CIS Critical Controls and their Vital Roles

Erika Hernandez

NET 4740 Security Vulnerabilities and Intrusion Mitigation

Dr. Paulson

April 10, 2022

CIS Critical Controls and their Vital Roles

We have given the opportunity to choose from a list of top 20 security controls. These very in different levels. Basic, Foundational and Organizational, these categories have the different topics in each to choose from. The topics I choose are topics that interested me and I wanted to learn more about. These I feel, are topics that would be useful in my current role. The topics I choose in the Basic level are Inventory and control of hardware assets. In Foundational Malware defense, Data protection. In the Organizational section I went with application software security. In this paper we will look further into these topics, and in my words I will explain more about the importance. Also how these will help any organization on the internet.

Inventory and Control Hardware Assets

The first topic I wanted to look further into was Inventory and control hardware assets. This was something I chose because at my work we were dealing with inventory issues. The issues were were having was that I would work around my organization at work and would look up a persons name and found nothing that belonged to them. At the same time if there was a computer monitor in front of me with an asset tag I would look it up and the person sitting down would not have that monitor assigned to them.

So essentially this was a huge problem if you can image, so we had to update everything at the same time we would have to make sure that all HR get the equipment back from the employee and return to the IT department where they would clean and reissue to the next employee. Not they would just hold on to it and give the credentials to the new employee.

As I was reading about this it confirms the why behind keeping track of all the devices on the company network. We need to protect the company and the assets on the network. If we dont know who has what then we wont know who has access to the companies information. At the same time knowing what is on the network is also good so we can do updates, patches, also we would know the location, IP address and more. As we are moving towards the direction of the future. Everyone has a min computer and its called a phone. With technology and where its heading, everyone almost has one at all times. As more companies are allowing them to connect to the network its also important to know to be extra cautious. Another reason why its important to know who has what of the physical side of things.

Malware Defense

So having an inventory and list of hardware on the network is important because it brings me to my second topic Malware defense. If we have a list of all the hardware in the organization we can push updates. Such as antivirus, anti-spyware and more, so many people don’t know and or don't want to update their systems. So what do they do? They just ignore updates not knowing that updates are very important. As we are moving in the direction of the future we are seeing more and more types of viruses that are out there.

Which is why its super important to update machines. What people do in their home is one thing, but when you have a company that is worth millions. Hackers are looking for that one time you lower your defense and that can be the small window they needed to do damage. Back in the day you had 400 hundred employees you had to manually go around and update all of those. Now with it being automated all you need to do is send out a push and it will automated the process. Also it will force the update even if the user doesn’t want the update.

Malware comes in all shapes and sizes, meaning that you there are a number of different types of infections that can happened with in your organization. You can have a Trojan, ransomware, and more. The number one way computer users get these types of attacks comes from a user. They can click on attachment, go to a wrong website and more. So again this is why its super important to have and up to date protection and system in place for this type of attacks.

Data Protection

Then it brings me to the next topic that I chose which is Data Protection, what is does this mean? What is the data? And why do we want to protect it? So I’m pretty old but back in the day when computers were coming out. We had floppy disk, so we would have to save everything on a floppy disk. When it would run out of storage we had to get another one. I would have to go to the store and get a packet of 20 floppy disks. Almost like the blank CD’s that they had to burn music. You would have to check to see if you had an empty one. But you coudn’t really store anything more. Then what ever you stored on those floppy’s you would have to store them in your desk. For safe keeping and make sure that no one could get them. If you didn’t label them correctly, you would then have go through all the disks to find what you had.

What a nightmare, so fast forward to now. I can essentially have a new computer every year and not lose one thing. I would have everything backed up into the cloud and with a login I would be able to access everything on my desktop. I would be up and running in an hour, and that's it. So whats the problem? Well no problem, but if you don't have a secure password then essentially anyone can access your data as well. So whatever you have on your computer anyone can access it. On top of that all your search history and login information can also be access. So your bank information and personal files.

So that's where the data protection comes into play. If you do not protect your data anyone and everyone can access it. At my current job my CEO which let me tell you my company its a non-profit and the CEO is older. He says who would want to attack a small non-profit that helps kids? Well I have to remind him, everyone does. It doesn't matter who or what you are. These hackers want money and want it fast. So they will do anything and everything to get it. So a company has data and they will try and hold that hostage for money or exploiting. It is very important to keep your data protected and secure.

