CYBER SECURITY BULLETIN

Cyber Security Bulletin Number: 013

Defense-in-Depth Part 1: Personal Computer

Defense in Depth is a security strategy that focuses on having multiple layers of protection for your network and computers. The theory is that if one layer is breached, there are still more protection layers in place that an attacker must go through before they get to your computer. Each layer slows the attacker down as they try to overcome it. Hopefully the attacker will either give up or move on to another target or they will be detected before they can achieve their goal:

1. For Windows users, use a licensed Operating System and licensed MS Office to avail of regular and free security updates and patches. Using a pirated or counterfeit OS makes your computer vulnerable to attacks.

2. Administrator Accounts should be used only for installation of software and periodic maintenance of the PC. Use a Standard Account for Day-to-Day Office Works.

3. Install a highly rated anti-virus program to protect you from malwares. Better yet, combine different protection programs like Ad-aware, Adwcleaner, Malwarebyte's Anti-Malware, Spybot, RUBotted and others to have layers of software protecting you from malwares. Make sure to update your anti-malware programs regularly.

4. Use a PC Auditing Program like Belarc Advisor to have a detailed profile of your installed software and hardware, network inventory, missing Microsoft hotfixes, anti-virus status, security benchmarks, and displays the results in your Web browser. All of your PC profile information is kept private on your PC and is not sent to any web server.

5. USB Thumb Drives must be scanned thoroughly, or disable autorun.inf (see more at http://support.microsoft.com/kb/967715 and at https://www.raymond.cc/blog/stop-windows-from-executing-instructions-found-in autoruninf/). Better yet, avoid using USB Thumb Drives on Work Computers. Burn data into optical discs to avoid propagation of malwares via USB thumb Drives.

6. Install a software-based firewall like Zone Alarm to have another layer of protection for your PC.

7. Install a password manager for your passwords. A good example is Keepass password manager.

8. Be informed about Social Engineering approaches of cybercriminals.(please read Cyber Security Bulletin Nr 11: Social Engineering)

9. Encrypt your Data. Take advantage of your OS built in disk encryption features such as BitLocker in Windows, or FileVault in Mac OS X. Encryption helps to ensure that if your computer is stolen that your files will be unreadable by hackers and thieves. There are also free products like TrueCrypt that you can use to encrypt partitions or your entire disk.

There is no one perfect network defense strategy, but combining multiple layers of defense will provide redundant protection should one or more layers fail. Hopefully the hackers will get tired and move on. Defense in depth is a process not a product. It's a proactive approach to thinking about security from the inside out. Certain architectural approaches such as centralized security overlays lend themselves well to solve today interior security problems. Security continues to be an ongoing process and constant vigilance and user awareness play equally important roles in building the best security posture.

REFERENCES:

http://www.sans.org/reading-room/whitepapers/bestprac/defense-depth-employing-layered-approach-protecting-federal-government-information-system-34047

http://netsecurity.about.com/od/toolsutilities/a/Protect-Your-Home-Pc-With-A-Defense-In-Depth-Strategy.htm

http://citadel-information.com/wp-content/uploads/2012/08/protecting-your-computer-an-example-of-defense-in-depth-citadel-2012.pdf

http://www.datamation.com/secu/article.php/11076_3878766_2/Top-10-Ways-to-Protect-Your-PC-Defense-in-Depth.htm

https://www.nsa.gov/ia/_files/support/defenseindepth.pdf

http://www.arubanetworks.com/pdf/technology/whitepapers/wp_Defense-in-depth.pdf