users, Workstations, LAN, WAN, LAN-To-WAN, Remote Access, and finally System/Application. Each of these components play an important role in the whole schema of a highly functioning network. Each of the layers listed above have risks associated with them and the grouping that has been set is a way to make understanding those risks a bit easier. Each layer has their own advantages and security concerns that will be addressed and looked at in greater detail in the sections to follow.

Each layer of the seven mentioned above plays a vital role in the scope of a network. With much greater detail given below a general overview of each is important to set the tone for what is to come. The user group is a reference to any person that would accessing the network. The Workstation group is a endpoint device that access the network and is another node. The LAN group is the networks local area network and the route for all communications between nodes. The Wan group is typically the infrustruce used to connect one office location to another via the internet. The LAN-To-Wan group is the infrustruce that connects the lan to the wan networks. The Remote access group is the means by which a user would connect to a local network (LAN) via the internet (WAN) connection. Finally the System/Application group refers to the physical hardware and/or software that is needed to collect and process data.

Each layer has their own distinct advantages and disadvantages when we look at them from a security perspective. Also each layer has there own level of security concerns that need to be addressed and potential weaknesses that can exploited upon. When we dive into each layer a bit deeper we will see the good and bad and explorations that can happen when a network goes unchecked and not properly maintained.

Literature Search Results

The user group is the group that looks at any person that might have access to a network. These people can be your employees, customers, consultants, contractors or any other third party that might come into contact with your network. Users are important to your network as they are the ones working and doing business that makes your business thrive. The harm that can arise within the user group is not educating them on how to function on the network. By not educating users you leave a wide host of unmitigated issues. For instance not detailing how your privacy policy works. The importances of a privacy policy is that it “addresses the importance the organization places on protecting privacy. It also discusses the regulatory landscape and government mandates. This policy discusses how to handle customer data as well as the individual obligation to protect the information” (Johnson, 2018). The biggest threat to the user group is authentication. When an organization sets up any authentication policy it needs to consider the risk analysis of what happens when property authentication techniques are not considered. Other risks include: “Users can destroy data in application (intentionally or not) and delete all files. Users can find that his girlfriend cheated on him and use her password to delete all her work so that she can be fired. Finally users can insert infected CD or USB flash drive into the work computer" (Kolawole, 2017).

The workstation group are the devices(nodes) that are used by the end users. These devices can include: laptops, cell phones, PDA's, tablets, etc. the potential security concern that is present, first is that of authentication. Does the user have rights to access this workstation? If no then they need to be stopped. But if they do then is the device they are using need to be filtered from the network? For instance, is the workstation a cell phone that needs internet access but not access to the SQL databases running in the backend. Another security concern for the workstation group is that of protection against viruses/malware/and spyware. Take the proper steps to prevent those attacks from operating on a workstation takes planning and resources to accomplish. Other risks include "A workstation's browser can have a software vulnerability which allows unsigned scripts to silently install malicious software. Or a workstation's hard drive can fail causing lost date." (Kolawole, 2017).

The LAN group is comprised of the physical devices that make up the LAN network. Those devices include but are not limited to: A router, Switches, firewalls, and an array of different types of servers. There are many security concerns within the LAN group. Mr Kolawole says "A worm can spread through the LAN and infect all computers in it. LAN server OS can have a known software vulnerability. An unauthorized user can access the organization's workstations in a LAN" (Kolawole, 2017). All the different types of servers need to be accounted for. For instance a simple web server can have a wide range of attacks that can be carried out against it. Also “As soon as the LAN is connected to another LAN or the Internet and becomes a WAN, all of that changes. The company does not know what physical protections have been made to the rest of the WAN, only its small portion. In the case of an Internet connection, they have no idea who might try to access their LAN. The entire threat model changes. Not that any of the threats from the LAN-only environment have gone away, but many more have been added. One can think of the threat profile for a LAN as being a subset of the threat profile for a WAN.” (SearchSecurity, 2001).

The WAN group is the layer that is primarily comprised of the internet. Another part of the WAN group would be any VPN services that needed to be set up for members of the organization to be able get onto the LAN service. Those VPN connections need to be encrypted to keep would be hackers and other cyber criminals from snipping packets and eavesdropping on activities between an employer and it’s employees. Mr Kolawole said “IT Network security is becoming of great importance because of intellectual property that can be easily acquired through the internet. Currently, internet is considered a data network. Since the current data network consists of computer-based routers, information can be obtained by special programs, such as Trojan horses, planted in the routers. This is the basic reason why security is emphasized in data networks, such as the internet, and other networks that link to the internet” (Kolawole, 2017).

The LAN-To Wan group is essentially the bridge that connects the two different infrastructures together. The main way you can effectively connect and keep and information secure between the WAN to LAN connection is by setting up a DMZ (Demilitarized zone). The DMZ “sits on the outside of your private network facing the public Internet. Servers in the DMZ provide public-facing access to the organization, such as public Web sites. They are especially hardened against security breaches because the servers are easily accessible to the public and hackers. Sitting between the DMZ and internal network are firewalls that filter traffic from the DMZ servers to the private LAN servers” (Johnson, 2018). There are other risks that can be associated with the LAN-To-Wan group, for instance “Weak ingress/egress traffic filtering can degrade performance. Or a firewall with unnecessary ports open can allow access from the internet” (Kolawole, 2017).