Software Security

We are on my last topic that I picked, which is application software security. I will admit when I was looking at the Top 20 security tools list. I was a little confused on whats the different between the inventory and control of software assets and what is the application software security. Now that I looked further into the matter I found they are totally different. What I mean is that software assets are what is on the network. What kind of software does the organization have in the company. I had to the other day get a list of all applications that are on each server because I was going to clone the VM and upgrade the OS to windows 2019. So I had to get a list of all that is on the sever. So that is the software assets part of it. The application software security is totally different.

I hear so many people that own home computers and say they either don't have a anti-virus or they rely on the windows to do the protection. And of course this isn’t their fault this is the fact that they are not educated in the matter. So its hard for them to know what to get if they don't know. At the same time they feel they need to get something and that's it. They don't need anything else. But depending on what they have on their computer you need to make sure that you have that type of protection in your system.

There are lot of attacks that can happen and making sure that you are protected are ways to prevent some buffer overflow, XSS and SQL injection attacks. These are ways to help with that sort of attacks. I will again say what I’ve been repeating in the other sections I’ve talked about. Which is educate the users and make sure that we have update software. Have routine check ups. Limit privileges to certain people and restrict their access and only admin people can add applications. To eliminate someone downloading the wrong application and potentially downloading the wrong type of application and downloading an virus.

CIS Critical Controls Project

The topics that I picked were almost all about security protection, whether it be on the side of the hardware or the software. As we have mentioned thought out this paper, I have mentioned about the important of knowing what is on your system and protecting them. As we move towards the future. More and more are things going to have to be protected, and that’s because things are being hacked every day. One thing that I make sure in my job at work is that the computer has an active anti virus, or malware software. As a system administrator, I get notified when some machines have to update their anti-virus or malware software. So what I will be doing is installing a software that we use at my job and I will be giving instructions on how to do so.

**Implementation**

I have opened a Windows sandbox to write my instructions. I have on my USB thumb drive the FortiClinet Installer ready to download. This was given to us by FortiGate since we have a licenses with them. Copy the installer and then paste it on your Desktop once its done downloading on your desktop. Double-click on the installer. Click on yes, I have read and accepted the terms and conditions. Click next, then next, then install, and its finished. Which all the computers being on our domain. This FortiClient will get all the computers information. Then it will notify me when I have to push an update. But once you install this you will have antivirus, malware and VPN compatibility.

**Challenges**

Some of the hurtles I have faced was the fact that I have to manually put the remote gateway to make sure that the person connects to the right VPN. The reason why they did this not sure. Because we have different VPNs for different departments. The ones that I have seen you just click on Connect and then you are connected. Its all synced up at the point where the system is on the domain and connected through there. But with this one we have to make sure that we are connected to the right VPN and then are able to sign in.

**Effectiveness**

This would be good if the VPN works and the system works great, ill get notification of things that are trying to connect to our system. We will also have the ability on our dashboard how to block very specific things form one machine as well. This works really well, but then again we have about 300 employees as a company so its not that big of an organization.

**Observations/ Enhancements**

We have to have the ability to do connect to the VPN faster and without the user having to do it. We have to be able to connect with the reliability and effectiveness. Once its connected we have a great system and it does it job. Thank you for this paper because that is my next project at work is to make sure we get this working better.

Conclusion

In closing I wanted to say that these topics were great looking into. The reason for that is because it gave me more of a detailed looked into understanding these security tools. Also the importance of them. The take away that I got from this was to update all your software. Know who and what the user has. Keep track of all the systems applications of all that is on the network. Push updates as they come in and be in the know of all new malware. Do the research of all the systems and what you have.

Having all these tools will not prevent all attacks and it doesn't mean that you are invisible to all types of attacks. But it will help you to not be out in the open with no protection. It will help your data, hardware and websites that you have. Along with making sure that you wont be a victim of millions that are being attacked everyday.

References

CIS #1: Inventory and control of hardware assets. (2018, August 16). Retrieved from <https://youtu.be/ph-JpsPd5EA>

CIS #2: Inventory and control of software assets. (2018, August 16). Retrieved from <https://youtu.be/cbAV9j4bEQw>

Inventory and management of hardware assets - Top 20 security controls | Viam technologies. (n.d.). Retrieved from <https://www.viam-tech.com/blog/top-20-hardware-inventory>

Software application security: Best practices all businesses must follow - Businesstechweekly.com. (2021, February 2). Retrieved from <https://www.businesstechweekly.com/cybersecurity/application-security/application-software-security/>

Top 20 critical security controls for effective cyber defense. (2018, February 1). Retrieved from <https://blog.netwrix.com/2018/02/01/top-20-critical-security-controls-for-effective-cyber-defense/>