Welcome to an Overview of Network Security

Common Threats And how to Prevent Them

- There are a number of threats that could affect you, or your organization
- Network Security is something that everyone will need to understand
- It's your job, as an Endpoint Administrator to educate your users. I suggest that you show the users in your organization this video.

Adware – What is Adware? Adware is designed to display advertisements on your computer

- People have asked, how did adware get installed on my computer?
  Most of the time you get Adware from downloading **software bundles** – These programs install **adware** alongside programs you can get for free.
- Adware knows what types of ads to display, based on the users computing habits. Sites visited and computer usage.
- For prevention download your software from an official site, not a third-party site.

Spyware – What is Spyware? Spyware is designed to steal a user's personal information.

- Spyware is a form of malware which is short for malicious software
- Spyware is installed without the users knowledge, it runs in the background.
- Spyware can record audio, video, and record calls from your smartphone and capture credit card numbers.
  For prevention – Be selective about what you download to your computer.
  Beware of clickable advertisements

Mitigation of spyware and adware

- Be aware that free software can include spyware or malware.
- Be sure that your antimalware software is up to date.

Viruses, Trojans and Rootkits

- These are all installed without user's knowledge

What is a computer virus?

- A computer virus is a piece of code that is capable of copying itself, and has the potential of destroying data and corrupting your operating system.
- A virus can be application specific. For example, a macro virus for a Microsoft Word application can replace the regular commands with the same name, and run, when the

command is selected. These malicious macros may start automatically when a document is opened or closed, without the user's knowledge.

- A virus can be triggered by date and time or event, the virus could be triggered next time you visit a certain website as well.

Rootkit – What is a rootkit? A rootkit allows a person to get admin level access to your computer system.

Rootkits:

- Often replaces operating system files
- Allows criminals access to the device
- Applies to Windows, Linux/Unix
- For prevention avoid clicking a questionable email link. The rootkit is spread because the user clicks on a malicious link in an email, and now the root kit is spread to all recipients and sent to all the people in the users contact list.

Trojan

- Masquerades as legitimate software
- The user is fooled thinking that they are downloading and installing helpful software when in fact it is malware.
- The criminal takes control of the computer in the background and starts sending personal information over the internet to thieves.
- Trojans are executables, they have extensions like "exe" "vbs" "com "bat". Generally, you have to **open the file** before you are affected.
- For prevention do not click on an attachment unless you are sure of the source.

Mitigation of Viruses, Trojans and Rootkits

- Educate your users, define each threat. Make your users aware of what to do and what not to do.
- Be sure your antimalware is up to date
- Beware of free software

Phishing

- Tricks victims into revealing personal or sensitive information such as passwords, SSN, addresses)
- Fraudulent email messages, telephone calls, website links
- Phishing is all about stealing personal information such as username and passwords

Ransomware

- Blocks access to your computer until a ransom is paid
- It could encrypt data files until the ransom is paid
- Ransomware requests Bitcoin payments, (which are hard to trace to the recipient of the payment)
- Does not guarantee that you will get your data back if your system has been encrypted with the ransomware.
- Can be infected by **viewing** a website not just clicking.
- Ransomware features unbreakable encryption
- It can scramble your file names and add a different extension to your files.

Mitigating Phishing and ransomware

- Malware scanning
- User awareness of all the threats that are prominent in the world today.
- Frequent backups - stored separately offline
- 97% of phishing emails deliver ransomware. Don't click on any email, attachment or link that you are not 100% sure is legitimate.

Zero-Day Attacks

- This refers to a hole in software that is unknown to the vender.
- The hole is then exploited by attackers before the vender becomes aware, and hurries to fix it.
- In February 2017, a Windows SMB (server message block) Zero Day vulnerability was discovered that affected shared access to files and printers on servers running Server 2012 and 2016 and on client Windows 10 machines which caused a Denial of Service on those affected systems. Currently there is no known fix for this vulnerability. Sysadmins can block outbound SMB connections from the local network to the WAN, which diminishes the attack probability.

Summary:

- Adware – Displays ads on your computer. Mostly comes from downloaded software packages
- Spyware - Spyware can record anything you do on your smartphone
  and capture credit card numbers.
- A virus is a piece of code that has the potential of destroying data and corrupting your operating system.
- Rootkit - A rootkit allows a person to get admin level access to your computer system.

- Trojan – A criminal takes control of the computer and starts sending personal information over the internet to thieves.
- Phishing – Victims are tricked into revealing personal information
- Ransomware – Locks or encrypts your system until you pay a ransom.
  Usually demands bitcoin payments
  No guarantee that payment will result in data access.
- Zero Day - This refers to a hole in software that is unknown to the vender

In this Video:

- We identified some of the threats that could affect you or your organization?
- You should now be aware of several methods of preventing these attacks.