Configuring Microsoft Baseline Security in a server Environment

Albert Brandon Kirby

Florida State College at Jacksonville

Microsoft’s Baseline security policy is a policy that server or system administrators can use to make Microsoft Operating Systems more secure or a term known in the information security industry as hardening. The Baseline policy is constantly updated usual major edits are made to coincide with the public release of major operating system upgrades or service packs. The current policy has only been out since August 30th of this year(2017) and the current release is v1703 and was released to coincide with the latest Microsoft Creator’s Update around the time of it’s released to the general public. The Creator’s Update had the codename of RedStone 2 while in development before being released to members of the Microsoft Windows Insiders program which is now a program open to the public but prior to windows 10 to join the program that allows for free beta releases of Microsoft software to help contribute to Microsoft’s software/hardware and general product line you had to be a Microsoft Partner I became a Microsoft Partner myself around the time of Window’s 7 and recommend everyone who plans to use windows in their IT career take the steps to join and as well as join MSDN (Microsoft developer’s Network) as well as Microsoft Virtual Academy a free learning tool for beginners to IT pros who are interested in learning more about Microsoft’s products and development for Microsoft hardware or software compatible with all Microsoft products. I have found it to be a great resource and within 6 months of MVA;s release I was in the top 2000 students of 12 million after the most recent changes to the site I didn’t have the time to devote I once did but still find it a valuable tool when I struggle with anything MS related.

The baseline security policy can be downloaded from the Microsoft TechNet blog which is open to anyone with a Microsoft log in to use and contribute to. The baseline policy consists almost entirely of registry edits that make Windows Operating sSstems more secure. Many of these are not well known and often hidden registry keys that the average user would not be aware of how to find. This policy has been corroborated with various government 3 letter agencies the Department of Defense as well as The Center for Internet Security. Since the NSA’s massive failure at a security policy for Windows XP that made unnecessary changes or changes that lowered security. There has been an official Microsoft baseline policy available since NT 4.0 or around the windows 2000 version of the Operating systems. Building on what the NSA made and using feedback from intelligence communities as well as the Department of Defense this policy has evolved to become better over time and remove unnecessary things as the world of Information security has changed. As an example, the baseline policy once had rules about setting a desktop wallpaper which was later deemed completely unnecessary and just a ludicrous waste of time to include in the policy. The policy will continue to change and evolve and all Microsoft admins are recommended to keep up with the updates and use them for their own system administration purposes, although there is no requirement of strict compliance as what works for some does not work for all. Maybe you have a computer that will never be connected to the internet just as a kiosk or POS system in a restaurant in that case many policies would not apply to you that would apply to a fortune 500 company with billions to lose that is on a network with multiple incoming connections from around the world. If you never connect to the internet a threat from the internet is non-existent. After the NSA had their blunder with their own security policy they asked Microsoft to step in and that is where the baseline policy as we know it today was born.

There are many tools or objects available to help you adhere to the baseline policy the two I will cover are known as LGPO which is a strictly command line tool. LGPO stands for Local Group Policy Object and is available for download through the Microsoft TechNet program via their blog. Policy Analyzer is a GUI (Graphical User Interface) tool that will allow you to choose the base ine policy settings you want to use and run it against the registry to check for compliance with the baseline. There are other tools out there but these are the two main utilities (tools, or objects) I will cover and both are recommended by Microsoft.

The baseline policy is a security policy that all users of Microsoft products with an emphasis on security should be aware of know where to find and know how to implement to protect their networks and their systems from their own users, outside threats, and potential disasters due to a lack of a decent security policy. Thanks to a mistake made by the NSA and their asking Microsoft for help we now have a set of rules or recommendations that have evolved to be the Microsoft Security Baseline that all admins should be using if they aren’t they should be looking for another line of work. I would suggest Linux admin since that is my OS of choice but if they can’t handle Microsoft they should probably look for a different field in IT more suited to their skills.

References

Margosis, A. (August 30, 2017). Security baseline for Windows 10 “Creators Update” (v1703) – FINAL. Retrieved from: https://blogs.technet.microsoft.com/secguide/2017/08/30/security-baseline-for-windows-10-creators-update-v1703-final/

Margosis, A. (January 21, 2016). LGPO.exe – Local Group Policy Object Utility, v1.0. Retrieved from: https://blogs.technet.microsoft.com/secguide/2016/01/21/lgpo-exe-local-group-policy-object-utility-v1-0/

Margosis, A. (January 16, 2016). New tool: Policy Analyzer Retrieved from: https://blogs.technet.microsoft.com/secguide/2016/01/22/new-tool-policy-analyzer/

Richards, A; Beeder, C. (2002). Defrag Tools #174 - Security Baseline, Policy Analyzer and LGPO. Retrieved from: https://channel9.msdn.com//Shows/Defrag-Tools/Defrag-Tools-174-Security-Baseline-Policy-Analyzer-and-LGPO/