The Remote access group is a more robust version of the user group. Here in the remote access group you are moving from an unsecured environment (WAN) to hopefully a secured environment (LAN). The main security concern is multiplied levels of authentication. Other risks include “Communication circuit outage can deny connection. Remote communication from office can be unsecured. VPN tunneling between remote computer and ingress/egress router can be hacked” (Kolawole, 2017). Another security concern is “Many enterprises permit (or fail to regulate) the use of third-party file storage services to facilitate remote access to data, but when files end up in cloud-based repositories, enterprises lose control. When Dropbox left user accounts wide open last June without realizing it, it's likely many ad-hoc enterprise data repositories were exposed. Screen sharing and remote administration software weaknesses are an increasing concern. A 2011 report from Trustwave found remote management software was one of the most commonly used attack vectors. And good luck to anyone using Symantec Corp.'s Norton pcAnywhere software; the ambiguous technical document released last month does little to assuage fears that the product has been completely compromised in the wake of Big Yellow's 2006 source code breach. Plus, recent research by Rapid7 CSO HD Moore found thousands of systems using pcAnywhere with open ports that could be accessed by an attacker. VPNs risks can't be ignored either. Trustwave also found a VPN or similar remote access method was exploited in more than half of the data breaches it investigated last year. Few though were as devastating and public as the Gucci network attack, in which a former employee used a VPN connection to wreak network havoc from afar" (Parizo, 2012).

The System/Application group is the final group. In the system/application group unlike in all the other groups this is the layer that many of your end users will use the most. This is the layer where the end users use the software and applications that they need to do their jobs well and efficiently. The security concerns here are those of software patches that are needed to make any third party software more security as well as OS fixes and updates that the operating system developers release to keep their software secure. An example of a typical operating system that is frequently used is Windows Server 2008. Mike McKenna defines server 2008 as "A server operating system produced by Microsoft with the ability to share files and printers, act as an application server, host message queues, provide email services, authenticate users, act as an X.509 certificate server, provide LDAP directory services, serve streaming media, as well as perform other server-oriented functions” (McKenna, 2010).

With knowledge on all seven layers of IT infrastructure we can look at other means of security that have yet to be presented. A important defense against software or people sniffing on a network is to use a IDS (intrusion Detection System. A IDS is “a device or software application that monitors network or system activities for malicious activities or policy violations and produces reports to a management station” (Kolawole, 2017). Another popular and vital way to ensure all traffic is encrypted is to utilize SSL (Secure Socket Layer). SSL is ”a protocol that is designed to create a secure channel, or tunnel, between a web browser and the web server so that and information exchanged is protected within the secured tunnel. It provides authentication of clients to server by using certificates” (Kolawole, 2017).

Conclusions

After compiling all my research and data I believe I have a better understanding what all goes into make each layer of the seven domains secure. Each layer has their own unique characteristics and properties that you have to account for. Each layer has their own set of disadvantages as well. Some are easier to secure while others have a wide range of security issues and potential risks that are hard if not impossible to account for. Mainly the end user factor. You can not account for every type of user and every skill level they may have. Some users will have authentication issues and others will be able to negate any system blocks with relative ease. When I was doing research on the seven different layers and how they all worked together to make a secure network I was reminded of Romans 12:6-8. Paul writes “6 We have different gifts, according to the grace given to each of us. If your gift is prophesying, then prophesy in accordance with your faith; 7 if it is serving, then serve; if it is teaching, then teach; 8 if it is to encourage, then give encouragement; if it is giving, then give generously; if it is to lead, do it diligently; if it is to show mercy, do it cheerfully” (Romans 12:6-8, NIV). I see a strong correlation between Paul’s words written to the roman church and the seven domains. Each domain has a specific purpose. No one domain is any greater then next or the one before it. They all play a role in an all encompassing umbrella of security. Just like the people of the roman church. Each person has a unique gift given to them by the Lord. No one is any greater than those around them. But they should use their gifts in a humble manner to serve each other in a God honoring way. Same goes for the different domains. Each layer builds upon the next to keep everyone in line and secure. Keep a network secure is a difficult job with a wide range of responsibilities and pressures. I like to think Paul felt similar pressures during his ministry. He was ministering to many different disciples as well as different groups of people all at the same time. He understood the work he was doing had a greater purpose. For the church to work the way God intended it to the everyone would have to play a role and be responsible for their own set of unique tasks. Similarly like in a IT department. There are many different teams that are all working together for the great good...to keep the IT operations up and running so everyone else can accomplish their goals and be productive members of the organization. Finally I leave with Colossians 3:23 “Whatever you do, work at it with all your heart, as working for the Lord, not for human masters.” (Colossians 3:23. NIV). Any work we take on we should be doing for th Lord and not for the people around us. Our work is important while we are here on earth and for the IT professional we have a responsibility to keep those around us safe. Having an deeper understanding of the seven domains of IT infrastructure is important because it gives us insight into all the components that make up a network and how they are to work together.

Bibliography

Johnson, Rob (2018). Security Policies and implementation issues(2nd ed.). Cambridge, MA: Wiley.

Kolawole, Emmanuel (2017, November 27) Partical approaches to securing an IT environment Retrieved from https://file.scirp.org/Html/4-6101641_80763.htm

McKenna, Mike (2010, December 15). Active Direcotry Optimization Reference Architecture Retrieved from https://dodcio.defense.gov/portals/0/documents/diea/adora_final_v1_20101215.pdf

Parizo, Eric (2012, March). Secure remote access? Security-related remote access problems abound Retrieved from https://searchsecurity.techtarget.com/opinion/Secure-remote-access-Security-related-remote-access-problems-abound

(2001, October). Security differences between a LAN and WAN Retrieved from https://searchsecurity.techtarget.com/answer/Security-differences-between-a-LAN-and-WAN